Jersey Financial Services Commission

Handbook for the prevention and detection of money laundering, the countering of terrorist financing, and the countering of proliferation financing

Note:

- This Handbook is applicable to all supervised persons. Supervised persons are described as 'relevant persons' in the Money Laundering (Jersey) Order 2008.
- The Handbook contains references to paraphrased Jersey AML/CFT/CPF legislation. Refer to our legislation pages for links to the full laws.
- Label references and colour-coding have been used to make the Handbook easier to navigate. The key below sets out which elements of the Handbook are mandatory and which may be treated as guidance.
- If a term is defined in the glossary, it appears in the Handbook in italic text.
- We would strongly encourage you to seek independent advice to ensure your compliance with the regulatory framework.

Key:

The below table is applicable to Sections 1-16 of this Handbook:

Section	Colour	Obligation explained
Section heading	**Blue**	Relates to all Supervised Persons (except Prescribed NPOs)
Sub-heading	**Grey**	Relates to all Supervised Persons (except Prescribed NPOs)
Statutory requirements	**Light blue**	Mandatory for all Supervised Persons (except Prescribed NPOs)
AML/CFT/CPF Codes of Practice	**Magenta**	Mandatory for all Supervised Persons (except Prescribed NPOs)
Guidance notes	**Green**	Guidance for all Supervised Persons (except Prescribed NPOs)

The sector-specific sections of this Handbook (11-16) are labelled with their relevant sector.

The below table is applicable to Section 17 of this Handbook concerning Prescribed NPOs only:

Section	Colour	Obligation explained
Section heading	**Blue**	Relates to Prescribed NPOs only
Sub-heading	**Grey**	Relates to Prescribed NPOs only
Statutory requirements	**Light blue**	Mandatory for Prescribed NPOs only
Codes of Practice	**Magenta**	Mandatory for Prescribed NPOs only
Guidance notes	**Green**	Guidance for Prescribed NPOs only

Contents

Glossary **10**

1 Introduction **21**

1.1 Objectives of the AML/CFT/CPF Handbook 22

1.2 Structure of the AML/CFT/CPF Handbook 23

1.3 Legal Status and Sanctions for Non-Compliance 25

1.3.1 AML/CFT/CPF Handbook 25

1.3.2 Money Laundering Order 25

1.3.3 AML/CFT/CPF Codes of Practice 26

1.4 Jurisdictional Scope of the Money Laundering Order and AML/CFT/CPF Codes 28

1.4.1 Application of the Money Laundering Order and AML/CFT/CPF Codes of Practice to *supervised persons* carrying on business in Jersey 28

1.4.2 Application of the Money Laundering Order to *supervised persons* carrying on business outside Jersey (overseas) 28

1.4.3 Application of AML/CFT/CPF Codes of Practice to *supervised persons* carrying on business outside Jersey (overseas) 30

1.5 Definition of Supervised Business 30

1.6 Business relationships and one-off transactions 30

1.7 Risk-based approach 31

1.8 Equivalence of requirements in other countries and territories 32

1.8.1 Equivalent business 32

1.8.2 Equivalent countries and territories 32

1.8.3 Determining equivalence 33

2 Corporate Governance **34**

2.1 Overview of section 34

2.2 Measures to prevent money laundering, the financing of terrorism, and the financing of proliferation 34

2.3 Board responsibilities 34

2.3.1 Business risk assessment 36

2.4 Adequate and effective systems and controls 39

2.4.1 Effectiveness of systems and controls 41

2.4.2 Testing of compliance with systems and controls 43

2.4.3 Consideration of cultural barriers 43

2.4.4 Outsourcing 45

2.5 The Money Laundering Compliance Officer (MLCO) 46

2.6 The Money Laundering Reporting Officer (MLRO) 48

2.7 Financial groups 50

3 Identification measures – Overview **52**

3.1 Overview of section 52

3.2 Obligation to apply identification measures 52
3.3 Risk-based approach to Identification Measures 55
3.3.1 Understanding ownership structure – Stage 1.1 58
3.3.2 Information for assessing risk – Stage 1.4 59
3.3.3 Source of Funds – Stage 1.4 60
3.3.4 Assessment of risk – Stage 2.1 61
3.3.5 Customer business and risk profile – Stage 2.2 66
3.3.6 Prepaid cards 67
3.4 On-going monitoring: ensuring that documents, data and information are up to date and remain relevant 72
3.5 Identification measures – taking on a book of business 72

4 Identification Measures – Finding Out Identity and Obtaining Evidence 74
4.1 Overview of section 74
4.2 Obligation to find out identity and obtain evidence 75
4.3 Obligation to find out identity and obtain evidence: individuals 75
4.3.1 Finding out identity 76
4.3.2 Obtaining evidence of identity 76
4.3.3 Suitable certification 80
4.3.4 Obtaining Evidence of Identity – Independent Data Sources 83
4.3.5 Use of electronic identification (E-ID) 84
4.3.6 Guarding against the financial exclusion of Jersey residents 92
4.3.7 Residential Address: Overseas Residents 93
4.4 Obligation to find out Identity and obtain evidence: Legal Arrangements 94
4.4.1 Finding out identity – Legal arrangement that is a trust 96
4.4.2 Obtaining Evidence of Identity – Legal Arrangement that is a Trust 97
4.4.3 Finding out identity – Legal Arrangement that is a Limited Partnership 98
4.4.4 Obtaining Evidence of Identity – Legal Arrangement that is a Limited Partnership 99
4.4.5 Copy documentation provided by regulated trust and company services provider 101
4.5 Obligation to find out identity and obtain evidence: Legal Persons 101
4.5.1 Finding out identity – Legal Person that is a company 104
4.5.2 Obtaining evidence of identity – Legal person that is a company 106
4.5.3 Finding out identity – Legal person that is a foundation 107
4.5.4 Obtaining evidence of identity – Legal person that is a foundation 109
4.5.5 Finding out identity – Legal Person that is a partnership 110
4.5.6 Obtaining evidence of identity – Legal person that is a partnership 112
4.5.7 Copy documentation provided by regulated trust and company services provider 113
4.6 Obligation to find out identity and obtain evidence: Person purporting to act for the customer 114
4.7 Timing of Identification Measures 115
4.7.1 Timing of identification measures during business relationship – Obtaining evidence 118
4.7.2 Timing for “Existing Customers” 118
4.8 Failure to Complete Identification Measures 120

5 Identification Measures – Reliance on Obliged Persons 122
5.1 Overview of section 122
5.1.1 Assessment of Risk 127
5.2 Group Reliance 129

6 Ongoing Monitoring – Scrutiny of transactions & activity 131
6.1 Overview of section 131
6.2 Obligation to perform on-going monitoring 131
6.2.1 Scrutiny of transactions and activity 132
6.2.2 Monitoring and recognition of business relationships and transactions – Person connected with an enhanced risk state or sanctioned country 136
6.3 Automated monitoring methods 138
6.4 Money laundering warning signs 140
6.4.1 Secretive customers 140
6.4.2 Unusual instructions 140
6.4.3 Use of client accounts 141
6.4.4 Money laundering offences factors 142
6.4.5 Administration of estates 143
6.4.6 Charities 144
6.4.7 Taxation matters 144
6.4.8 Observation of unlawful conduct 145

7 Enhanced and simplified CDD measures and exemptions 146
7.1 Overview of section 146
7.2 Requirement to apply enhanced CDD measures 147
7.3 Higher risk customer 147
7.4 Customer not physically present for Identification Measures 149
7.5 Customer with relevant connection to an enhanced risk state 151
7.5.1 Application of enhanced CDD measures to a customer with a relevant connection to an enhanced risk state 151
7.6 Customer who is a Politically Exposed Person (PEP) 153
7.6.1 Determining whether a customer is a PEP 154
7.6.2 Enhanced customer due diligence measures in relation to PEPs 154
7.7 Non-resident customer 158
7.8 Customer provided with private banking services 158
7.9 Customer that is a personal asset holding vehicle 159
7.10 Customer that is a company with nominee shareholders or issues bearer shares 160
7.11 Correspondent banking and similar relationships 161
7.12 Enhanced CDD measures – transitional arrangements 163
7.13 Exemptions from CDD Requirements – Overview 163
7.14 Exemption from applying third party identification requirements in relation to relevant customers acting in certain regulated, investment or fund services business 165

7.15 Exemption from applying third party identification requirements in relation to certain relevant customers involved in unregulated or non-public funds, trust company business or the legal profession 166
7.15.1 Assessment of risk 168
7.16 Further exemptions from applying identification requirements 171
7.16.1 Pension, superannuation, employee benefit, share option or similar schemes ... 172
7.16.2 Jersey Public Authority 173
7.16.3 Body Corporate/limited liability company with Listed Securities 173
7.16.4 Regulated persons and those carrying on equivalent business 174
7.16.5 Person authorised to act on behalf of a customer 174
7.17 Simplified Identification Measures – Obtaining evidence of identity for very low risk products/services 175

8 Reporting money laundering and the financing of terrorism, and sanctions reporting obligations 177
8.1 Overview of section 177
8.2 Reporting knowledge or suspicion 177
8.2.1 Requirement to report knowledge or suspicion 179
8.2.2 Protective report 182
8.2.3 What constitutes knowledge or suspicion? 184
8.3 Procedures for Reporting 185
8.3.1 Internal *SARs* 186
8.3.2 External *SARs* 187
8.4 JFCU Consent 189
8.5 Tipping off 190
8.5.1 CDD Measures 193
8.5.2 Terminating a business relationship 194
8.6 Disclosure to group companies and networks 194
8.7 Investigation and the use of court orders 195
8.7.1 Updates/Feedback from the JFCU 195
8.8 Sanctions compliance reporting obligations under the Sanctions and Asset-Freezing Law 196

9 Screening, awareness and training of employees 200
9.1 Overview of section 200
9.2 Screening of *employees* 200
9.3 Obligations to promote awareness and to train 201
9.4 Awareness of relevant employees 203
9.4.1 Monitoring and testing effectiveness 204
9.4.2 Technological developments 204
9.5 Training of *employees* 205
9.5.1 All relevant employees 205
9.5.2 The Board or equivalents 206
9.5.3 The *MLCO* 206

9.5.4 The MLRO and Deputy MLRO(s) 206
9.5.5 Non-relevant *employees* 207
9.5.6 Timing and frequency of training 207
9.5.7 Monitoring the effectiveness of screening, awareness and training 207

10 Record-keeping 208
10.1 Overview of section 208
10.2 Recording evidence of identity and other *CDD* measures 208
10.3 Recording transactions 209
10.4 Other recording-keeping requirements 211
10.4.1 Corporate governance 211
10.4.2 Identification measures 211
10.4.3 On-going monitoring 212
10.4.4 SARs 212
10.4.5 Screening, awareness and training of *employees* 213
10.5 Access and retrieval of records 213
10.5.1 External record-keeping 213
10.5.2 Reorganisation or termination 214
10.6 Disclosure of records 214

11 Wire Transfers 216
11.1 Overview of Section 216
11.2 Scope of the Wire Transfers Regulations 217
11.3 Outgoing transfers – obligations upon the PSP of the payer 218
11.3.1 Transfers for non-account holders 218
11.3.2 Transfers for Account holders 219
11.3.3 Batch Files – payments either inside or outside of British Islands 221
11.4 Incoming Transfers - Obligation on the PSP of the payee and IPSP 221
11.4.1 Admissible characters or input and missing information checks 222
11.4.2 Managing transfers of funds with missing information or inadmissible characters or inputs 223
11.4.3 Failure to provide information 224
11.4.4 Additional obligations on IPSPs 225
11.5 Reporting of breaches 225
11.6 Information, data protection and record retention 226
11.7 Offences and criminal liability 227

12 Trust Company Business 228
12.1 Definition of Trust Company Business 228
12.2 Identification measures 228
12.2.1 Obligation to apply Identification Measures 228
12.2.2 Information for assessing risk – Stage 1.4 229
12.2.3 Assessment of risk – Stage 2.1 231
12.2.4 Identification measures: Finding out identity and obtaining evidence 231

12.2.5 Timing of identification measures 235
12.2.6 Failure to complete identification measures 236
12.2.7 Provision of information by trustees 237

13 Funds and Fund Operators 238
13.1 Overview of section 238
13.2 AML/CFT/CPF risk assessments 240
13.2.1 Overview – Obligation to conduct risk assessments 240
13.2.2 Business risk assessment 240
13.2.3 Customer risk assessment – Risk indicators 246
13.2.4 Risk assessments for SPV governing bodies 248
13.2.5 Documenting risk assessments 248
13.3 Customer Identification Measures 249
13.3.1 Obligation to apply identification measures 250
13.3.2 Identification Measures - Fund operators 252
13.3.3 Identification Measures - Unit trusts 253
13.3.4 Fund operators – Passive investors 254
13.3.5 Fund operators - Promoters 255
13.3.6 Multiple layers 255
13.3.7 Nominees/Investment managers 257
13.3.8 Fund operators – Residual assets 259
13.4 Timing of identification measures 259
13.5 Failure to complete identification measures 259
13.6 Updating identification information 260
13.7 On-going monitoring: Scrutinising of transactions & activity 260
13.8 Collation of CDD 261
13.8.1 Exemptions from identification measures 261
13.8.2 Reliance on obliged persons 263
13.8.3 Obtaining copy documentation from a supervised Trust and company service provider in the Crown Dependencies 263
13.8.4 Outsourcing 264
13.9 Enhanced due diligence measures – Non-Jersey investors 265

14 Estate Agents and High Value Dealers 266
14.1 Definition of estate agents and high value dealers undertaking Supervised Business 266
14.1.1 Estate agents 266
14.1.2 High value dealers 267
14.2 Identification measures: Finding out identity and obtaining evidence 270
14.2.1 Obligation to find out identity and obtain evidence 270
14.2.2 Timing of identification measures 270
14.2.3 Timing for 'existing customers' 271
14.3 Exemptions from *CDD* measures – Jersey property transactions 272
14.4 Business risk assessment 272
14.4.1 Service area vulnerabilities and warning signs – Estate agents 272

14.4.2 Criminal use of conveyancing services Estate Agents 273
14.4.3 Recognising suspicious behaviour and unusual instructions Estate Agents 274
14.4.4 Service area vulnerabilities and warning signs – High Value Dealers 277
14.4.5 Recognising suspicious behaviour and unusual transactions – High Value Dealers277

15 Lawyers 284
15.1 Definition of Lawyers undertaking Supervised Business 284
15.1.1 Activities to which the Money Laundering Order applies 284
15.2 Business relationships and one-off transactions 286
15.3 Business Risk Assessment 287
15.3.1 Considering and assessing service area vulnerabilities and warning signs 287
15.4 Corporate governance 295
15.4.1 The Money Laundering Reporting Officer 295
15.5 Identification Measures: Finding out identity and obtaining evidence 295
15.5.1 Timing of Identification Measures 295
15.5.2 Timing for "existing clients" 296
15.5.3 Ascertaining Legal Position 296
15.6 Exemptions from CDD measures 297
15.6.1 Exemption from applying third party identification requirements in relation to certain relevant customers involved in *trust company business* 297
15.6.2 Jersey property transfers 300
15.7 Reporting Money Laundering and Terrorist Financing Activity 300
15.7.1 Legal Professional Privilege (LPP) 300

16 Accountants 306
16.1 Definition and overview of Accountants undertaking supervised business 306
16.1.1 Accountancy Services 306
16.1.2 Tax Advisers 306
16.1.3 Audit Services 307
16.1.4 Insolvency services 308
16.1.5 Accountants undertaking Supervised Business 308
16.2 Business Risk Assessment 309
16.2.1 Considering customer and service risks to the business 309
16.3 Risk-based approach to Identification Measures 311
16.4 Identification Measures 312
16.4.1 Obligation to find out identity and obtain evidence: Individuals 312
16.4.2 Timing of identification measures 313
16.4.3 Timing for "Existing Clients" 313
16.4.4 Ascertaining Legal Position 313
16.5 Exemptions from CDD Measures 314
16.6 Money laundering, terrorist financing, and proliferation financing warning signs for the Accountancy Sector 315
16.6.1 Accountancy and Audit Services 316

16.6.2 Tax Advisers 316
16.6.3 Business recovery or receiverships 317
16.7 Reporting Money Laundering and Terrorist Financing activity 318
16.7.1 Further enquiries by auditors 318
16.7.2 Auditor's responsibility for monitoring compliance 319
16.7.3 Reporting to regulators 321
16.7.4 Balancing Professional Work and Post-Reporting Requirements 321
16.7.5 Auditor's report on financial statements 322
16.7.6 Resignation as auditor 323

17 Prescribed Non-profit organisations 324
17.1 Introduction 325
17.2 Vulnerabilities of Prescribed NPOs 326
17.3 Risk-based approach 327
17.3.1 NPO programme risk assessment (NPO PRA) and associated *activities* 328
17.3.2 Ongoing risk monitoring 332
17.4 NPO Beneficiaries, Associate NPOs and donors 334
17.4.1 NPO Beneficiaries 334
17.4.2 Associate NPOs 336
17.4.3 NPO donors 341
17.5 Identification, screening and training of relevant volunteers, relevant employees, owners and controllers 343
17.5.1 Overview of section 343
17.5.2 Identifying NPO owners and controllers 343
17.5.3 Screening of relevant volunteers, relevant employees and controllers 345
17.5.4 Training and awareness of relevant volunteers, relevant employees and controllers 346
17.6 Accounting for funds 349
17.7 Record-keeping 350
17.7.1 Overview and general requirements 350
17.7.2 Access and retrieval of records 352
17.7.3 External records 352
17.7.4 Reorganisation or termination 353

GLOSSARY

Term	Definition
accountancy services	Has the meaning given in Section 16.1.1 of the AML/CFT/CPF Handbook.
Anti-Money Laundering and Counter-Terrorism Legislation	Has the meaning given in Article 3(1) of the Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008 [the *Supervisory Bodies Law*].
AML/CFT/CPF	Anti-money laundering/countering the financing of terrorism/countering proliferation financing.
AML/CFT/CPF programme	A programme against money laundering, terrorist financing, and proliferation financing which includes policies and procedures by which every member of the group who carries on a financial services business (or equivalent) shares information that is appropriate for the purpose of preventing and detecting money laundering, terrorist financing, and proliferation financing.
AML/CFT/CPF Codes of Practice	Codes of Practice for supervised persons, issued under Article 22 of the Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008 [the *Supervisory Bodies Law*]. This includes Codes in Sections 1 to 10 that relate to all *supervised persons* and Codes that relate to particular activities in the sector-specific Sections 11-16.
AML/CFT/CPF Handbook	Handbook for the prevention and detection of money laundering, the countering of terrorist financing, and the countering of proliferation financing. May also be referred to as "the Handbook" or "this Handbook".
associate NPO	Has the meaning given in Article 6(2) of the Non-Profit Organisations (Prescribed NPOs – Additional Obligations) (Jersey) Order 2022 [the Prescribed NPO Order]. May also be referred to as "partners" by the NPO sector.
audit services	Has the meaning given in paragraph 2(3) of Part B of Schedule 2 to the Proceeds of Crime (Jersey) Law 1999 [the *Proceeds of Crime Law*].
Basel Committee	Basel Committee on Banking Supervision.
BB(J) Law	Banking Business (Jersey) Law 1991.
Beneficial owners and/or controllers	Has the meaning set out in Article 2 of the Money Laundering (Jersey) Order 2008 [the *Money Laundering Order*].
BRA	Business Risk Assessment.
business relationship	Has the meaning set out in Article 1 of the Money Laundering (Jersey) Order 2008 [the *Money Laundering Order*]. Certain professions may refer to a business relationship as a "matter".
CDD	Customer due diligence.
CFT	Countering the financing of terrorism.
CIF(J) Law	Collective Investment Funds (Jersey) Law 1988.

Term	Definition
Collective investment scheme	Means any of the funds specified in Article 13(10) of the Money Laundering (Jersey) Order 2008 [*the Money Laundering Order*].
Commission Law	Financial Services Commission (Jersey) Law 1998.
Companies Law	Companies (Jersey) Law 1991.
Compliance Officer	Has the meaning given in Article 1 of the Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008 [the *Supervisory Bodies Law*].
CPF	Countering proliferation financing
CRA	Customer risk assessment.
Customer	A person with whom a *business relationship* has been formed or *one-off transaction* carried out. References to *customer* also include, where appropriate, a prospective *customer* (an applicant for business) with whom a *business relationship* is to be established or *one-off transaction* carried out. A *customer* may be an individual (or group of individuals) or a legal person. May also be referred to by Industry as a 'client'.
Deposit-taking business	Has the meaning given in Article 3 of the Banking Business (Jersey) Law 1991 [the *BB(J) Law*].
Deputy MLRO	A person designated by the *supervised person* to whom suspicious activity reports may be made.
Designated Police or Customs Officer	Police and customs officers that hold posts within the Joint Financial Crimes Unit [*JFCU*], as per notices issued under Article 6(1) and Article 6(2) of the Money Laundering (Jersey) Order 2008 [*the Money Laundering Order*].
designated person	Has the meaning given in Article 9 of the Sanctions and Asset-Freezing (Jersey) Law 2019 [the *Sanctions and Asset-Freezing Law*].
Designated relationship	A relationship established by a *customer* on behalf of one third party, including a relationship involving sub-accounts for each third party.
Directions Law	Money Laundering and Weapons Development (Directions) (Jersey) Law 2012.
Diversion	Transactions by a non-profit organisation's [*NPO*] NPO Representatives or external parties such as associate NPOs that divert NPO Funds away from the *NPO*'s legitimately intended purposes to a terrorist, terrorist cell or terrorist organisation for them to benefit from, directly or indirectly.
DNFBPs	Designated Non-Financial Businesses and Professions, as defined in the FATF glossary.
DPRK	Democratic People's Republic of Korea
EEA	European Economic Area.
E-ID	Electronic Identification.

Term	Definition
Employee	Includes officers of a *supervised person* and is not limited to individuals working under a contract of employment. Includes temporary and contract employees, and the employee of any external party fulfilling a function in relation to a *supervised person* under an outsourcing agreement. Please note that a variation of this definition applies to Section 17 (Prescribed NPOs), using the term "relevant employees".
Enhanced customer due diligence (measures) or enhanced CDD measures	Has the meaning given in Article 1 of the Money Laundering (Jersey) Order 2008 [the *Money Laundering Order*].
enhanced risk state	Has the meaning given in Article 15(1)(c) of the Money Laundering (Jersey) Order 2008 [the *Money Laundering Order*]. Refer to Appendix D1 of the *AML/CFT/CPF Handbook* for the current list of *enhanced risk states*.
equivalent business	Has the meaning given in Article 5 of the Money Laundering (Jersey) Order 2008 [*the Money Laundering Order*].
estate agency services	Has the meaning given in Paragraph 3 of Part B of Schedule 2 to the Proceeds of Crime (Jersey) Law 1999 [the *Proceeds of Crime Law*].
EU	The European Union.
EU Regulation	Regulation (EU) 2015/847 of 20 May 2015 on information accompanying transfers of funds.
external accountancy services	Has the meaning given in paragraph 2(2) of Part B of Schedule 2 to the Proceeds of Crime (Jersey) Law 1999 [the *Proceeds of Crime Law*].
Facilitator	An *active* supporter of a terrorist, terrorist cell or terrorist organisation, e.g. a terrorist financier, a regulated and registered professional or a recruiter.
FATF	The Financial Action Task Force.
FATF Recommendations	The *FATF* Recommendations adopted on 16th February 2012 and as amended to the date of issue of this Handbook.
financial group	A collection of persons who are members of the same group, each person fulfilling the conditions set out in Article 1(5) of the Money Laundering (Jersey) Order 2008 [the *Money Laundering Order*].
Financial Institutions	As defined in the *FATF* glossary.
financial services business	Has the meaning in Article 36 of the Proceeds of Crime (Jersey) Law 1999 [the *Proceeds of Crime Law*].
financing of proliferation	For the purposes of this Handbook, this term means: Conduct which creates the risk of non-implementation, breaching, circumvention, or evasion of the Targeted financial sanctions related to proliferation of weapons of mass destruction and its financing, effective in Jersey

Term	Definition
	Persons involved in the financing of proliferation are sometimes described as *proliferators* or *proliferation financiers*.
financing of terrorism	For the purposes of this Handbook, means: › Conduct which is an offence under any provision of Articles 15, 16 and 16A of the Terrorism (Jersey) Law 2002 [the Terrorism Law] › Conduct outside Jersey which, if occurring in Jersey, would be an offence under Articles 15, 16 and 16A of the Terrorism Law › Conduct which is an offence under any provision of Article 21 of the Terrorism Law, and › Conduct which is an offence under any provision of Parts 3, 4 and 6 of the Sanctions and Asset-Freezing (Jersey) Law 2019 [the Sanctions and Asset-Freezing Law]. May also be referred to as *terrorist financing*. Persons involved in the *financing of terrorism* are sometimes described as *terrorist financiers*.
Foundations Law	Foundations (Jersey) Law 2009.
FSIU	Financial Sanctions Implementation Unit, part of Jersey's Ministry of External Relations.
FS(J) Law	Financial Services (Jersey) Law 1998.
FSRB	FATF Style Regional Body.
Guidance notes	Present ways of complying with the *statutory requirements* and *AML/CFT/CPF Codes of Practice* and must always be read in conjunction with these.
Hawala	Hawala refers to a traditional system of transferring money without money movement. It is done with the help of a brokering third party and it is predominantly used in the Middle East, Africa and South Asia. These payment systems may also be referred to as Hundi or Havala.
higher risk country or territory	A country or territory which a *supervised person* has concluded presents a higher risk of *money laundering*, the *financing of terrorism*, and the *financing of proliferation*, using reliable and independent third party sources.
IAIS	International Association of Insurance Supervisors.
IB(J) Law	Insurance Business (Jersey) Law 1996.
ICC	Incorporated cell company.
identification measures	Those measures described in Article 3(2) of the Money Laundering (Jersey) Order 2008 [the *Money Laundering Order*].
IMF	International Monetary Fund.
insolvency practitioners	Those in the business of undertaking *insolvency services*.

Term	Definition
insolvency services	Has the meaning given in paragraph 2(4) of Part B of Schedule 2 to the Proceeds of Crime (Jersey) Law 1999 [the *Proceeds of Crime Law*].
IOSCO	International Organization of Securities Commissions.
JFCU	The Joint Financial Crimes Unit, an arm of the States of Jersey Police. The *JFCU* is the body designated as the financial intelligence unit under Regulation 2 of the Proceeds of Crime (Financial Intelligence) (Jersey) Regulations 2015. Officers of the *JFCU* are the designated police and customs officers for the purposes of the Money Laundering (Jersey) Order 2008 [the *Money Laundering Order*].
JFSC	Jersey Financial Services Commission (abbreviated in relevant Jersey legislation as "the Commission").
Lawyers	Persons carrying on the business described at Paragraph 1 of Part B of Schedule 2 to the Proceeds of Crime (Jersey) Law 1999 [the *Proceeds of Crime Law*].
Licence	A generic term to cover: › A registration granted under the Banking Business (Jersey) Law 1991 [the *BB(J) Law*] › A permit granted pursuant to the Collective Investment Funds (Jersey) Law 1988 [the *CIF(J) Law*] › A certificate issued pursuant to the Collective Investment Funds (Jersey) Law 1988 [the *CIF(J) Law*] › A registration granted under the Financial Services (Jersey) Law 1998 [the *FS(J) Law*] › A permit granted pursuant to the Insurance Business (Jersey) Law 1996 [the *IB(J) Law*].
limited liability company	Has the meaning given in Article 1(1) of the Money Laundering (Jersey) Order 2008 [the *Money Laundering Order*].
LPP	Legal professional privilege. This term covers both advice privilege and litigation privilege (see Section 15.7.1).
(the) Minister	Unless otherwise specified, means the Minister for External Relations and Financial Services.
MLCO	Money Laundering Compliance Officer, as described in Article 7 of the Money Laundering (Jersey) Order 2008 [the *Money Laundering Order*].
MLRO	Money Laundering Reporting Officer, as described in Article 8 of the Money Laundering (Jersey) Order 2008 [the *Money Laundering Order*]. Also refer to *Deputy MLRO* above.

Term	Definition
money laundering	For the purposes of this Handbook, means: › Conduct which is an offence under any provision of Articles 30 and 31 of the Proceeds of Crime (Jersey) Law 1999 [the Proceeds of Crime Law] › Conduct which is an offence under any provision of Articles 34A and 34D of the Proceeds of Crime Law, and › Conduct which falls within the definition of financing of terrorism set out in this Handbook. Persons involved in *money laundering* are sometimes described as *money launderers*.
Money Laundering Order	Money Laundering (Jersey) Order 2008.
NPO	Non-profit organisations – defined under Article 1 of the Non-Profit Organizations (Jersey) Law 2008 [the *NPO Law*]. The definitions extend to both *Regulated NPOs* and *Registered NPOs.* The sector, including all NPOs may also be referred to as the non-profit sector.
NPO Beneficiaries	Natural persons or groups of natural persons who receive humanitarian, charitable or other types of assistance through the services of a non-profit organisation [*NPO*].
NPO Funds	This term includes both money and NPO Resources that may be of value to terrorists, terrorist cells or terrorist organisations. Value does not need to include physical assets, it can for example be provision of training.
NPO Law	Non-Profit Organizations (Jersey) Law 2008.
NPO Owners and/or Controllers	For the purposes of this Handbook, means the individuals listed at Articles 4(1)(a) and 4(1)(b) of the Prescribed Non-profit Organisations (Jersey) Order 2022 [the Prescribed NPO Order].
NPO Representative	Referring to a Board member (or its equivalent), an employee, volunteer or another individual acting in an official capacity representing the non-profit organisation [*NPO*], irrespective of whether that person is paid for their services or not.
NPO Resources	Includes financial and non-financial non-profit organisation [*NPO*] assets (e.g. donations, gifts/benefits-in-kind, property of every kind, documentation and personnel).
obliged person	Has the meaning given in Article 1 the Money Laundering (Jersey) Order 2008 [the *Money Laundering Order*].
one-off transaction	Has the meaning given in in Article 4 of the Money Laundering (Jersey) Order 2008 [the *Money Laundering Order*].
PCC	A protected cell company.
PEP	Politically Exposed Person – an individual who is any of the following (within the meaning of Article 15A of the Money Laundering (Jersey) Order 2008 *[*the *Money Laundering Order]*: (a) A domestic politically exposed person;

Term	Definition
	(b) A foreign politically exposed person; or (c) A prominent person.
policies and procedures	The way in which a business' systems and controls are implemented into the day-to-day operation of the business.
pooled relationship	A relationship established by a *customer* on behalf of more than one third party.
Prescribed NPO	Has the meaning given in Article 1 of the Non-Profit Organisations (Prescribed NPOs – Additional Obligations) (Jersey) Order 2022 [the *Prescribed NPO Order*]. The sub-set of *NPOs* which present a higher risk of being abused for terrorist financing purposes.
Prescribed NPO Order	Non-Profit Organisations (Prescribed NPOs – Additional Obligations) (Jersey) Order 2022.
Proscribed terrorist organisation	Individuals or organisations that are placed on national and international lists of actors known to be engaged in terrorist activities Jersey's proscribed terrorist organisation list may be accessed via the JFSC's Sanctions designations lists webpage. Part 2 of the Terrorism Law sets out that the UK's proscribed list automatically forms part of the Jersey proscribed list, hence both lists must be considered.
Proceeds of Crime Law	Proceeds of Crime (Jersey) Law 1999.
proliferation financing	Refer to the definition of *financing of proliferation*.
PTC	Private Trust Company - has the meaning set out in Paragraphs 4 and 4A of the Schedule to the Financial Services (Trust Company Business (Exemptions)) Jersey Order 2000.
regulated business	Has the meaning provided given in Article 1 of the Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008 [the *Supervisory Bodies Law*].
regulated market	Has the meaning given in Article 2(5) of the Money Laundering (Jersey) Order 2008 [the *Money Laundering Order*]. To access the list of *EU*-regulated markets, follow this link and select 'Regulated Market' from the 'Entity Type' drop-down list.
regulated person	Has the meaning given in Article 1 of the Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008 [the *Supervisory Bodies Law*].
Regulatory Laws	A collective name of the following four laws: › The Banking Business (Jersey) Law 1991 [the *BB(J) Law*] › The Collective Investment Funds (Jersey) Law 1988 [the *CIF(J) Law*] › The Financial Services (Jersey) Law 1998 [the *FS(J) Law*] › The Insurance Business (Jersey) Law 1996 [the *IB(J) Law*].

Term	Definition
reliance identification measures	Has the meaning given in Article 16(1) of the Money Laundering (Jersey) Order 2008 [the *Money Laundering Order*].
relevant connection	Has the meaning given in Article 15(2)(b) of the Money Laundering (Jersey) Order 2008 [the *Money Laundering Order*].
relevant employee	An employee whose duties relate to the provision of a *financial services business*.
relevant financial institution	Has the meaning given in Article 1 of the Sanctions and Asset-Freezing (Jersey) Law 2019 [the *Sanctions and Asset-Freezing Law*].
relevant person	Means, for the purposes of this Handbook, a person carrying on a *financial services business* (as described in Schedule 2 of the Proceeds of Crime (Jersey) Law 1999 [the *Proceeds of Crime Law*]), and which is carrying on that business in or from within Jersey, or, if a Jersey legal person, carrying on that business in any part of the world. This definition **does not** capture a person carrying on the business of acting, other than by way of business, as the trustee of an express trust. Where specific articles of the Money Laundering (Jersey) Order 2008 [the *Money Laundering Order*] proscribe that the term *relevant person* includes a person who **was formerly** a *relevant person*, any references to *relevant person* in this Handbook that relate to or are derived from those particular articles should also have the same meaning.
sanctioned country or territory	Means, at any time, a country or territory which is itself, or whose government (or equivalent) is, the subject of any sanctions broadly prohibiting dealings with such government (or equivalent), country or territory, including trade sanctions, arms embargoes and other trade restrictions in force in Jersey (refer to Sources 6 and 12 of Appendix D2 of this Handbook for current list of sanctioned countries and territories).
sanctioned person	Means a person or entity listed on the sanctions designations lists under the Jersey sanctions regime.
Sanctions and Asset-Freezing Law	Sanctions and Asset-Freezing (Jersey) Law 2019
SAR	Suspicious Activity Report.
Schedule 2 Business	Has the meaning given in Article 1 of the Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008 [the *Supervisory Bodies Law*].
sensitive activities	Refers to activities that have been established, as a matter of policy, by the Jersey Financial Services Commission [the *JFSC*] as sensitive activities, and which are listed in the *JFSC's* Sound Business Practice Policy.
similar identification measures	Has the meaning given in Article 16A(1) of the Money Laundering (Jersey) Order 2008 [the *Money Laundering* Order].
sole trader	Has the meaning given in Article 1 of the Money Laundering (Jersey) Order 2008 [the *Money Laundering* Order].

Term	Definition
source of funds	The activity that generates the funds for a *customer* (e.g. salary, trading revenues, or payments out of a trust). *Source of funds* relates directly to the economic origin of funds to be used in a *business relationship* or *one-off transaction*.
source of wealth	The activities that have generated the total net worth of a *customer* (e.g. ownership of a business, inheritance, or investments). Source of wealth is the origin of the accrued body of wealth of an individual.
SPV	Special Purpose Vehicle – An entity established for a specific purpose e.g. to act as a governing body of a specific fund.
specified Schedule 2 business	Has the meaning given in Article 1 of the Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008 [the *Supervisory Bodies Law*].
statutory requirements	describe the statutory provisions that must be complied with by a supervised person (natural or legal) when carrying on a supervised business, in particular requirements set out in the Money Laundering Order.
supervised business	Has the meaning given in Article 1 of the Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008 [the *Supervisory Bodies Law*].
supervised person	Defined in Article 1 of the Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008 [the *Supervisory Bodies Law*]. Covers persons that are required to comply with the Money Laundering (Jersey) Order 2008 [the *Money Laundering Order*] (referred to in the *Money Laundering Order* as "relevant persons"). *Prescribed NPOs* are also classed as *Supervised Persons*. References in this Handbook where legislation is quoted, summarised or paraphrased will be to *relevant persons* to align with the *Money Laundering Order*.
Supervisory Bodies Law	Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008.
Sympathiser	An individual who is *not actively* engaged in terrorist acts but that supports individual terrorists, terrorist cells or terrorist organisations indirectly.
systems and controls	A *supervised person's* general framework to combat *money laundering,* the *financing of terrorism,* and the *financing of proliferation*.
Targeted Financial Sanctions Measures	Targeted Financial Sanctions Measures include any measures made under: › The Sanctions and Asset-Freezing (Jersey) Law 2019 › Any Regulations or Orders made under the enactment falling within the above law (e.g. the Sanctions and Asset-Freezing (Implementation of External Sanctions) (Jersey) Order 2021).
tax advisers	Persons providing, by way of business, the service set out at Paragraph 2(1)(b) of Part B of Schedule 2 to the Proceeds of Crime (Jersey) Law 1999 [the *Proceeds of Crime Law*].

Term	Definition
Terrorism and related terms	"Terrorism", "act of terrorism" and "terrorist entity" are defined in the Terrorism (Jersey) Law 2002 [the Terrorism Law]. "Terrorist activity" is defined in Article 18 of the Sanctions and Asset-Freezing (Jersey) Law 2019 [the Sanctions and Asset-Freezing Law]. For the purposes of this Handbook, Targeted financial sanctions related to terrorism and terrorist financing are those described on the JFSC's website.
Terrorism Law	Terrorism (Jersey) Law 2002.
terrorist financing	Refer to the definition of *financing of terrorism*.
TF Recruitment	Active and passive processes through which terrorists, terrorist cells and terrorist organisations seek to enlist operational personnel, facilitated by a recruiter.
Third party identification requirements	Has the meaning given at Article 17 of the Money Laundering (Jersey) Order 2008 [the *Money Laundering Order*].
Tipping Off Regulations	Proceeds of Crime and Terrorism (Tipping Off – Exceptions) (Jersey) Regulations 2014.
Transfer risk	This risk manifests in multiple ways, all ultimately benefiting terrorists, terrorist cells or terrorist organisations directly or indirectly. It is closely related to fraud, corruption and bribery risks. Examples of transfer risk materialising into *Diversion* are the risk of transferring Funds to terrorists directly or indirectly, for example by the NPO: 1. Paying salaries to a Facilitator, making donations to a Terrorist, making cash payments to settle access fees such as road checkpoint tools or other forms of 'taxation' to Facilitators, such as making donations for particular causes as directed by them, including where tender processes have been predetermined, to certain suppliers or where this means Terrorists or Facilitators are obtaining access to Resources, influencing aid locations and Beneficiaries. At times, such payments may also be misrepresented in the NPOs financial records as fees for logistics, security etc. 2. The risk of transferring Funds to another Charity, NPO, or associate NPO that, in turn, suffers the transfer risk materialising as noted under (1).
Trust Company Business	Subject to any Order under Article 4 of the Financial Services (Jersey) Law 1998 [the *FS(J) Law*], has the meaning given at Article 2(3) of the *FS(J) Law*. Persons carrying on Trust Company Business may also be referred to as "Trust and Company Service Providers" or "TCSPs".
UN	The United Nations.
UNSC	United Nations Security Council.
unit	Has the meaning given in Article 1(1) of the Collective Investment Funds (Jersey) Law 1988 [*the CIF(J) Law*].

Term	Definition
VAT	Value Added Tax.
Wire Transfers Regulations	EU Legislation (Information Accompanying Transfers of Funds) (Jersey) Regulations 2017.

1 INTRODUCTION

1. The continuing ability of Jersey's finance industry to attract legitimate customers with funds and assets that are clean and untainted by criminality depends, in large part, upon the Island's reputation as a sound, well-regulated jurisdiction. Any business that assists in *money laundering*, the *financing of terrorism*, or *the financing of proliferation*, whether:

   › with knowledge or suspicion of the connection to crime or

   › acting without regard to what it may be facilitating through the provision of its products or services

   › will face the loss of its reputation, risk the loss of its licence or other regulatory sanctions (where regulated and supervised), damage the integrity of Jersey's finance industry as a whole, and may risk prosecution for criminal offences.

2. Jersey has had in place a framework of anti-money laundering legislation since 1988, and for the countering of terrorism since 1990. This legislation has continued to be updated as new threats have emerged, including legislation to extend the definition of criminal conduct for which a money laundering offence can be committed and to combat international terrorism.

3. Criminals are aware the AML/CFT/CPF measures taken by the traditional financial sector over the past decade and may seek other means to convert their proceeds of crime, or to mix them with legitimate income before they enter the banking system, thus making them harder to detect. Lawyers, trust company businesses and providers of accountancy services have all been used as a conduit for criminal property to enter the financial system and are sometimes referred to as "gatekeepers". Some have also been used to assist terrorists and proliferators of weapons of mass destruction to plan and finance their operations.

4. For example, criminals may try to exploit the services offered by lawyers, through the business of undertaking property and financial transactions, setting up corporate and trust structures and when acting as directors or trustees. In addition, client accounts can provide a money launderer with a route into the banking system.

5. The result has been that international money laundering, financing of terrorism, and financing of proliferation legislation and standards have been extended beyond the traditional financial sector to specified schedule 2 businesses. This *AML/CFT/CPF Handbook* applies to all supervised persons (throughout this Handbook, where provisions of the *Money Laundering Order* are quoted, paraphrased or summarised, the text refers to a relevant person to match the language of the *Money Laundering Order*).

6. Jersey's defences against money laundering, the financing of terrorism, and financing of proliferation rely heavily on the vigilance and co-operation of the finance sector. *The Money Laundering Order* is therefore also in place covering supervised persons.

7. The primary legislation on money laundering, the financing of terrorism, and the financing of proliferation is defined in the glossary above as the *Anti-Money Laundering and Counter-Terrorism Legislation*.

8. The international standards require that all Financial Institutions, DNFBPs and virtual asset service providers must be supervised on a risk-based approach by an appropriate anti-money laundering supervisory body. Within Jersey, the JFSC has been designated as the relevant supervisory body under the Supervisory Bodies Law. The JFSC is the AML/CFT/CPF supervisor for all supervised persons. Ensuring compliance and taking action against those that do not comply with the measures to guard against money laundering, the *financing of terrorism*, and the *financing of proliferation*, is crucial to the effectiveness of Jersey's preventative regime.

9. Supervised persons may get a visit from the JFSC to carry out an examination. Further information can be found on the JFSC's website. In certain circumstances, the JFSC may also serve a notice on a supervised person which would require, among other things, senior management to attend interviews and to answer questions and/or provide information and documents.

10. Each supervised person in Jersey must recognise the role that it must play in protecting itself, and its employees, from involvement in money laundering, the *financing of terrorism*, and the *financing of proliferation*, and also in protecting the Island's reputation. This relates not only to business operations within Jersey, but also operations conducted by supervised persons outside the Island.

11. The JFSC strongly believes that the key to the prevention and detection of money laundering, the *financing of terrorism*, and the *financing of proliferation* lies in the implementation of, and strict adherence to, effective systems and controls, including sound CDD measures based on international standards. The AML/CFT/CPF Handbook therefore establishes standards which match international standards issued by the FATF. The Handbook also has regard to the standards promoted by the Basel Committee, IOSCO and the IAIS. The Handbook takes account of the requirements of EU legislation to counter money laundering, the *financing of terrorism*, and the *financing of proliferation* and its application of standards set by the FATF.

12. The JFSC is also mindful of the importance of financial services being generally available to all Jersey residents and, where necessary, the AML/CFT/CPF Handbook incorporates measures to guard against the financial exclusion of Jersey residents from financial services and products.

13. Throughout this Handbook, supervise*d persons* should have regard to the defined terms set out in the Glossary above.

1.1 Objectives of the AML/CFT/CPF Handbook

14. The objectives of the *AML/CFT/CPF Handbook* are:

- to outline the relevant requirements of the Anti-Money Laundering and Counter-Terrorism Legislation
- to set out the JFSC's requirements, expressed as AML/CFT/CPF Codes of Practice - to be followed by all supervised persons
- to assist supervised persons to comply with the requirements of the Anti-Money Laundering and Counter-Terrorism Legislation and the AML/CFT/CPF Codes of Practice, through practical interpretation
- to outline good practice in developing systems and controls to prevent supervised persons from being used to facilitate money laundering, the *financing of terrorism*, and the *financing of proliferation*

- to provide a base from which supervised persons can design and implement systems and controls and tailor their own policies and procedures for the prevention and detection of money laundering, the *financing of terrorism*, and the *financing of proliferation* (and which may also help to highlight identity fraud)
- to ensure that Jersey matches international standards to prevent and detect money laundering, the *financing of terrorism*, and the *financing of proliferation*
- to provide direction on applying the risk-based approach effectively
- to provide more practical guidance on applying CDD measures, including finding out identity and obtaining evidence of identity
- to emphasise the responsibilities of the Board and senior management of a supervised person in preventing and detecting money laundering, the *financing of terrorism*, and the *financing of proliferation*
- to promote the use of a proportionate, risk-based approach to CDD measures, which directs resources towards higher risk customers
- to emphasise the particular money laundering, the *financing of terrorism*, and the *financing of proliferation* risks of certain financial services and products
- to provide an information resource to be used in training and raising awareness of money laundering, the *financing of terrorism*, and the *financing of proliferation*.

15. The *AML/CFT/CPF Handbook* will be reviewed on a regular basis and, where necessary following consultation, amended in light of experience, changes in legislation, and the development of international standards.

16. This Handbook is intended to be used by senior management and compliance staff in the development of a *supervised person's systems and controls*, and detailed *policies and procedures*. Each *supervised person* is expected to draw up its own *policies and procedures* based on the guidance set out in the Handbook. These *policies and procedures* will also help senior management and staff to comply with their own personal obligations under the *Anti-Money Laundering and Counter-Terrorism Legislation*. This Handbook is not intended to be used by *supervised persons* as an internal procedures manual.

17. *Supervised persons* are expected to think about how they might be vulnerable to and exploited by criminals. The *Anti-Money Laundering and Counter-Terrorism Legislation* expects *supervised persons* to manage the risks of being used by criminals, terrorist groups or proliferators of weapons of mass destruction, and to document how they are managing those risks.

18. **All *supervised persons*** should have regard to the main sections of this Handbook (Sections 1-10). S*upervised persons* should also refer to the sector-specific sections of this Handbook (Sections 11-16) relevant to their type of business when drawing up their *policies and procedures*.

1.2 Structure of the AML/CFT/CPF Handbook

19. The *AML/CFT/CPF Handbook* describes *statutory requirements* (defined below), sets out principles and detailed requirements (*AML/CFT/CPF Codes of Practice*), and presents ways of complying with *statutory requirements* and the *AML/CFT/CPF Codes of Practice* (*guidance notes*).

20. *Statutory requirements* describe the statutory provisions that must be complied with by a *supervised person* (natural or legal) when carrying on a supervised *business*, in particular requirements set out in the *Money Laundering Order*. Some *statutory requirements* place obligations on individuals. Failure to follow a *Statutory Requirement* is a criminal offence and may also attract regulatory sanction.

21. The *AML/CFT/CPF Codes of Practice* set out principles and detailed requirements for compliance with *statutory requirements,* failure to follow any *AML/CFT/CPF Codes of Practice* may attract regulatory sanction. The *AML/CFT/CPF Codes of Practice* comprise a number of individual elements:

- to be followed in the area of corporate governance which must be in place in order for a *supervised person* to comply with *statutory requirements* and
- explain in more detail how a *Statutory Requirement* is to be complied with.

22. *Guidance notes* present ways of complying with the *statutory requirements* and *AML/CFT/CPF Codes of Practice* and must always be read in conjunction with these. A *supervised person* may adopt other measures to those set out in the *guidance notes*, including *policies and procedures* established by a group that it is part of, so long as it can demonstrate that such measures also achieve compliance with the *statutory requirements* and *AML/CFT/CPF Codes of Practice*. This allows a *supervised person* discretion as to how to apply requirements in the particular circumstances of its business, products, services, transactions and *customers*. The soundly reasoned application of the provisions contained within the *guidance notes* will provide a good indication that a *supervised person* is in compliance with the s*tatutory requirements* and *AML/CFT/CPF Codes of Practice*.

23. The provisions of the *statutory requirements* and of the *AML/CFT/CPF Codes of Practice* are described using the term **must**, indicating that these requirements are mandatory. However, in exceptional circumstances, where strict adherence to any of the *AML/CFT/CPF Codes of Practice* would produce an anomalous result, a *supervised person* may apply in advance in writing to the *JFSC* for a variance from the requirement. Section 1.8 also explains that an obligation to do something outside Jersey may be met through applying measures that are at least equivalent to the *AML/CFT/CPF Codes of Practice*.

24. In contrast, the *guidance notes* use the term **may**, indicating ways in which the requirements may be satisfied, but allowing for alternative means of meeting the *statutory requirements* or *AML/CFT/CPF Codes of Practice*..

25. This Handbook also contains **Overview** text which provides context relevant to particular sections or sub-sections of the *AML/CFT/CPF Handbook*.

26. The *AML/CFT/CPF Handbook* is not intended to provide an exhaustive list of *systems and controls* to counter *money laundering*, the *financing of terrorism*, and the *financing of proliferation*. In complying with the *statutory requirements* and *AML/CFT/CPF Codes of Practice*, and in applying the *guidance notes*, a *supervised person* should (where permitted) adopt an appropriate risk-based approach and should always consider what additional measures might be necessary to prevent its exploitation, and that of its products and services, by persons seeking to engage in *money laundering*, the *financing of terrorism*, and the *financing of proliferation*.

27. The text in *statutory requirements* sections necessarily paraphrases provisions contained in the *Anti-Money Laundering and Counter-Terrorism Legislation* and should always be read and understood in conjunction with the full text of each law. *Statutory requirements* are presented in light blue boxes and in italics, to distinguish them from other text.

1.3 Legal Status and Sanctions for Non-Compliance

1.3.1 AML/CFT/CPF Handbook

28. The *AML/CFT/CPF Handbook* is issued by the *JFSC*:

- pursuant to its powers under Article 8 of the *Commission Law*
- in accordance with Article 22 of the *Supervisory Bodies Law*, which provides for *Codes of Practice* to be prepared and issued for the purpose of setting out principles and detailed requirements
- in light of Article 37(1)(a) of the *Proceeds of Crime Law*, which provides for the *Money Laundering Order* which prescribes measures to be taken (or not to be taken) by persons who carry on *financial services business*.

29. The *AML/CFT/CPF Codes of Practice* in this Handbook are applicable to **all *supervised persons*.**

30. Sector-specific sections for *supervised Persons* subject to the *Wire Transfers Regulations*, *Trust Company Business*, Funds and Fund Operators, Estate Agents and High Value Dealers, Lawyers and Accountants are set out at Sections 11-16 of this Handbook and provide some additional *AML/CFT/CPF Codes of Practice* and *guidance notes* for *supervised persons* carrying on those types of business.

1.3.2 Money Laundering Order

31. The *Money Laundering Order* is made by the Minister for External Relations and Financial Services under Article 37(1)(a) of the *Proceeds of Crime Law*. The Order prescribes measures to be taken (including measures not to be taken) by a *relevant person* for the purposes of preventing and detecting *money laundering* and the *financing of terrorism and proliferation*.

32. Failure to comply with the *Money Laundering Order* is a criminal offence under Article 37(4) of the *Proceeds of Crime Law*. In determining whether a *supervised person* has complied with any of the requirements of the *Money Laundering Order*, the Royal Court is, pursuant to Article 37(8) of the *Proceeds of Crime Law*, required to take account of the *AML/CFT/CPF Code of Practice* and *guidance notes* issued by the *JFSC*, as amended from time to time.

33. The sanction for failing to comply with the *Money Laundering Order* may be an unlimited fine or up to two years imprisonment, or both.

34. Under Article 39A(2) of the *Proceeds of Crime Law*, if a 'relevant offence' is proved to have been committed by a financial services business with the consent or connivance of a 'relevant person' (both as defined in Article 39A(1) of that law) that 'relevant person' is also guilty of the offence and liable to the same penalty for that offence as the financial services business.

35. Under Article 35A of the *Proceeds of Crime Law*, a *financial services business* commits an offence if a person is engaged in money laundering when acting in the capacity of a person associated with that business (as defined in Article 35A(4) of that Law).

36. If the *financial services business* is a body corporate, it is liable to a fine. If the business is not a body corporate, they are liable to imprisonment for a term not exceeding 2 years or to a fine or to both.

37. In determining whether a person has committed an offence under Article 21 of the *Terrorism Law* (the offence of failing to report), the Royal Court is, pursuant to Article 21(6) of the *Terrorism Law*, required to take account of the of any guidance provided (for this purpose guidance will include the *AML/CFT/CPF Code of Practice* read in conjunction with Overview text and the *guidance notes*), as amended from time to time. The sanction for failing to comply with Article 21 of the *Terrorism Law* may be an unlimited fine or up to five years imprisonment, or both.

38. It should be emphasised that the *AML/CFT/CPF Handbook* is not a substitute for the law and compliance with it is not of itself a defence to offences under the various legislation referenced above. However, the *Handbook shall be taken into account by* the courts when considering the standards of a *supervised person's* conduct and whether they acted reasonably, honestly, and appropriately, and took all reasonable steps and exercised necessary due diligence to avoid committing the offence.

39. Under Article 21A of the *Commission Law* the *JFSC* may impose a civil financial penalty on a *supervised person* (except where that person is a fund) where the *JFSC* is satisfied that the *supervised person* has, to a significant and material extent, contravened the *Money Laundering Order*.

40. Article 21A of the *Commission Law* also permits the *JFSC* to impose a civil financial penalty on a principal person, a key person or a person who performs or performed a senior management function (all as defined in Article 1 of the *Commission Law*) where the *JFSC* is satisfied that the contravention of the *Money Laundering Order* by the *supervised person* was:

- committed with the consent or connivance of, or is attributable to neglect on the part of, the principal person, key person or the person who performs or performed a senior management function or
- aided, abetted, counselled or procured by such a person.

1.3.3 AML/CFT/CPF Codes of Practice

41. An *AML/CFT/CPF Code of Practice* is prepared and issued by the *JFSC* under Article 22 of the *Supervisory Bodies Law*. The *AML/CFT/CPF Codes of Practice* set out the principles and detailed requirements that must be complied with in order to meet certain statutory provisions of the *Supervisory Bodies Law* and the *anti-money laundering and counter-terrorism legislation (Proceeds of Crime Law*, *Terrorism Law*, *Directions Law*, *Targeted Financial Sanctions Measures*, *Wire Transfers Regulations*, and the *Money Laundering Order)* by *supervised persons*. The *AML/CFT/CPF Codes of Practice* comprise a number of individual AML/CFT/CPF Codes of Practice.

42. Article 5 of the *Supervisory Bodies Law* states that the *JFSC* shall be the supervisory body to exercise supervisory functions in respect of a *regulated person (*as defined Article 1 of the *Supervisory Bodies* Law). The *JFSC* is also designated under Article 6 of the *Supervisory Bodies Law* to exercise supervisory functions in respect of any other person carrying on a *specified Schedule 2 business*. The effect of these provisions is to give the *JFSC* supervisory functions in respect of all *supervised persons*.

43. Article 8A of the *Supervisory Bodies Law* requires a supervisory body (the *JFSC*) to use a risk-based approach when performing its obligations under said law, which means determining the scrutiny that a *supervised person* requires on the basis of:

- the *money laundering* and *terrorist financing* risks associated with the *supervised person*, as identified by the supervisory body's assessment of the *supervised person's* risk profile

- the policies, internal controls and procedures associated with the *supervised person*, as identified by the supervisory body's assessment of the *supervised person's* risk profile
- the *money laundering* or *terrorist financing* risks present in the jurisdiction in which the *supervised person* is based
- any other characteristic of the *supervised person* that the supervisory body reasonably considers to be relevant.

44. Article 8A(3) requires the supervisory body (the *JFSC*) to take account of *FATF* standards when devising a risk profile for a *supervised person*.

45. Compliance with the *AML/CFT/CPF Codes of Practice* will be considered by the *JFSC* in the conduct of its supervisory programme, including on-site examinations.

46. The consequences of non-compliance with any *AML/CFT/CPF Codes of Practice* could include an investigation by or on behalf of the *JFSC* and the imposition of regulatory sanctions. Regulatory sanctions available to the JFSC under the *Supervisory Bodies Law* and the *Regulatory Laws* (where applicable) include:

- issuing a public statement
- imposing a registration condition
- objecting to the appointment, or continued appointment, of a principal person (or equivalent controller or manager of a *regulated person*) or key person
- imposing a direction and making this public, including preventing an individual from working in a *supervised person* and where already appointed requiring their removal and
- revoking a supervised person's registration.

47. In addition, under Article 21A of the *Commission Law* the *JFSC* may impose a civil financial penalty on a *supervised person* (except where that person is a fund) where the *JFSC* is satisfied that the *supervised person* has, to a significant and material extent, contravened an *AML/CFT/CPF Code of Practice*.

48. Article 21A of the *Commission Law* also permits the *JFSC* to impose a civil financial penalty on a principal person, a key person or a person who performs or performed a senior management function (all as defined in Article 1 of the *Commission Law*) where the *JFSC* is satisfied that the contravention of the *AML/CFT/CPF Code of Practice* by the *supervised person* was:

- committed with the consent or connivance of, or is attributable to neglect on the part of, the principal person, key person or the person who performs or performed a senior management function; or
- aided, abetted, counselled or procured by such a person.

49. The ability of a *supervised person* to demonstrate compliance with *AML/CFT/CPF Codes of Practice* will also be directly relevant to its regulated status and any assessment of fitness and propriety of its *principal persons* and *key persons*. Non-compliance with any *AML/CFT/CPF Code of Practice* may be regarded by the *JFSC* as an indication of:

- a lack of fitness and propriety under Articles 7 or 8B of the *CIF(J) Law*, Article 10 of the *BB(J) Law*, Article 7 of the *IB(J) Law*, and Article 9 of the *FS(J) Law* and/or

› a failure to follow certain fundamental principles within a Code of Practice issued under each of the *regulatory laws*.

50. Where a breach of an *AML/CFT/CPF Code of Practice* results in contravention of the *Money Laundering Order*, a *supervised person* and its employees can be criminally prosecuted.

1.4 Jurisdictional Scope of the Money Laundering Order and AML/CFT/CPF Codes

1.4.1 Application of the Money Laundering Order and AML/CFT/CPF Codes of Practice to *supervised persons* carrying on business in Jersey

51. By virtue of the definition of *relevant person* in Article 1(1), the *Money Laundering Order* applies to **any *supervised person*** who is carrying on a *supervised business* in or from within Jersey. This will include Jersey-based branches of companies incorporated outside Jersey conducting *supervised* business in Jersey.

52. By virtue of Articles 5, 6 and 22 of the Supervisory Bodies Law, the AML/CFT/CPF Codes of Practice apply to **any supervised person** who is carrying on a supervised business in or from within Jersey. This will include Jersey-based branches of companies incorporated outside Jersey conducting supervised business in Jersey.

53. The *AML/CFT/CPF Codes of Practice* in Sections 2 to 10 of this Handbook must be complied with by **all *supervised persons***. The sector-specific sections within this Handbook only provide additional *AML/CFT/CPF Codes of Practice* for particular business types in very limited circumstances.

1.4.2 Application of the Money Laundering Order to *supervised persons* carrying on business outside Jersey (overseas)

54. Article 10A of the *Money Laundering Order* explains and regulates the application of the *Money Laundering Order* to *supervised business* carried on outside Jersey.

55. Article 10A(2)(a) of the *Money Laundering Order* explains that a Jersey body corporate or other legal person registered in Jersey (*supervised person*) that carries on a *supervised business* through an overseas branch must comply with the *Money Laundering Order* in respect of that business, irrespective of whether it also carries on *supervised business* in or from within Jersey.

56. However, Article 10A(9) of the *Money Laundering Order* explains that a *supervised person* carrying on any of the business activities described in paragraphs 1-5 of Part B of Schedule 2 to the *Proceeds of Crime Law* need not comply with paragraphs (2), (3) and (4) in a country or territory outside Jersey in respect of their *Schedule 2 business*.

57. Notwithstanding the above paragraph, all of the provisions of the *Money Laundering Order* apply to a *supervised person* that is a **legal person** carrying on *supervised business* anywhere in the world. However, in practice this may not apply to all *supervised persons* carrying on *Schedule 2 business* on the basis that some businesses currently registered under the *Supervisory Bodies Law* are either sole practitioners or Jersey customary law partnerships.

58. Article 10A(3) of the *Money Laundering Order* requires a *supervised person* (subject to Article 10A(9) see above) who: (i) is registered, incorporated or otherwise established under Jersey law, but who is not a legal person; and (ii) carries on a *supervised business* in or from within Jersey, to apply measures that are at least equivalent to the requirements of the *Money Laundering Order* in respect of any *supervised business* carried on by that person through an overseas branch. This requirement will apply to a limited partnerships registered under the Limited Partnerships (Jersey) Law 1994 and general partnership established under Jersey customary law.

    Note that the term "registered, incorporated or otherwise established" in Article 10A(5) of the Money Laundering Order is intended to be understood only to refer to the creation of a legal arrangement. In particular, it is not intended that "registered" be understood in the more general sense of registering under commercial or other legislation, or that "established" be understood in the more general sense of establishing a branch or representative office.

59. Article 10A(2)(b) of the *Money Laundering Order* requires a Jersey body corporate or other legal person (*supervised person*) registered in Jersey (subject to Article 10A(9) see above) to ensure that any legal person that is majority owned or controlled by that person (referred to in the *Money Laundering Order* as a "subsidiary") applies measures that are at least equivalent to the requirements of the *Money Laundering Order* in respect of any *supervised business* carried on outside Jersey by that subsidiary.

60. Article 10A(4) of the *Money Laundering Order* requires a *supervised person* (subject to Article 10A(9) see above) who: (i) is registered, incorporated or otherwise established under Jersey law, but who is not a legal person; and (ii) carries on a *supervised business* in or from within Jersey, to ensure that any subsidiary applies measures that are at least equivalent to the requirements of the *Money Laundering Order* in respect of any *supervised business* carried on outside Jersey by that subsidiary. This requirement will apply to a limited partnership registered under the Limited Partnerships (Jersey) Law 1994 and general partnership established under Jersey customary law.

61. In summary, Jersey companies and other legal persons registered in Jersey (subject to Article 10A(9) see above) are covered by Article 10A(2) in relation to their overseas branches and subsidiaries. Other types of entity who do not have legal personality but who are constituted under Jersey law fall into Article 10A(3) and (4) in relation to their overseas branches and subsidiaries.

62. Article 10A(6) of the *Money Laundering Order* requires a *supervised person* (subject to Article 10A(9) see above) to take reasonable steps to comply with paragraphs (2), (3) and (4) to the extent that the law of the country or territory in which that person carries on a *supervised business*, or has a subsidiary carrying on such a business, does not have the effect of prohibiting or preventing the *supervised person* from taking such steps. If the *supervised person* does not comply with paragraphs (2), (3) and (4), the following steps must be taken by the *supervised* person: (i) the *JFSC* must be informed that this is the case; (ii) other reasonable steps to deal effectively with the risk of *money laundering* and the *financing of terrorism* must be taken.

63. If a *supervised person* carries on a *supervised business* or has a subsidiary carrying on such a business overseas that has more stringent requirements than those set out in the *Money Laundering Order*, Article 10A(10) of the *Money Laundering Order* requires that the *supervised person* ensure that the more stringent requirements are complied with.

1.4.3 Application of AML/CFT/CPF Codes of Practice to *supervised persons* carrying on business outside Jersey (overseas)

64. By virtue of Articles 5, 6 and 22 of the *Supervisory Bodies Law*, a *supervised person* (subject to Article 10A(9) see above) that is a company incorporated in Jersey that carries on a *supervised business* through an overseas branch must comply with the *AML/CFT/CPF Code of Practice* in respect of that business, irrespective of whether it also carries on *supervised business* in or from within Jersey.

65. By concession, measures that are at least equivalent to *AML/CFT/CPF Codes of Practice* may be applied as an alternative to complying with the *AML/CFT/CPF Codes of Practice*.

66. A *supervised person* (subject to Article 10A(9) see above) who (i) is registered, incorporated or otherwise established under Jersey law, but who is not a Jersey incorporated company; and (ii) carries on a *supervised business* in or from within Jersey, must apply measures that are at least equivalent to *AML/CFT/CPF Codes of Practice* in respect of any *supervised business* carried on by that person through an overseas branch. This requirement will apply to a foundation or partnership established under Jersey law.

    Note that the term "registered, incorporated or otherwise established" is intended to be understood only to refer to the creation of a legal person or legal arrangement.

67. A *supervised person* (subject to Article 10A(9) see above) that is a Jersey incorporated company must ensure that any subsidiary applies measures that are at least equivalent to *AML/CFT/CPF Codes of Practice* in respect of any *supervised business* carried on outside Jersey by that subsidiary.

68. A *supervised person* (subject to Article 10A(9) see above) who (i) is registered, incorporated or otherwise established under Jersey law, but who is not a Jersey incorporated company; and (ii) carries on a *supervised business* in or from within Jersey, must ensure that any subsidiary applies measures that are at least equivalent to *AML/CFT/CPF Codes of Practice* in respect of any *supervised business* carried on outside Jersey by that subsidiary. This requirement will apply to a foundation or partnership established under Jersey law.

69. Where overseas provisions prohibit compliance with one or more of the *AML/CFT/CPF Codes of Practice* (or measures that are at least equivalent), the requirements do not apply and the *JFSC* must be informed that this is the case. In such circumstances, the *AML/CFT/CPF Codes of Practice* require a *supervised person* to take other reasonable steps to effectively deal with the risk of *money laundering*, the *financing of terrorism*, and the *financing of proliferation*.

1.5 Definition of Supervised Business

70. S*upervised business* is defined in Article 1 of the *Supervisory Bodies Law*. This reflects the definition of *financial services business* as provided by Article 36 of the *Proceeds of Crime Law* (which in turn refers to Schedule 2 of the *Proceeds of Crime Law)*.

71. In practice, this means that all activities listed in Schedule 2 of the *Proceeds of Crime Law* are covered by the term *supervised business*.

72. The sector specific sections of this Handbook (sections 11 – 16) include specific information regarding the activities of *supervised persons* that are: Estate Agents, High Value Dealers, Lawyers, Accountants, Trust Company Businesses, and Funds and Fund Operators.

1.6 Business relationships and one-off transactions

73. The terms *business relationship* and *one-off transaction* are defined in the Glossary above.

Guidance notes

74. A *supervised person* may demonstrate that the basis upon which it has determined the value of a transaction for the purposes of Article 4 of the *Money Laundering Order* (e.g. in order to determine whether a transaction falls within the definition of a *one-off transaction* described in that article) is appropriate where it applies the value of the underlying asset(s) to which the instruction relates. For example, with regard to services provided in respect of a trust, a *supervised person* may apply the value of the trust assets.

75. Where a value to the underlying assets cannot be determined or no value for the underlying assets is readily available or ascertainable, the *supervised person* should assume the value of the transaction to be 15,000 euro or more. Please note the lower thresholds for money service business, virtual currency exchange business or operating a casino

76. With reference to the above paragraph, persons carrying on money services business, virtual currency exchange business or operating a casino should apply their specific transaction thresholds set out in Article 4 of the *Money Laundering Order*.

77. Further sector-specific guidance on determining the value of transactions is provided, where appropriate, in the relevant sector-specific sections.

78. Where a transaction is likely to become a *one-off transaction* or develop into a *business relationship*, the *supervised person* should consider undertaking identification measures at the outset.

79. Where the *supervised person* suspects *money laundering* or the *financing of terrorism* whilst undertaking the above, they should refer to Section 8 of this Handbook.

1.7 Risk-based approach

Overview

80. To assist the overall objective of detecting and preventing *money laundering*, the *financing of terrorism*, and the *financing of proliferation*, the *AML/CFT/CPF Handbook* adopts a risk-based approach. Such an approach:

- recognises that the *money laundering*, *financing of terrorism*, and *financing of proliferation* threat to a *supervised person* varies across *customers*, countries and territories, products and delivery channels
- allows a *supervised person* to differentiate between *customers* in a way that matches risk in a particular *supervised person*
- while establishing minimum standards, allows a *supervised person* to apply its own approach to *systems and controls*, and arrangements in particular circumstances
- helps to produce a more cost effective system.

81. A risk-based approach requires steps to be taken to identify how a *supervised person* could be used for *money laundering*, the *financing of terrorism*, or the *financing of proliferation* and establishing the most effective and proportionate way to manage and mitigate the risks in the same way as for all business risks faced by a *supervised person*.

82. The possibility of being used to assist with *money laundering,* the *financing of terrorism*, and the *financing of proliferation* poses many risks for *supervised persons* including:

- criminal and disciplinary sanctions for the *supervised person* and for *key* and *principal persons*

- civil action against the *supervised person* as a whole and against individual staff
- damage to reputation leading to loss of business.

83. *Systems and controls* will not detect and prevent all *money laundering*, *terrorist financing,* or *proliferation financing* activity. A risk-based approach will, however, serve to balance the cost burden placed on a *supervised person* and on its *customers* with a realistic assessment of the threat of it being used in connection with *money laundering,* the *financing of terrorism,* or the *financing of proliferation* by focusing effort where it is needed and has most impact.

84. How a risk-based approach is applied will also depend on the structure of the *supervised person's* business, its size and the nature of its products and services.

85. The *policies and procedures* put in place should be proportionate to the size of the business and the identified risks.

86. *Policies and procedures* may be more straightforward for smaller businesses. Such businesses may offer a smaller range of products or services, with most *customers* falling into similar categories. In these circumstances, a simpler approach may be appropriate for most *customers*, with the focus being on those *customers* that fall outside the usual categories. Larger businesses with a small range of products or services can put standard *AML/CFT/CPF policies and procedures* in place based on generic profiles of *customers*.

87. In more complex business relationships, risk assessment, mitigation, and ongoing monitoring will be more sophisticated and will take into account additional information held and knowledge of the *customer's* business activities.

88. An effective and documented risk-based approach will enable a *supervised person* to justify its position on managing *money laundering,* the *financing of terrorism*, and the *financing of proliferation* risks to law enforcement, the courts, regulators and supervisory bodies.

1.8 Equivalence of requirements in other countries and territories

1.8.1 Equivalent business

89. Articles 16 and Part 3A of the *Money Laundering Order* respectively permit reliance to be placed on an *obliged person* and exemptions from *CDD* requirements to be applied to a *customer* carrying on a *supervised business* that is overseen for *AML/CFT/CPF* compliance in Jersey or carrying on business that is *equivalent business*. Sections dealing with the acquisition of a business or block of *customers* and verification of identity also provide concessions from *AML/CFT/CPF Codes of Practice* on a similar basis.

90. *Equivalent business* is defined in Article 5 of the *Money Laundering Order*.

91. The condition set out in Article 5 requiring that the business must be subject to requirements to combat *money laundering,* and the *financing of terrorism* consistent with those in the *FATF Recommendations* will be satisfied, **among other things**, where a person is located in an equivalent country or territory.

1.8.2 Equivalent countries and territories

92. With effect from 31 May 2021 the *JFSC* no longer maintains a list of Equivalent Countries and Territories within this Handbook. Guidance to assist *supervised persons* to determine equivalence is set out in Section 1.8.3 below.

93. A country or territory may be considered to be equivalent where:

    a. Financial institutions and *DNFBPs* are required to take measures to detect and prevent *money laundering,* the *financing of terrorism*, and the *financing of proliferation* that are consistent with those in the *FATF Recommendations*

    b. Financial institutions and *DNFBPs* are supervised for compliance with those requirements by a regulatory or supervisory authority.

1.8.3 Determining equivalence

94. Requirements for measures to be taken by an *obliged person* or *customer* will be considered to be consistent with the *FATF Recommendations* only where those requirements are established by law, regulation, or other enforceable means.

95. In determining whether or not the requirements for measures to be taken in a country or territory are consistent with the *FATF Recommendations*, a *supervised person* should have regard for the following:

- generally - whether or not the country or territory is a member of the *FATF*, a member of a *FATF* Style Regional Body (**FSRB**) or subject to its assessment and follow-up process, a Member State of the *EU*, or a member of the *EEA*

- specifically - whether a country or territory is compliant or largely compliant with those *FATF Recommendations* that are directly relevant to the application of available concessions. These are Recommendations 10-13, 15-21 and 26. Where a person with a specific connection to a *customer* is a *DNFBP* (a term that is defined by the *FATF*), then Recommendations 22, 23 and 28 will be relevant

- specifically – the extent to which a country or territory is achieving the Immediate Outcomes that are directly relevant to the application of available concessions, namely whether Immediate Outcomes 3 and 4 are assessed at a high or substantial level of effectiveness.

- the following sources may be used to determine whether a country or territory is compliant or largely compliant or achieving the Immediate Outcomes:

    a) the laws and instruments that set requirements in place in that country or territory

    b) recent independent assessments of that country's or territory's framework to combat *money laundering,* the *financing of terrorism*, and the *financing of proliferation*, such as those conducted by the *FATF*, FSRBs, the *IMF* and the World Bank (and published remediation plans)

    c) other publicly available information concerning the effectiveness of a country's or territory's framework.

96. Where a *supervised person* assesses whether a country or territory is an equivalent country or territory, the *supervised person* must conduct an assessment process comparable to that described above, and must be able to demonstrate on request the process undertaken and the basis for its conclusion.

97. Links to potential sources of additional information are included in Appendix B. These are not intended to be exhaustive, nor are they placed in any order of priority. Independent research and judgement will be expected in order to cater for the requirements in the individual case.

2 CORPORATE GOVERNANCE

2.1 Overview of section

1. Corporate governance is the system by which enterprises are directed and controlled and their risks managed. For supervised persons, money laundering, the *financing of terrorism*, and the *financing of proliferation* are risks that must be managed in the same way as other business risks.
2. Under the general heading of corporate governance, this section considers:
   - › board responsibilities for the prevention and detection of *money laundering,* the countering of *terrorist financing*, and the countering of *proliferation financing*
   - › requirements for systems and controls, training and awareness
   - › the appointment of a ***MLCO*** and ***MLRO***.
3. The *AML/CFT/CPF Handbook* describes a *supervised person's* general framework to combat *money laundering,* the *financing of terrorism*, and the *financing of proliferation* as its *systems and controls*. The *Handbook* refers to the way in which those systems and controls are implemented into the day-to-day operation of a *supervised person* as its *policies and procedures*.
4. Where a *supervised person* is not a company but is, for example, a partnership, references in this section to "the Board" should be read as meaning the senior management function of that person, including the Board of a legal arrangement's governing body. In the case of a *sole trader*, "the Board" will be the *sole trader*. In the case of an overseas company carrying on a *supervised business* in Jersey through a branch, "the Board" should be read as including the local management function of that branch in Jersey.

2.2 Measures to prevent money laundering, the financing of terrorism, and the financing of proliferation

Statutory requirements (paraphrased wording)

5. *In accordance with Article 37 of the Proceeds of Crime Law, a relevant person must take prescribed measures to prevent and detect money laundering and the financing of terrorism. Failure to take such measures is a criminal offence and, where such an offence is proved to have been committed with the consent or connivance of, or to be attributable to neglect on the part of, a director or manager or officer of the relevant person, they too shall be deemed to have committed a criminal offence.*
6. *Article 37 enables the Minister for External Relations and Financial Services to prescribe by Order the measures that must be taken (including measures not to be taken) by a relevant person. These measures are established in the Money Laundering Order.*

2.3 Board responsibilities

Overview

7. The key responsibilities of the Board, set out in further detail below, are to:
   - › identify the supervised person's money laundering, the financing of terrorism, and the financing of proliferation risks

- ensure that its systems and controls are appropriately designed and implemented to manage those risks, and
- ensure that sufficient resources are devoted to fulfilling these responsibilities.

8. The Board is assisted in fulfilling these responsibilities by a *MLCO* and *MLRO*. Larger or more complex *supervised persons* may also require dedicated risk and internal audit functions to assist in the assessment and management of *money laundering,* the *financing of terrorism*, and the *financing of proliferation* risk.

Statutory requirements (paraphrased wording)

9. *Article 11(1) of the Money Laundering Order requires a relevant person to establish and maintain appropriate and consistent policies and procedures in respect of the person's financial services business, and financial services business carried on by a subsidiary, in order to prevent and detect money laundering and the financing of terrorism.*
10. *Article 11(11) of the Money Laundering Order requires a relevant person to establish and maintain adequate procedures for monitoring compliance with, and testing the effectiveness of: (i) its policies and procedures; (ii) its measures to promote AML/CFT awareness; and (iii) its training of relevant employees (see Section 9 of this Handbook).*
11. *Articles 7 and 8 of the Money Laundering Order require that a relevant person appoints a MLCO and a MLRO.*

AML/CFT/CPF Codes of Practice

12. The Board must conduct and record a business risk assessment in respect of the *supervised person*. In particular, the Board must consider, on an on-going basis, the *supervised person's* risk appetite and the extent of the *supervised person's* exposure to *money laundering,* the *financing of terrorism*, and the *financing of proliferation* risks "in the round" or as a whole by reference to the *supervised person's* organisational structure, *customers*, the countries and territories with which those *customers* are connected, the products and services the *supervised person* provides and how those products and services are delivered. The assessment must consider the cumulative effect of risks identified, which may exceed the sum of each individual risk element. The Board's assessment must be kept up to date. (See Section 2.3.1).
13. On the basis of its business risk assessment, the Board must establish a formal strategy to counter *money laundering,* the *financing of terrorism*, and the *financing of proliferation*. Where a *supervised person* forms part of a group operating outside the Island, that strategy may protect both its global reputation and its Jersey business.
14. Taking into account the conclusions of the business risk assessment and strategy, the Board must:
    - organise and control its affairs in a way that effectively mitigates the risks that it has identified, including areas that are complex; and
    - be able to demonstrate the existence of adequate and effective systems and controls (including policies and procedures) to counter *money laundering*, the *financing of terrorism*, and the *financing of proliferation* (see Section 2.4).

15. The Board must document its *systems and controls* (including *policies and procedures*) and clearly apportion responsibilities for countering *money laundering*, the *financing of terrorism*, and the *financing of proliferation*, and, in particular, responsibilities of the *MLCO* and *MLRO* (see Sections 2.5 and 2.6).
16. The Board must assess both the effectiveness of, and compliance with, *systems and controls* (including *policies and procedures*) and take prompt action necessary to address any deficiencies. (See Sections 2.4.1 and 2.4.2).
17. The Board must consider what barriers (including cultural barriers) exist to prevent the operation of effective *systems and controls* (including *policies and procedures*) to counter *money laundering*, the *financing of terrorism,* and the *financing of proliferation*, and must take effective measures to address them. (See Section 2.4.3).
18. The Board must notify the *JFSC* immediately in writing of any material failures to comply with the requirements of the Money Laundering Order or the *AML/CFT/CPF Handbook*.

2.3.1 Business risk assessment

AML/CFT/CPF Codes of Practice

19. A *supervised person* must maintain appropriate *policies and procedures* to enable it, when requested by the *JFSC*, to make available to that authority a copy of its BRA.

Guidance notes

20. A *supervised person* may extend its existing risk management systems to address *AML/CFT/CPF* risks. The detail and sophistication of these systems will depend on the *supervised person's* size and the complexity of the business it undertakes. Ways of incorporating a *supervised person's* BRA will be governed by the size of the *supervised person* and how regularly compliance staff and the Board are involved in day-to-day activities.
21. The Board of a *supervised person* may demonstrate that it has considered its exposure to *money laundering,* the *financing of terrorism,* and the *financing of proliferation* risk by:

    - involving all members of the Board in determining the risks posed by *money laundering*, the *financing of terrorism,* and the *financing of proliferation* within those areas for which they have responsibility
    - considering organisational factors that may increase the level of exposure to the risk of *money laundering*, the *financing of terrorism,* and the *financing of proliferation*, e.g. outsourced aspects of regulated activities or compliance functions
    - considering the nature, scale and complexity of its business, the diversity of its operations (including geographical diversity), the volume and size of its transactions, and the degree of risk associated with each area of its operation
    - considering who its customers are and what they do
    - considering whether any additional risks are posed by the countries and territories with which its customers are connected. Factors such as high levels of organised crime, increased vulnerabilities to corruption and inadequate frameworks to prevent and detect money laundering *the financing of terrorism, and the financing of proliferation* will impact the risk posed by relationships connected with such countries and territories

- considering the characteristics of the products and services that it offers and assessing the associated vulnerabilities posed by each product and service. For example:

  a. products that allow a *customer* to "pool" third party funds will tend to be more vulnerable - because of the anonymity provided by the co-mingling of assets or funds belonging to several third parties by the *customer*

  b. products such as standard current accounts are more vulnerable because they allow payments to be made to and from external parties, including cash transactions

  c. conversely, those products that do not permit external party transfers or where redemption is permitted only to an account from which the investment is funded will be less vulnerable

- considering the risk that is involved in placing reliance on *obliged persons* to apply *reliance identification measures*

- considering how it establishes and delivers products and services to its *customers*. For example, risks are likely to be greater where relationships may be established remotely (non-face to face), or may be controlled remotely by the *customer* (straight-through processing of transactions)

- considering the accumulation of risk for more complex *customers*.

22. When conducting a business risk assessment care should be taken not to focus too much on any single factor. All factors (including those identified by a National Risk Assessment or similar), as well as the wider picture (and cumulative risk) should be considered.

23. A generic example of how risk might be calculated in a BRA is set out below. Please note this methodology is for illustrational purposes only. It should not be construed as the JFSC taking a position on how risk should be calculated and represented in a BRA. Each BRA should uniquely consider and represent the risks and controls identified by the supervised person:

Impact (implications of event)	**Likelihood (of event happening)**	**Inherent Risk (Impact x Likelihood)**	**Impact and Likelihood after controls applied**	**Residual Risk (Impact x Likelihood after controls applied)**
3 – Significant impact on business	3 – Very likely	9 – High inherent risk	Each rating may range from 1-3	Possible scores: 1-9
2 – Moderate impact on business	2 – Moderately likely	4 – Moderate inherent risk	Each rating may range from 1-3	Possible scores: 1-9
1 – Minimal impact on business	1 – Unlikely to happen	1 – Low inherent risk	Each rating may range from 1-3	Possible scores: 1-9

24. A generic example of a BRA is set out below. Please note the descriptions and scores assigned to these risks are for illustrational purposes only. They should not be construed as the JFSC taking a position on how these risks should be scored and/or controlled. Each BRA should uniquely consider and represent the risks and controls identified by the supervised person:

Risk descriptor	**Impact**	**Likelihood**	**Inherent Risk**	**Controls applied**	**Residual Risk**
Customer is involved in evasion of sanctions relating to financing of proliferation	3 (Reputational damage, potential legal/regulatory sanctions)	2	6	Business will not engage with customers involved in shipping or have connections to Iran or DPRK. Reduces likelihood to 1.	3 x 1 = 3
Pandemic requiring national lockdown	3 (Business unable to operate)	1	3	All staff able to work remotely. All customer transactions can be undertaken electronically. Reduces impact to 1.	1 x 1 = 1
Breach of Money Laundering Order	3 (Reputational damage, potential legal/regulatory sanctions)	2	6	Staff receive training at on-boarding, and regularly thereafter. Staff are required to comply with policies and procedures. Breaches are recorded and considered at Board meetings. Consideration includes trends analysis, lessons learned, training needs and strengthening controls. Reduces likelihood to 1.	3 x 1 = 3

25. In developing a risk-based approach, *supervised persons* need to ensure that the BRA can be understood by the Board, other *relevant employees* and relevant third parties e.g. *auditors* and the *JFSC*.

26. In the case of a *supervised person* that is dynamic and growing, the Board may demonstrate that its BRA is kept up-to-date where it is reviewed annually. In some other cases, this may be too often, e.g. a *supervised person* with a stable customer base, products, and services. In all cases, the Board may demonstrate that its BRA is kept up-to-date where it is reviewed when events (internal and external) occur that may materially change *money laundering, terrorist financing,* and *proliferation financing* risk.
27. It may be beneficial for money laundering, financing of terrorism, and financing of proliferation risks and controls to each be considered separately.
28. Where a *supervised person* is subject to a regulatory code of practice (such as the Trust Company Business Code of Practice) there is also an obligation for a wider, operational business risk assessment to be conducted. When preparing an *AML/CFT/CPF* BRA or *customer* risk assessment, factors in this operational BRA may be relevant. Therefore, a combined *AML/CFT/CPF* and operational BRA may be appropriate.
29. Risks that are not normally considered to be specific *AML/CFT/CPF* risks may also be relevant to an *AML/CFT/CPF* BRA, such for example, credit risk, tax risk, investor eligibility risk, cyber security etc.
30. It is likely that the BRA will be conducted by the *supervised person* prior to any *customer* risk assessment. When *a customer* risk assessment is prepared the BRA may need to be updated (for example, to take into account new risk factors or the *supervised person's* changing risk tolerance/appetite).

2.4 Adequate and effective systems and controls

Overview

31. For *systems and controls* (including *policies and procedures*) to be adequate and effective in preventing and detecting *money laundering*, countering the *financing of terrorism,* and countering the *financing of proliferation*, they will need to be appropriate to the circumstances of the *supervised person*.

Statutory requirements (paraphrased wording)

32. *Article 11(1) of the Money Laundering Order requires a relevant person to establish and maintain appropriate and consistent policies and procedures in respect of the person's financial services business, and financial services business carried on by a subsidiary, in order to prevent and detect money laundering and the financing of terrorism.*
33. *Parts 3, 3A, 4 and 5 of the Money Laundering Order set out the measures that are to be applied in respect of CDD, record-keeping and reporting.*
34. *Article 11(2) of the Money Laundering Order requires that policies and procedures established and maintained under Article 11(1) are appropriate and consistent having regard to the degree of risk of money laundering and the financing of terrorism taking into account: (i) the level of risk identified in a national or sector-specific risk assessment in relation to money laundering carried out in respect of Jersey; and (ii) the type of customers, business relationships, products and transactions with which the relevant person's business is concerned.*
35. *Article 11(3) lists a number of policies and procedures that must be established and maintained.*

36. *Article 11(9) of the Money Laundering Order requires a relevant person to take appropriate measures for the purpose of making employees whose duties relate to the provision of financial services ("relevant employees") aware of policies and procedures under Article 11(1) and of legislation in Jersey to counter money laundering and the financing of terrorism. Article 11(10) of the Money Laundering Order requires a relevant person to provide relevant employees with training in the recognition and handling of transactions carried out by or on behalf of persons who are, or appear to be, engaged in money laundering or financing terrorism.*

37. *Article 11(11) of the Money Laundering Order requires a relevant person to establish and maintain policies and procedures for monitoring compliance with, and testing the effectiveness of: (i) its policies and procedures; (ii) its measures to promote AML/CFT awareness; and (iii) its training of relevant employees (see Section 9 of this Handbook).*

38. *When considering the type and extent of testing to be carried out under Article 11(11), Article 11(12) of the Money Laundering Order requires a relevant person to have regard to the risk of money laundering or financing of terrorism that exists in respect of the relevant person's business, and matters that have an impact on that risk, such as the size and structure of the relevant person.*

39. *Article 11(8) requires that a relevant person operating through branches or subsidiaries, which carry on financial services business, must communicate its policies and procedures, maintained in accordance with Article 11(1), to those branches or subsidiaries. In addition, Article 11A requires group programmes for information sharing (see Section 2.7 of this Handbook).*

AML/CFT/CPF Codes of Practice

40. A *supervised person* must establish and maintain appropriate and consistent *systems and controls* to prevent and detect *money laundering,* the *financing of terrorism,* and the *financing of proliferation*, that enable it to:

- apply the policies and procedures referred to in Article 11 of the Money Laundering Order
- apply CDD measures – in line with Sections 3 to 7 of this Handbook
- report to the JFCU when it knows, suspects, or has reasonable grounds to know or suspect that another person is involved in money laundering or the financing of terrorism, including attempted transactions – in line with Section 8 of this Handbook
- adequately screen relevant employees when they are initially employed, make employees aware of certain matters and provide training – in line with Section 9 of this Handbook
- keep complete records that may be accessed on a timely basis – in line with Section 10 of this Handbook
- liaise closely with the JFSC and the JFCU on matters concerning vigilance, systems and controls (including policies and procedures)
- communicate policies and procedures to overseas branches and subsidiaries (subject to Article 10A(9) see section 1.4.2), and monitor compliance therewith and
- monitor and review instances where exemptions are granted to policies and procedures, or where controls are overridden.

41. In addition to those listed in Article 11(3) of the Money Laundering Order, a *supervised person's policies and procedures* must include *policies and procedures* for:

- customer acceptance (and rejection), including approval levels for higher risk customers
- the use of transaction limits and management approval for higher risk customers
- placing reliance on obliged persons
- applying exemptions from customer due diligence requirements under Part 3A of the Money Laundering Order and enhanced CDD measures under Articles 15, 15A and 15B
- keeping documents, data or information obtained under identification measures up to date and relevant, including changes in beneficial ownership and control
- taking action in response to notices highlighting countries and territories in relation to which the FATF has called for the application of countermeasures or enhanced CDD measures
- taking action to comply with the *Targeted Financial Sanctions Measures* and the Directions Law.

42. In maintaining the required *systems and controls* (including *policies and procedures*), a *supervised person* must check that the *systems and controls* (including *policies and procedures*) are operating effectively and test that they are complied with.

2.4.1 Effectiveness of systems and controls

Guidance notes

43. A *supervised person* may demonstrate that it checks that *systems and controls* (including *policies and procedures*) are adequate and operating effectively where the Board periodically considers the efficacy (capacity to have the desired outcome) of those *systems and controls* (including *policies and procedures*, and those in place at branches and in respect of subsidiaries) in light of:
    - changes to its business activities or business risk assessment
    - information published from time to time by the *JFSC* or *JFCU*, e.g. findings of supervisory and themed examinations and typologies
    - changes made or proposed in respect of new legislation, *AML/CFT/CPF Codes of Practice* issued under the Supervisory Bodies Law or guidance
    - resources available to comply with the *Anti-Money Laundering and Counter-Terrorism Legislation* and *AML/CFT/CPF Codes of Practice* issued under the *Supervisory Bodies Law*, in particular resources provided to the *MLCO* and *MLRO*, to apply enhanced *CDD* measures and to scrutinise transactions.

44. A *supervised person* may demonstrate that it checks that *systems and controls* (including *policies and procedures*) are operating effectively where the Board periodically considers the effect of those *systems and controls* (including *policies and procedures*, and those in place at branches and in respect of subsidiaries) in light of the information that is available to it, including:
    - reports presented by the *MLCO* and others (e.g., where appropriate, risk management and internal audit functions) on compliance matters and *MLRO* on reporting
    - reports summarising findings from supervisory and themed examinations and action taken or being taken to address recommendations

- the number and percentage of *customers* that have been assessed by the *supervised person* as presenting a higher risk
- the number of applications to establish business relationships or carry-out one-off transactions which have been declined due to *CDD* issues, along with reasons
- the number of business relationships terminated due to *CDD* issues, along with reasons
- the number of "existing *customers*" that have still to be remediated under Section 4.7.2 of this Handbook
- details of failures by an *obliged person* or *customer* to provide information and evidence on demand and without delay under Articles 16, 16A and 17B-D of the Money Laundering Order, and action taken
- the number of alerts generated by automated on-going monitoring systems
- the number of internal *SARs* made to the *MLRO* (or *Deputy MLRO*), the number of subsequent external *SARs* submitted to the *JFCU*, and timeliness of reporting (by business area if appropriate)
- inquiries made by the *JFCU*, or production orders received, without issues having previously been identified by *CDD* or reporting *policies and procedures*, along with reasons
- results of testing of awareness of *relevant employees* with *policies and procedures* and legislation
- the number and scope of exemptions granted to *policies and procedures*, including at branches and subsidiaries, along with reasons.

45. The level of *systems and controls*, and the extent to which monitoring needs to take place will be affected by:
    - the supervised person's size
    - the nature, scale and complexity of its operations
    - the number of different business types it is involved in
    - the types of services it offers and how it delivers those services
    - the type of business transactions it becomes involved in or advises on
    - its overall risk profile.
46. Areas which are required under the *Money Laundering Order* to be covered in *systems and controls* include (but are not limited to):
    - the manner in which disclosures are to be made to the *MLRO*
    - the circumstances in which delayed *CDD* is permitted
    - when outsourcing of *CDD* obligations or reliance on third parties will be permitted, and on what conditions
    - *CDD* requirements to be met for simplified, standard and enhanced due diligence

- how the *supervised person* will restrict work being conducted for a *customer* where *CDD* has not been completed

47. Issues which may also be covered in *systems and controls* include:

- the level of personnel permitted to exercise discretion on the risk-based application of the *Money Laundering Order* and this Handbook, and under what circumstances
- when cash payments will be accepted
- when payments will be accepted from or made to third parties
- the *supervised person's* policy for applying legal professional privilege (*LPP*). Note that *LPP* is only applicable to lawyers – see Section 15.7.1 of this Handbook for specific guidance.

2.4.2 Testing of compliance with systems and controls

Guidance notes

48. A *supervised person* may demonstrate that it has tested compliance with *systems and controls* (including *policies and procedures*) where the Board periodically considers the means by which compliance with its *systems and controls* (including *policies and procedures*) has been monitored, compliance deficiencies identified and details of action taken or proposed to address any such deficiencies.

49. A *supervised person* may demonstrate that it has tested compliance with *systems and controls* (including *policies and procedures*) where testing covers all of the *policies and procedures* maintained in line with Article 11(1) of the *Money Laundering Order* and the *AML/CFT/CPF Code of Practice* at paragraph 41 above, and in particular:

- the application of simplified and enhanced *CDD* measures
- reliance placed on *obliged persons* under Article 16 of the Money Laundering Order
- action taken in response to notices highlighting countries and territories in relation to which the *FATF* has called for the application of countermeasures or enhanced CDD measures
- action taken to comply with the Targeted Financial Sanctions Measures and the Directions Law, and
- the number or type of employees who have received training, the methods of training and the nature of any significant issues arising from the training.

2.4.3 Consideration of cultural barriers

Overview

50. The implementation of *systems and controls* (including *policies and procedures*) for the prevention and detection of *money laundering*, the countering of *terrorist financing*, and the countering of *proliferation financing* does not remove the need for a *supervised person* to address cultural barriers that can prevent effective control. Human factors, such as the inter-relationships between different employees, and between employees and *customers*, can result in the creation of damaging barriers.

51. Unlike *systems and controls* (including *policies and procedures*), the prevailing culture of an organisation is intangible. As a result, its impact on a *supervised person* can sometimes be difficult to measure.

Guidance notes

52. A *supervised person* may demonstrate that it has considered whether cultural barriers might hinder the effective operation of *systems and controls* (including *policies and procedures*) to prevent and detect *money laundering*, counter *terrorist financing*, and *counter proliferation financing* where the Board considers the prevalence of the following factors:

- an unwillingness on the part of employees to subject high value (and therefore important) *customers* to effective *CDD* measures for commercial reasons
- pressure applied by management or *customer* relationship managers outside Jersey upon employees in Jersey to transact without first conducting all relevant *CDD*
- undue influence exerted by relatively large *customers* in order to circumvent *CDD* measures
- excessive pressure applied on employees to meet aggressive revenue-based targets, or where employee or management remuneration or bonus schemes are exclusively linked to revenue-based targets
- an excessive desire on the part of employees to provide a confidential and efficient *customer* service
- design of the *customer* risk classification system in a way that avoids rating any *customer* as presenting a higher risk
- the inability of employees to understand the commercial rationale for business relationships, resulting in a failure to identify non-commercial and therefore potential *money laundering, terrorist financing,* or *proliferation financing* activity
- negative handling by managerial staff of queries raised by more junior employees regarding unusual, complex or higher risk activity and transactions
- an assumption on the part of more junior employees that their concerns or suspicions are of no consequence
- a tendency for line managers to discourage employees from raising concerns due to lack of time and/or resources, preventing any such concerns from being addressed satisfactorily
- dismissal of information concerning allegations of criminal activities on the grounds that the *customer* has not been successfully prosecuted or lack of public information to verify the veracity of allegations
- the familiarity of employees with certain *customers* resulting in unusual or higher risk activity and transactions within such relationships not being identified as such
- little weight or significance is attributed to the role of the *MLCO* or *MLRO*, and little cooperation between these post-holders and *customer*-facing employees
- actual practices applied by employees do not align with *policies and procedures*
- employee feedback on problems encountered applying *policies and procedures* is ignored
- non-attendance of senior employees at training sessions on the basis of a mistaken belief that they cannot learn anything new or because they have too many other competing demands on their time.

2.4.4 Outsourcing

Overview

53. In a case where a *supervised person* outsources a particular activity, it bears the ultimate responsibility for the duties undertaken in its name. This will include the requirement to determine that the external party has in place satisfactory *systems and controls* (including *policies and procedures*), and that those *systems and controls* (including *policies and procedures*) are kept up to date to reflect changes in requirements. See the table below for details of which *CDD* activities may be outsourced.

<table>
<tr><th>CDD (always the ultimate responsibility of the supervised person)</th><th colspan="2">Activities which may be outsourced</th></tr>
<tr><td rowspan="6">*Identification measures*</td><td colspan="2">Risk assessment</td></tr>
<tr><td colspan="2">ID *customer*</td></tr>
<tr><td colspan="2">ID third parties</td></tr>
<tr><td>ID person acting for *customer*</td><td>Verify authority to act</td></tr>
<tr><td rowspan="2">Where *customer* not individual:</td><td>Understand ownership/control structure</td></tr>
<tr><td>ID *beneficial owners/controllers*</td></tr>
<tr><td colspan="2">Obtain information on purpose/nature</td></tr>
<tr><td rowspan="2">On-going monitoring</td><td colspan="2">Scrutinising transactions/activity</td></tr>
<tr><td colspan="2">Keep documents/information up-to-date</td></tr>
</table>

54. Depending on the nature and size of a *supervised person*, the roles of the *MLCO* and *MLRO* may require additional support and resourcing. Where a *supervised person* elects to bring in additional support, or to delegate areas of the *MLCO* or *MLRO* functions to external parties, the *MLCO* or *MLRO* will remain directly responsible for their respective role, and the Board will remain responsible for overall compliance with the *Anti-Money Laundering and Counter-Terrorism Legislation* (and by extension, also this Handbook). Note that the *AML/CFT/CPF Codes of Practice* at Paragraphs 69 and 82 below provide that the role of the *MLCO* and *MLRO* must be undertaken by an employee of the *supervised person* based in Jersey, unless the circumstances set out in the sub-paragraphs to those specific codes of practice apply.

55. The JFSC has also issued an Outsourcing Policy and guidance note for *supervised persons*, which outlines its own set of requirements and obligations in respect of outsourcing.

AML/CFT/CPF Codes of Practice

56. All *supervised persons* must comply with the JFSC's Outsourcing Policy and guidance note.

57. A *supervised person* must consider the effect that outsourcing has on *money laundering, terrorist financing, and proliferation financing* risk, in particular where a *MLCO* or *MLRO* is provided with additional support from other parties, either from within group or externally.

58. A *supervised person* must assess possible *money laundering, terrorist financing, and proliferation financing* risk associated with outsourced functions, record its assessment, and monitor any risk on an on-going basis.

59. Where an outsourced activity is a *supervised business* activity, then a *supervised person* must be satisfied that the provider of the outsourced services has in place *policies and procedures* that are consistent with those required under the Money Laundering Order and, by association, this Handbook.

60. In particular, a *supervised person* must be satisfied that knowledge, suspicion, or reasonable grounds for knowledge or suspicion of *money laundering* or *financing of terrorism* activity will be reported by the provider of the outsourced service to the *MLRO* (or *deputy MLRO*) of the *supervised person*.

2.5 The Money Laundering Compliance Officer (MLCO)

Overview

61. The *Money Laundering Order* requires a *supervised person* to appoint an individual as *MLCO*, and tasks that individual with the function of monitoring its compliance with legislation in Jersey relating to *money laundering,* the *financing of terrorism,* and the *financing of proliferation* and *AML/CFT/CPF Codes of Practice* issued under the Supervisory Bodies Law. The objective of this requirement is to require *supervised persons* to clearly demonstrate how they ensure compliance with the requirements of the same.

62. The Money Laundering Order also requires a *supervised person* to maintain adequate procedures for:

    a. monitoring compliance with, and testing the effectiveness of, *policies and procedures* and

    b. monitoring and testing the effectiveness of measures to raise awareness and training. When considering the type and extent of compliance testing to be carried out, a *supervised person* shall have regard to the risk of *money laundering,* the *financing of terrorism,* and the *financing of proliferation* and matters that have an impact on risk, such as size and structure of the *supervised person's* business.

63. The *MLCO* may have a functional reporting line, e.g. to a group compliance function.

64. The *Money Laundering Order* does not rule out the possibility that the *MLCO* may also have other responsibilities. To the extent that the *MLCO* is also responsible for the development of *systems and controls* (and *policies and procedures*) as well as monitoring subsequent compliance with those *systems and controls* (and *policies and procedures*), some additional independent assessment of compliance will be needed from time to time to address this potential conflict. Such an independent assessment is unlikely to be needed where the role of the *MLCO* is limited to actively monitoring the development and implementation of such *systems and controls*.

Statutory requirements (paraphrased wording)

65. *Article 7 of the Money Laundering Order requires a relevant person to appoint a MLCO to monitor whether the enactments in Jersey relating to money laundering and the financing of terrorism and AML/CFT/CPF Codes of Practice are being complied with. The same person may be appointed as both MLCO and MLRO.*

66. *Article 7(2A) of the Money Laundering Order requires a relevant person to ensure that the individual appointed is of an appropriate level of seniority and has timely access to all records that are necessary or expedient.*

67. *Article 7(6) of the Money Laundering Order requires a relevant person to notify the JFSC in writing within one month when a person is appointed as, or ceases to be, a MLCO. However, Article 10 provides that the JFSC may grant exemptions from this notification requirement, by way of notice.*

68. *Article 7 of the Money Laundering Order recognises that a relevant person that is also a regulated person may have notified the JFSC of the appointment or cessation of a MLCO under other legislation. If so, a duplicate notification is not required under the Money Laundering Order.*

AML/CFT/CPF Codes of Practice

69. A supervised person must appoint a MLCO that:

- is employed by the *supervised person* or an enterprise in the same financial group as the *supervised person*
    - In the case of a supervised person that: carries on the business of being a functionary, recognized fund, or unclassified fund or is a Category B insurance permit holder, a managed bank, or other managed entity; has no employees of its own; and is administered by a person carrying on a supervised business, it is acceptable for an employee of the administrator to be appointed by the supervised person as its MLCO
- is based in Jersey
    - In the case of a supervised person that is a Category A insurance business permit holder with no employees of its own in Jersey, it is acceptable to appoint an employee outside Jersey. In the case of a supervised person that is carrying on a money service business and has no employees of its own in Jersey, it is acceptable for the supervised person to appoint an employee outside Jersey as its MLCO, provided the employee is based in an equivalent jurisdiction; and
- has sufficient experience and skills.

70. A *supervised person* must ensure that the *MLCO*:

- has appropriate independence, in particular from *customer*-facing, business development and *systems and controls* development roles
- reports regularly and directly to the Board and has a sufficient level of authority within the *supervised person* so that the Board reacts to and acts upon reports made by the *MLCO*
- has sufficient resources, including sufficient time and (if appropriate) a *deputy MLCO* and compliance support staff
- is fully aware of both their and the supervised person's obligations under the Anti-Money Laundering and Counter-Terrorism Legislation and AML/CFT/CPF Codes of Practice issued under the Supervisory Bodies Law.

71. In the event that the position of MLCO is expected to fall vacant, to comply with the *statutory requirement* to have an individual appointed to the office of MLCO at all times, a supervised person must take action to appoint a member of the Board (or other appropriate member of senior management) to the position on a temporary basis.

72. If temporary circumstances arise where the supervised person has a limited or inexperienced money laundering compliance resource, it must ensure that this resource is supported as necessary.

73. When considering whether it is appropriate to appoint the same person as *MLCO* and *MLRO*, a *supervised person* must have regard to:

- the respective demands of the two roles, taking into account the size and nature of the *supervised person's* activities; and
- whether the individual will have sufficient time and resources to fulfil both roles effectively.

Guidance notes

74. A *supervised person* may demonstrate that its *MLCO* is monitoring whether enactments and *AML/CFT/CPF Codes of Practice* issued under the Supervisory Bodies Law are being complied with where they:
    - regularly monitor and test compliance with *systems and controls* (including *policies and procedures*) in place to prevent and detect *money laundering,* counter the *financing of terrorism,* and counter the *financing of proliferation* – supported as necessary by a compliance or internal audit function
    - report periodically, as appropriate, to the Board on compliance with the *supervised person's systems and controls* (including *policies and procedures*) and issues that need to be brought to its attention
    - respond promptly to requests for information made by the *JFSC* and the *JFCU*.
75. In a case where the *MLCO* is also responsible for the development of *systems and controls* (including *policies and procedures*) in line with evolving requirements, a *supervised person* may demonstrate that the *MLCO* has appropriate independence where such *systems and controls* are subject to periodic independent scrutiny.

2.6 The Money Laundering Reporting Officer (MLRO)

Overview

76. Whilst the *Money Laundering Order* requires one individual to be appointed as *MLRO*, it recognises that, given the size and complexity of operations of many enterprises, it may be appropriate to designate additional persons (*deputy MLROs*) to whom *SARs* may be made.

Statutory requirements (paraphrased wording)

77. *Article 8 of the Money Laundering Order requires a relevant person to appoint a MLRO. The MLRO's function is to receive and consider internal SARs in accordance with internal reporting procedures. The same person may be appointed as both MLCO and MLRO.*
78. *Article 8(2A) of the Money Laundering Order requires a relevant person to ensure that the individual appointed is of an appropriate level of seniority and has timely access to all records that are necessary or expedient.*
79. *Article 8(4) of the Money Laundering Order requires a relevant person to notify the JFSC in writing within one month when a person is appointed as, or ceases to be, a MLRO. However, Article 10 provides that the JFSC may grant exemptions from this notification requirement, by way of notice.*
80. *Article 8 of the Money Laundering Order recognises that a relevant person that is also a regulated person may have notified the JFSC of the appointment or cessation of a MLRO under other legislation. If so, a duplicate notification is not required under the Money Laundering Order.*
81. *Article 9 of the Money Laundering Order allows a relevant person to designate one or more deputy MLROs, in addition to the MLRO, to whom internal SARs may be made.*

AML/CFT/CPF Codes of Practice

82. A *supervised person* must appoint a *MLRO* that:

- is employed by the *supervised person* or enterprise in the same financial group as the *supervised person*
    - In the case of a supervised person that: carries on the business of being a functionary, recognized fund, or unclassified fund, or is a Category B insurance permit holder, a managed bank, or other managed entity; has no employees of its own; and is administered by a person carrying on supervised business that is a supervised person, it is acceptable for an employee of the administrator to be appointed by the supervised person as its MLRO.
- is based in Jersey
    - In the case of a supervised person that is a Category A insurance business permit holder with no employees of its own in Jersey, it is acceptable to appoint an employee outside Jersey In the case of a supervised person that is carrying on a money service business and has no employees of its own in Jersey, it is acceptable for the supervised person to appoint an employee outside Jersey as its MLRO, provided the employee is based in an equivalent jurisdiction; and
- has sufficient experience and skills.

83. A *supervised person* must ensure that the *MLRO*:

- has appropriate independence, in particular from *customer*-facing and business development roles
- has a sufficient level of authority within the *supervised person*
- has sufficient resources, including sufficient time, and (if appropriate) is supported by *deputy MLROs*
- is able to raise issues directly with the Board, and
- is fully aware of both their and the supervised person's obligations under the Anti-Money Laundering and Counter-Terrorism Legislation and AML/issued under the Supervisory Bodies Law.

84. Where a *supervised person* has appointed one or more *deputy MLROs* the requirements set out above for the *MLRO* must also be applied to any *deputy MLROs*.

85. Where a *supervised person* has appointed one or more *deputy MLROs*, it must ensure that the *MLRO*:

- keeps a record of all *deputy MLROs*
- provides support to, and routinely monitors the performance of, each *deputy MLRO*
- considers and determines that *SARs* are being handled in an appropriate and consistent manner.

86. In the event that the position of *MLRO* is expected to fall vacant, to comply with the statutory requirement to have an individual appointed to the office of *MLRO* at all times, a *supervised person* must take action to appoint a member of the Board (or other appropriate member of senior management) to the position on a temporary basis.

87. If temporary circumstances arise where a *supervised person* has a limited or inexperienced *money laundering* reporting resource, it must ensure that this resource is supported as necessary.

Guidance notes

88. A *supervised person* may demonstrate that its *MLRO* (and any *deputy MLRO*) is receiving and considering *SARs* in accordance with Article 21 of the Money Laundering Order where, among other things, its *MLRO*:

- maintains a record of all requests for information from law enforcement authorities and records relating to all internal and external *SARs* (see Section 8 of this Handbook)
- manages relationships effectively post disclosure to avoid tipping off any external parties
- acts as the liaison point with the *JFSC* and the *JFCU* and in any other external enquiries in relation to *money laundering* or the *financing of terrorism*.

89. A *supervised person* may demonstrate routine monitoring of the performance of any *deputy MLROs* by requiring the *MLRO* to review:

- samples of records containing internal *SARs* and supporting information and documentation
- decisions of the *deputy MLRO* concerning whether to make an external *SAR*
- the bases for decisions taken.

2.7 Financial groups

Overview

90. A *Financial Group* of which a *supervised person* is a member must maintain a group programme for the sharing of *AML/CFT/CPF* information.

91. In addition, as explained in Section 1.4.3, where a company incorporated in Jersey (a *supervised person)* carries on a *supervised business* through an overseas branch, it must comply with *AML/CFT/CPF Codes of Practice* issued under the Supervisory Bodies Law in respect of that business, irrespective of whether it also carries on *supervised business* in or from within Jersey.

92. In practice, the above only applies to *supervised persons* that meet the definition of a *financial group*, this includes a requirement that a parent company or other legal person exercise control over every member of that group for the purposes of applying group supervision.

    Group supervision refers to (a) the core principles for effective banking supervision published by the Basel Committee on Banking Supervision; (b) the Objectives and Principles of Securities Regulation issued by the International Organisation of Securities Commissions; or (c) the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.

Statutory requirements (paraphrased wording)

93. *Article 11A of the Money Laundering Order applies to a financial group of which a relevant person is a member.*

94. *Article 11A(2) of the Money Laundering Order requires a financial group to maintain a programme to prevent and detect money laundering and the financing of terrorism that includes:*

- *Policies and procedures by which a relevant person within a financial group, which carries on financial services business or equivalent business, may disclose information to a member of the same financial group, but only where such disclosure is appropriate for the purpose of preventing and detecting money laundering or managing money laundering risks*
- *Adequate safeguards for the confidentiality and use of any such information*
- *The monitoring and management of compliance with, and the internal communication of, such policies and procedures (including the appointment of a compliance officer for the financial group)*
- *The screening of employees.*

95. *Under Article 11A(3) of the Money Laundering Order "information" includes the following:*

- *Information or evidence obtained from applying identification measures*
- *Customer, account and transaction information*
- *Information relating to the analysis of transactions or activities that are considered unusual.*

AML/CFT/CPF Codes of Practice

96. A *supervised* person that is a Jersey incorporated company must ensure that any subsidiary applies measures that are at least equivalent to the *AML/CFT/CPF Codes of Practice* in respect of any *supervised business* carried on outside Jersey by that subsidiary.

97. A *supervised* person who:

- is registered, incorporated or otherwise established under Jersey law, but who is not a Jersey incorporated company, and
- carries on a *supervised business* in or from within Jersey

must apply measures that are at least equivalent to the *AML/CFT/CPF Codes of Practice* in respect of any *supervised business* carried on by that person through an overseas branch/office.

95. A person who:

- is registered, incorporated or otherwise established under Jersey law, but who is not a Jersey incorporated company, and
- carries on a *supervised business* in or from within Jersey

must ensure that any subsidiary applies measures that are at least equivalent to the *AML/CFT/CPF Codes of Practice* in respect of any *supervised business* carried on outside Jersey by that person.

96. Where overseas legislation prohibits compliance with an *AML/CFT/CPF Code of Practice* (or measures that are at least equivalent) then the *AML/CFT/CPF Codes of Practice* do not apply and the *JFSC* must be informed that this is the case. In such circumstances, a *supervised person* must take other reasonable steps to effectively deal with the risk of *money laundering,* the *financing of terrorism,* and the *financing of proliferation*.

3 IDENTIFICATION MEASURES – OVERVIEW

3.1 Overview of section

1. This section explains the *identification measures* required under Article 13 of the *Money Laundering Order*, and the framework under which a *supervised person* is required to apply a risk based approach to the application of such measures.
2. This section should be read and understood in conjunction with the following sections:
   - section 4 – which explains the basis for finding out identity and obtaining evidence of identity
   - section 5 – which considers the circumstances in which reliance might be placed on another party to have applied *reliance identification measures*
   - section 7 – which explains the application of enhanced *CDD* measures (including the case of a *customer* that is assessed as presenting a higher risk) and simplified *identification measures*.
3. Sound *identification measures* are vital because they:
   - help to protect the *supervised person* and the integrity of the financial sector in which it operates by reducing the likelihood of the business becoming a vehicle for, or a victim of, financial crime, including *money laundering,* the *financing of terrorism,* and the *financing of proliferation*
   - assist law enforcement, by providing available information on *customers* or activities and transactions being investigated
   - constitute an essential part of sound risk management, e.g. by providing the basis for identifying, limiting and controlling risk
   - help to guard against identity fraud.
4. The inadequacy or absence of *identification measures* can expose a *supervised person* to serious *customer* and counterparty risks, as well as reputational, operational, legal, regulatory and concentration risks, any of which can result in significant financial cost to the business. Documents, data or information held also assist the *MLRO* (or *deputy MLRO*) and other employees to determine whether a *SAR* is appropriate.
5. A *customer* may be an individual (or group of individuals) or legal person. Section 4.3 deals with a *customer* who is an individual (or group of individuals), Section 4.4 deals with a *customer* (an individual or legal person) who is acting for a legal arrangement, and Section 4.5 deals with a *customer* who is a legal person.
6. The term customer, as used in this Handbook, is defined in the Glossary above. As noted in the definition, *customers* can include a prospective *customers* (i.e. applicants for business).

3.2 Obligation to apply identification measures

Statutory requirements (paraphrased wording)

7. *Article 13(1) of the Money Laundering Order requires a relevant person to apply CDD measures. CDD measures comprise identification measures and on-going monitoring. Identification measures must be applied:*

- *subject to Article 13(4) to (11) of the Money Laundering Order, before the establishment of a business relationship or before carrying out a one-off transaction*
- *where a relevant person suspects money laundering*
- *where a relevant person has doubts about the veracity of documents, data or information previously obtained under CDD measures.*

Identification Measures

8. *Article 3(2) of the Money Laundering Order sets out what **identification measures** are to involve:*

- *finding out the identity of a **customer** and obtaining evidence of identity from a reliable and independent source that is reasonably capable of verifying that the person to be identified is who the person is said to be and satisfies the person responsible for the identification of a person that the evidence does establish that fact (referred to as "**obtaining evidence**"). See Article 3(2)(a) of the Money Laundering Order*
- *finding out the identity of any person purporting to act on behalf of the customer and verifying the authority of any person purporting so to act. See Article 3(2)(aa) of the Money Laundering Order*
- ***where the customer is a legal person**, understanding the ownership and control structure of that customer and the provisions under which the customer can enter into contracts, or other similarly legal binding arrangements, with third parties. See Article 3(2)I(ii) of the Money Laundering Order*
- ***where the customer is a legal person**, finding out the identity of individuals who are the beneficial owners or controllers of the customer and obtaining evidence of the identity of those individuals. See Article 3(2)(c)(iii) of the Money Laundering Order*
- *determining whether the customer is acting for a third party (or parties), whether directly or indirectly. See Article 3(2)(b) of the Money Laundering Order*
- *finding out the identity of any **third party** (or parties) on whose behalf the customer is acting and obtaining evidence of the identity of those persons. See Article 3(2)(b)(i) of the Money Laundering Order*
- ***where the third party is a legal person**, understanding the ownership and control of that third party, finding out the identity of the individuals who are the beneficial owners or controllers of the third party and obtaining evidence of the identity of those individuals. See Article 3(2)(b)(ii) of the Money Laundering Order*
- ***where the third party is a legal arrangement**, e.g. a trust, understanding the nature of the legal arrangement under which the third party is constituted. See Article 3(2)(b)(iii)(A) of the Money Laundering Order*
- ***where the third party is a legal arrangement**, e.g. a trust, finding out the identity of the persons who are listed in Article 3(7) of the Money Laundering Order. See Article 3(2)(b)(iii)(B) of the Money Laundering Order*
- ***where the third party is a legal arrangement**, e.g. a trust, where any person listed in Article 3(7) is not an individual, finding out the identity of the individuals who are the beneficial owners or controllers of the person and obtaining evidence of the identity of those individuals. See Article 3(2)(b)(iii)(C) of the Money Laundering Order*
- *obtaining information on the purpose and intended nature of the business relationship or one-off transaction. See Article 3(2)(d) of the Money Laundering Order.*

9. *Article 3(5) of the Money Laundering Order requires identification measures to include the assessment (i.e. customer risk assessment) by a relevant person of the risk that a business relationship or one-off transaction will involve money laundering. This must include obtaining appropriate information for assessing that risk.*
10. *Article 3(6) requires, in cases where a customer is acting for a third party, and where the customer is a legal person, measures for obtaining evidence of identity for third parties, persons purporting to act on behalf of the customer, and individuals who are the customer's beneficial owners or controllers, to involve reasonable measures having regard to all the circumstances of the case, including the degree of risk assessed.*
11. *For persons who are not individuals, Article 2 of the Money Laundering Order describes:*
    - *beneficial owners as individuals with ultimate beneficial ownership of that person*
    - *beneficial controllers as individuals who ultimately control that person or otherwise exercise control over the management of that person.*
12. *The description of a beneficial owner or controller will apply whether the individual satisfies the description alone or jointly with other persons.*
13. *Article 2 of the Money Laundering Order provides that no individual is to be treated as a beneficial owner of a person that is a body corporate or a limited liability company, the securities of which are listed on a regulated market.*

On-going Monitoring

14. *Article 3(3) of the Money Laundering Order sets out what **on-going monitoring** is to involve:*
    - *scrutinising transactions undertaken throughout the course of a business relationship to ensure that the transactions being conducted are consistent with the relevant person's knowledge of the customer, including the customer's business and risk profile. See Article 3(3)(a) of the Money Laundering Order*
    - *keeping documents, data or information up to date and relevant by undertaking reviews of existing records, particularly in relation to higher risk categories of customers. See Article 3(3)(b) of the Money Laundering Order.*

Policies and Procedures

15. *Among other things, Article 11(1) and (2) of the Money Laundering Order requires a relevant person to maintain **policies and procedures** for the application of CDD measures that are appropriate and consistent having regard to the degree of risk of money laundering and the financing of terrorism taking into account:*
    - *the level of risk identified in a national or sector-specific risk assessment in relation to money laundering carried out in respect of Jersey*
    - *the type of customers, business relationships, products and transactions with which the relevant person's business is concerned.*
16. *Among other things, Article 11(3) of the Money Laundering Order requires that the appropriate and consistent policies and procedures include policies and procedures which:*
    - *determine whether a customer (and others connected to the customer) is a PEP, has a connection with a country or territory that does not apply, or insufficiently applies the FATF Recommendations, or is subject to or connected with a country, territory or organization that is subject to a call from the FATF for the application of enhanced due diligence measures*

- *determine whether a transaction is with a person connected with a country or territory that does not apply, or insufficiently applies the FATF Recommendations, or is subject to or connected with a country, territory or organisation that is subject to a call from the FATF for the application of enhanced due diligence measures*
- *assess and manage the risk of money laundering or the financing of terrorism occurring as a result of completing identification measures after the establishment of a business relationship (where permitted), and ensure periodic reporting to senior management in such cases.*

17. *Article 13(10) to (12) provides that a relevant person that is a collective investment scheme shall not be required to apply customer due diligence measures to a person that becomes a unitholder through a secondary market transaction, so long as:*

- *a person carrying on investment business has applied identification measures; or*
- *a person carrying on equivalent business to investment business has applied identification measures in line with FATF Recommendation 10.*

18. *A "secondary market" is a financial market in which previously issued units are bought and sold.*

19. *Where a relationship between a relevant person and a customer has no "element of duration" and is not a one-off transaction within the meaning of Article 4 of the Money Laundering Order, identification measures within the meaning of Article 13 of the Money Laundering Order are not required unless:*

- *the relevant person suspects money laundering or financing of terrorism; or*
- *the relevant person has doubts about the veracity or adequacy of any documents, data or information previously obtained under the CDD measures.*

3.3 Risk-based approach to Identification Measures

Overview

20. A risk-based approach to the application of *identification measures* is one that involves a number of discrete stages in assessing the most effective and proportionate way to manage the *money laundering, terrorist financing,* and *proliferation financing risk* faced by a *supervised person*. While these stages must be incorporated into *policies and procedures*, they do not need to take place in the sequence outlined below and may occur simultaneously.

21. The risk assessment of a particular *customer* (customer risk assessment) will determine the extent of information which will be requested, what evidence of identity will be obtained, the extent to which the resulting relationship will be scrutinised, and how often documents, data or information held will be reviewed.

22. Section 2.3 of this Handbook requires the Board (or where the *supervised person* is not a company, the senior management function) of a *supervised person* to conduct (and keep up-to-date) a business risk assessment, which considers the *supervised person's* risk appetite, activities and structure and concludes on the *supervised person's* exposure to *money laundering*, the *financing of terrorism,* and the *financing of proliferation* risk.

23. This business risk assessment will enable a *supervised person* to determine its initial approach to performing Stage 1 of the identification process as set out below, depending on the type of *customer*, product or service involved. The remaining stages of the process require a *supervised person* to consider whether the specific circumstances of the *customer* will necessitate the application of further measures.

24. Part 3A of the *Money Laundering Order* sets out exemptions from *CDD* requirements, including circumstances in which exemptions do not apply (See Article 17A), exemptions from applying third party and other identification requirements (See Articles 17B, 17C, 18) and the obligations of a *supervised person* who is exempt from applying third party identification requirements (See Article 17D).

25. The following are the stages in the identification process:

Stage	Identification measure	Article(s)	Guidance
1.1	In the case of a *customer* that is a legal person, a *supervised person* must understand the ownership and control structure of the *customer* (and provisions under which the *customer* can enter into contracts).	3(2)(c)(ii)	Section 3.3.1
1.2	A *supervised person* must find out the identity of: › the *customer*; › any *beneficial owners and controllers* of the *customer*; › any third party (or parties) – including a legal arrangement - on whose behalf the *customer* acts. Whether directly or indirectly (and *beneficial owners and controllers* of the third party (or parties)); ○ For the avoidance of doubt, the above will include any person who is a named beneficiary of a life assurance policy entered into by the customer; and › others listed in Article 3(2).	3(2)(a) to (c) 3(4)(a)	Section 4
1.3	A *supervised person* must obtain information on the purpose and intended nature of the *business relationship* or *one-off transaction*.	(2)(d)	Sections 3.3.2 and 3.3.3 Section 7
1.4	A *supervised person* must obtain appropriate information for assessing the risk that a *business relationship* or *one-off transaction* will involve *money laundering*, the *financing of terrorism,* or the *financing of proliferation*. It may be necessary to repeat this stage following an assessment of risk under stage 2.1.	3(5) 15(1)	Sections 3.3.2 and 3.3.3 Section 7
2.1	A *supervised person* must, on the basis of information collected at stage 1, assess the risk that a *business relationship* or *one-off transaction* will involve *money laundering*, *the financing of terrorism,* or the *financing of proliferation* (risk profile).	3(5)	Section 3.3.4
2.2	A *supervised person* must prepare and record a *customer* business and risk profile.	3(3)(a)	Section 3.3.5
3	A *supervised person* must obtain evidence of the identity of those whose identity is found out at stage 1.2.	3(2)(a) to (c) 3(4)(b) 15(1)	Section 4 Section 7

26. By virtue of on-going monitoring, particularly in relation to higher risk categories of *customers*, under Article 3(3)(b) of the *Money Laundering Order*, a *supervised person* must keep documents, data and information obtained under Stages 1 and 3 up to date and relevant. See Section 3.4 of this Handbook.

27. *Systems and controls* (including *policies and procedures*) will not detect and prevent all instances of *money laundering*, the *financing of terrorism,* or the *financing of proliferation*. A risk-based approach will, however, serve to balance the cost burden placed on a *supervised person* and on *customers* with the risk that the business may be used in *money laundering,* the *financing of terrorism,* or the *financing of proliferation* by focusing resources on higher risk areas.

28. Care has to be exercised under a risk based approach. Being identified as carrying a higher risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* does not automatically mean that a customer is a money launderer, is financing terrorism, or is financing proliferation. Similarly, identifying a *customer* as carrying a lower risk of *money laundering,* the *financing of terrorism,* or *financing of proliferation* does not mean that the *customer* is not a *money launderer*, a *terrorist financier* or a proliferator.

AML/CFT/CPF Codes of Practice

29. A *supervised person* must apply a risk-based approach to determine the extent and nature of the measures to be taken when undertaking the identification process set out above.

3.3.1 Understanding ownership structure – Stage 1.1

Overview

30. Article 3(2)(c)(ii) of the *Money Laundering Order* requires a *supervised person* to understand who owns and controls a *customer* that is a legal person. Without such an understanding, it will not be possible to identify the individuals who are the customer's *beneficial owners and controllers*.

31. Understanding ownership involves taking three separate steps:

- requesting information from the *customer* (or a professional)
- validating that information
- checking that information held makes sense.

Guidance notes

32. **Step 1** – A *supervised person* may demonstrate that it understands the ownership and control structure of a *customer* that is a legal person where it applies one of the following *identification measures*:

- it requests the *customer* to provide a statement of legal and *beneficial ownership and control* as part of its application to become a *customer*. In the case of a legal person that is part of a group, this will include a group structure
- to the extent that a *customer* is, or has been, provided with professional services by a *lawyer* or *accountant*, or is "administered" by a Trust and Company Services provider, it requests that lawyer, accountant or Trust and Company Services provider to provide a statement of legal and *beneficial ownership and control*. In the case of a legal person that is part of a group, this will include a group structure.

33. **Step 2** – A *supervised person* may demonstrate that it understands the **legal** ownership and control structure of a *customer* that is a legal person where it takes into account information that is held:

- by the *customer*, e.g. recorded in its share register
- by a *lawyer*, *accountant* or Trust and Company Services provider

- by a trusted external party, in the case of a legal person with bearer shares, where bearer certificates have been lodged with that trusted external party
- publicly, e.g. information that is held in a central register in the country of establishment.

34. A *supervised person* may demonstrate that it understands the ***beneficial*** *ownership and control* structure of a *customer* that is a legal person where it takes into account information that is:
    - held by the *customer*, e.g. in line with company law, *AML/CFT/CPF* requirements, or listing rules, e.g. a declaration of trust in respect of shares held by a nominee shareholder
    - held by a *lawyer, accountant* or Trust and Company Services provider, e.g. in order to meet *AML/CFT/CPF* requirements
    - held in a public register, e.g. information that is held in a central register of *beneficial ownership* in the country of establishment, information that is published in financial statements prepared under generally accepted accounting principles, or information available as a result of a listing of securities on a stock exchange
    - provided directly by the ultimate beneficial owner(s) of the legal person
    - publicly available, e.g. in commercial databases and press reports.

35. **Step 3** – A *supervised person* may demonstrate that it understands the ownership and control structure of a *customer* that is a legal person where it applies one or more of the following *identification measures*:
    - it considers the purpose and rationale for using an entity with a separate legal personality
    - in the case of a legal person that is part of a group, it considers whether the corporate structure makes economic sense, taking into account complexity and multi-jurisdictional aspects.

3.3.2 Information for assessing risk – Stage 1.4

Guidance notes

36. A *supervised person* may demonstrate that it has obtained appropriate information for assessing the risk that a business relationship or one-off transaction will involve *money laundering,* the *financing of terrorism,* or the *financing of proliferation* where it collects the following information:

All *customer* types	
All *customer* types	› Type, volume and value of activity expected (having regard for the *JFSC's* Sound Business Practice Policy). › *Source of funds*, e.g. nature and details of occupation or employment. › Details of any existing relationships with the *supervised person*.

Additional relationship information	
Express trusts	› Type of trust (e.g. fixed interest, discretionary, testamentary). › Classes of beneficiaries, including any charitable causes named in the trust instrument.
Foundations	› Classes of beneficiaries, including any charitable objects.

Legal persons and legal arrangements (including express trusts and foundations)	› Ownership structure of any underlying legal persons. › Type of activities undertaken by any underlying legal persons (having regard for the *JFSC's* Sound Business Practice Policy and trading activities). › Geographical sphere of activities and assets. › Name of regulator, if applicable.

37. The extent of information sought in respect of a particular *customer*, or type of *customer*, will depend upon the country or territory with which the *customer* is connected, the characteristics of the product or service requested, how the product or service will be delivered, as well as factors specific to the *customer*.

3.3.2.1 Terms of Business

Overview

38. It may be helpful to:

› explain to the *customer* the reason for requiring *CDD* information and for the *customer* identification procedures. This can be achieved by including an additional paragraph in the terms of business or in pre-engagement communications.

› inform *customers* of the *supervised person's* reporting responsibilities under the primary legislation and the restrictions created by the 'tipping-off' rule on the *supervised person's* ability to discuss such matters with its *customers*.

39. Whether or not to advise the *customer* of these issues is a decision to be taken by individual *supervised persons*. However, if it is to be done it is important that the policy should apply consistently for all *customers*. A decision only to do so once a suspicion has arisen could result in the *supervised person* committing a tipping-off offence (see Section 8.5 of this Handbook).

3.3.2.2 Issues that might be covered when drawing up a profile

Guidance notes

40. To assist in drawing up a customer profile, supervised persons may wish to obtain information via a questionnaire. Supervised persons should be mindful that the questionnaire requests information they are legally obligated to obtain. *Supervised persons* should amend the questions and focus to suit their own *customer* base and products/services offered.

41. The *supervised person* may also be able to obtain further information prior the start of a *business relationship* or *one-off transaction* from other sources. Examples include:

› carrying out background searches and database screening and

› communicating with existing or previous providers of professional accountancy, banking and legal services to the *customer*.

3.3.3 Source of Funds – Stage 1.4

Overview

42. The ability to follow the audit trail for criminal funds and transactions flowing through the professional and financial sector is a vital law enforcement tool in *money laundering, financing of terrorism,* and *financing of proliferation* investigations. Understanding the *source of funds* and, in higher risk relationships, the customer's *source of wealth* is also an important aspect of *CDD*.

43. *Source of funds* is defined in the Glossary above. Information concerning the geographical sphere of the activities generating the *source of funds* may also be relevant.

44. *Supervised persons* should monitor whether funds received from *customers* are from credible sources. If funding is from a source other than a *customer*, a *supervised person* may need to make further enquiries. If it is decided to accept funds from a third party, perhaps because time is short, *supervised persons* should ask how and why the third party is helping with the funding.

45. In some circumstances, cleared funds will be essential for transactions and *customers* may want to provide cash to meet a deadline. *Supervised persons* should assess the risk in these cases and ask more questions if necessary.

46. The *Money Laundering Order* and the *AML/CFT/CPF Handbook* stipulate record-keeping requirements for transaction records. These require information concerning the remittance of funds to be recorded (e.g. the name of the bank and the name and account number of the account from which the funds were remitted). This remittance information is the source of transfer and not to be confused with *source of funds* information.

47. *Source of wealth* is defined in the Glossary above. It should also be reiterated that *source of wealth* is distinct from *source of funds*. Information concerning the geographical sphere of the activities that have generated a *customer's* wealth may also be relevant.

48. In finding out a *customer's source of wealth* it may not be necessary to determine the monetary value of their net worth.

3.3.4 Assessment of risk – Stage 2.1

49. The following factors - country risk, product/service risk, delivery risk, and *customer*-specific risk - will be relevant when assessing and evaluating the *CDD* information collected at Stage 1, and are not intended to be exhaustive. A *supervised person* should consider whether other variables are appropriate factors to consider in the context of the products and services that it provides and its *customer* base.

50. In assessing *customer* risk, the presence of one factor that might indicate higher risk will not automatically mean that a *customer* is in fact higher risk. Equally, the presence of one lower risk factor should not automatically lead to a determination that a *customer* is lower risk.

51. The sophistication of the risk assessment process may be determined according to factors supported by the business risk assessment.

52. Inconsistencies between information obtained may also assist in assessing risk. For example, a *supervised person* might identify inconsistencies between specific information concerning *source of funds* (or *source of wealth*), and the nature of the *customer's* expected activity.

53. A *supervised person* may demonstrate that it has assessed the risk that a *business relationship* or *one-off transaction* will involve *money laundering*, the *financing of terrorism,* or the *financing of proliferation* where it takes into account the factors set out at Section 3.3.4.1 below.

54. A *supervised person* may demonstrate that it has assessed the risk that a *business relationship* or *one-off transaction* will involve *money laundering*, the *financing of terrorism,* or the *financing of proliferation* where it takes into account other factors that are relevant in the context of the products and services that it provides and its *customer* base.

55. A *supervised person* may demonstrate that it has assessed the risk that a *business relationship* or *one-off transaction* will involve *money laundering,* the *financing of terrorism,* or the *financing of proliferation* where it takes into account the effect of a combination of several factors – e.g. the use of complex structures by a *customer* who is a non-resident high-net worth individual making use of wealth management services – which may increase the cumulative level of risk beyond the sum of each individual risk element. The **accumulation of risk** is itself a factor to take into account.

56. Notwithstanding the above, where it is appropriate to do so, a *supervised person* may demonstrate that it has assessed the risk that a *business relationship* or *one-off transaction* will involve *money laundering,* the *financing of terrorism,* or the *financing of proliferation* where it assesses that risk "generically" for *customers* falling into similar categories. For example:

- the business of some *supervised persons*, their products, and *customer* base, can be relatively simple, involving few products, with most *customers* falling into similar risk categories. In such circumstances a simple approach, building on the risk that the *supervised person's* products are assessed to present, may be appropriate for most *customers*, with the focus being on those *customers* who fall outside the norm

- other *supervised persons* may have a greater volume of business, but large numbers of their *customers* may be predominantly "retail", served through delivery channels that offer the possibility of adopting a standardised approach to many procedures. Here too, the approach for most *customers* may be relatively straight forward - building on product risk

- in the case of Jersey residents seeking to establish retail relationships, and in the absence of any information to indicate otherwise, such *customers* may be considered to present a lower risk.

3.3.4.1 Factors to consider

57. **Country Risk** – A connection to a country or territory that presents a higher risk of money laundering, the financing of terrorism, or the financing of proliferation. The following types of countries or territories may be considered to present a higher risk:

- those with strategic deficiencies in the fight against *money laundering,* the *financing of terrorism,* and the *financing of proliferation*, e.g. those identified by the *FATF* as having strategic deficiencies

- those identified as major illicit drug producers or through which significant quantities of drugs are transited, e.g. those listed by the US Department of State in its annual International Narcotics Control Strategy Report

- those that do not take efforts to confront and eliminate human trafficking, e.g. those listed in Tier 3 of the US Department of State's annual Trafficking in Persons Report

- those that have strong links (such as funding or other support) with terrorist activities, e.g. those designated by the US Secretary of State as state sponsors of terrorism; and those physical areas identified by the US (in its annual report entitled Country Reports on Terrorism) as ungoverned, under-governed or ill-governed where terrorists are able to organise, plan, raise funds, communicate, recruit, train, transit and operate in relative security because of inadequate governance capability, political will or both

- those that are involved in the proliferation of nuclear and other weapons, e.g. those that are the subject of sanctions measures in place in Jersey, or, as appropriate, elsewhere

- those that are vulnerable to corruption, e.g. those with poor ratings in Transparency International's Corruption Perception Index or highlighted as a concern in the Worldwide Governance Indicators project, or whose companies engage in bribery when doing business abroad, e.g. those with poor ratings in Transparency International's Bribe Payers Index
- those in which there is no, or little, confidence in the rule of law, in particular the quality of contract enforcement, property rights, the police and the courts, e.g. those highlighted as a concern in the Worldwide Governance Indicators project
- those in which there is no, or little, confidence in government effectiveness, including the quality of the civil service and the degree of its independence from political pressures, e.g. those highlighted as a concern in the Worldwide Governance Indicators project
- those that are politically unstable, e.g. those highlighted as a concern in the Worldwide Governance Indicators project, or which may be considered to be a "failed state", e.g. those listed in the Failed State Index (central government is so weak or ineffective that it has little practical control over much of its territory; non-provision of public services; widespread corruption and criminality; refugees and involuntary movement of populations; sharp economic decline)
- those that are the subject of sanctions measures that are in place in Jersey or elsewhere, e.g. those dealing with the abuse of human rights of misappropriation of state funds
- those that lack transparency or which have excessive secrecy laws, e.g. those identified by the OECD as having committed to internationally agreed tax standards but which have not yet implemented those standards
- those with inadequate regulatory and supervisory standards on international cooperation and information exchange, e.g. those identified by the Financial Stability Board as just making material progress towards demonstrating sufficiently strong adherence, or being non-cooperative, where it may not be possible to investigate the provenance of funds introduced into the financial system.

58. In addition to the above, *supervised persons* should also consider whether a *customer* has a *relevant connection* to a country or territory named in Appendix D1 of this Handbook (countries or territories for which a *FATF* call for action applies), as well as those that are generally considered to be un-cooperative in the fight against *money laundering,* the *financing of terrorism,* and the *financing of proliferation*.

59. **Country risk** – A connection to a country or territory that presents a lower risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*. The following factors may be indicative of lower risk:

- a favourable rating in the Worldwide Governance Indicators project
- the application of national financial reporting standards that follow international financial reporting standards, e.g. those countries identified by the European Commission as having generally accepted accounting principles that are equivalent to International Financial Reporting Standards
- a commitment to **international export control regimes** (Missile Technology Control Regime, the Australia Group, the Nuclear Suppliers Group, Wassenaar Arrangement and the Zangger Committee)

- a favourable assessment by the Financial Stability Board concerning adherence to regulatory and supervisory standards on international cooperation and information exchange
- familiarity of a *supervised person* with a country or territory, including knowledge of its local legislation, regulations and rules, as well as the structure and extent of regulatory oversight, for example as a result of a *supervised person's* own or group operations within that country or territory.

60. **Product or Service risk** – Features that may be attractive to *money launderers* or those *financing terrorism*:
    - ability to make payments to, or receive funds from, external parties
    - ability to pay in or withdraw cash
    - ability to migrate from one product or service to another
    - use of numbered accounts (without reference to the name of the *customer*)
    - ability to use "hold mail" facilities and "care of" addresses which are not temporary arrangements
    - ability to place funds in client, pooled, nominee or other accounts, where funds are mingled with those of other persons
    - ability to place sealed parcels or sealed envelopes in safe custody boxes.
61. **Product or Service risk** – Features that may indicate a higher risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*:
    - work which is outside the *supervised person's* normal range of expertise – the *money launderer* might be targeting the *supervised person* to avoid answering too many questions
62. Instructions that are unusual in themselves or that are unusual for the *supervised person* or the *customer* may give rise to concern, particularly where no rational or logical explanation can be given. Additional service area vulnerabilities and risk factors specific to certain types of *supervised business* are set out in the sector-specific Sections 14.4, 15.3 and 16.2 below.
63. An additional Section covering the issuance of **Prepaid Cards** and their associated risks is set out as Section 3.3.6 below.
64. **Delivery risk** – Features that may be attractive to *money launderers* or those *financing terrorism*:
    - non-face to face relationships - product or service delivered exclusively by post, telephone, internet, video call etc. where there is no physical contact with the *customer*
    - indirect relationship with the *customer* - use of reliance on *obliged persons* or other third parties
    - availability of "straight-through processing" of *customer* transactions (where payments may be made electronically without the need for manual intervention by a *supervised person*).
65. **Customer-specific risk** – Features that may indicate whether a *customer* is a *money launderer* or is *financing terrorism*:
    - type of *customer*, e.g. an individual who meets any of the definitions of a *PEP* may present a higher risk

- nature and scope of business activities generating the funds/assets. The below examples may indicate higher risk:
    - a *customer* conducting "sensitive" activities (as defined by the *JFSC's* Sound Business Practice Policy) or conducting activities which are prohibited if carried on with certain countries
    - a *customer* engaged in higher risk trading activities
    - a *customer* engaged in a business which involves handling significant amounts of cash
- transparency of *customer*. For example:
    - persons that are subject to public disclosure rules, e.g. on exchanges or *regulated markets* (or majority-owned and consolidated subsidiaries of such persons), or subject to licensing by a statutory regulator, e.g. the Jersey Competition Regulatory Authority may indicate lower risk
    - *customers* where the structure or nature of the entity or relationship makes it difficult to identify the true *beneficial owners and controllers* may indicate higher risk, for example those with nominee directors, nominee shareholders or which have issued bearer shares
- behaviour by the *customer* may indicate a higher risk. For example:
    - whilst face-to-face contact with *customers* is not always necessary or possible, an excessively obstructive or secretive *customer* may be a cause for concern
    - where a customer requests undue levels of secrecy, a customer is reluctant or unwilling to provide adequate explanations or documents, or where it appears that an "audit trail" has been deliberately broken or unnecessarily layered
    - where there is no commercial rationale or logical explanation for use of the products or services that are being sought
- reputation of *customer*. For example a well-known, reputable person, with a long history in their industry, and with abundant independent and reliable information about it and its *beneficial owners and controllers* may indicate lower risk
- jurisdiction of *customer*. If the *customer* is based outside Jersey, *supervised persons* will need to consider the rationale as to why the customer is seeking services outside of their home jurisdiction. The lack of an appropriate rationale may indicate higher risk
- the regularity or duration of the *business relationship*. For example, longstanding *business relationships* involving frequent *customer* contact that result in a high level of understanding of the *customer* may indicate lower risk
- type and complexity of relationship. The below examples may indicate higher risk:
    - the use of overly complex or opaque structures with different layers of entities situated in two or more countries
    - cross-border transactions involving counterparties in different parts of the world

- the unexplained use of corporate structures and express trusts
- the use of nominee and bearer shares

› value of assets handled, e.g. higher value assets may indicate higher risk

› value and frequency of cash or other "bearer" transactions (e.g. travellers' cheques and electronic money purses), e.g. a higher value and/or frequency may indicate higher risk

› delegation of authority by the *customer*. For example, the use of powers of attorney, mixed boards and representative offices may indicate higher risk

› involvement of persons other than *beneficial owners and controllers* in the operation of a *business relationship* may indicate higher risk

› in the case of an express trust, the nature of the relationship between the settlor(s) and beneficiaries with a vested interest, other beneficiaries and persons who are the object of a power. For example, a trust that is established for the benefit of the close family of the settlor may indicate a lower risk.

3.3.4.2 External data sources

66. In assessing the risk that countries and territories may present a higher risk, objective data published by the *IMF*, *FATF*, World Bank and the Egmont Group of Financial Intelligence Units will be relevant, as will objective information published by national governments (such as the World Factbook published by the US Central Intelligence Agency) and other reliable and independent sources, such as those referred to in Section 3.3.4.1 above. Often, this information may be accessed through country or territory profiles provided on electronic subscription databases and on the internet. Some profiles, such as those available through KnowYourCountry, are free to use.

67. Information on sanctions may be found on the *JFSC's* website.

68. Appendix D2 of the *AML/CFT/CPF Handbook* lists a number of countries and territories that are identified by reliable and independent external sources as presenting a higher risk. When assessing country risk for *AML/CFT/CPF* purposes, in addition to considering the particular features of a *customer*, it will be relevant to take account of the number of occasions that a particular country or territory is listed for different reasons.

69. There are also a number of providers of country risk "league tables" that rate countries according to risk (e.g. lower, medium or higher). Some of these are free to use, e.g. KnowYourCountry and the Basel AML Index. These are based on weighted data published by external sources. Before placing reliance on country risk "league tables", care should be taken to review the methodology that has been used, including the basis followed for selecting sources, weighting applied to those sources and approach that is taken where data for a country or territory is missing.

70. External data sources may also assist in establishing *customer*-specific risk. For example, electronic subscription databases list individuals entrusted with prominent public functions who may therefore meet the definition of a *PEP*. The list of sanctions in force in Jersey may be accessed through the *JFSC's* website.

3.3.5 Customer business and risk profile – Stage 2.2

71. A *supervised person* may demonstrate that it has prepared a *customer* business and risk profile where the profile enables it to:

› identify a pattern of expected transactions and activity within each *business relationship*

› recognise unusual transactions and activity, unusually large transactions or activity, and unusual patterns of transactions or activity.

72. For certain types of products or services, a *supervised person* may demonstrate that it has prepared a *customer* business and risk profile where it does so on the basis of generic attributes, so long as this enables it to recognise the transactions and activity referred to in the above paragraph. For more complex products or services, however, tailored profiles will be necessary.

3.3.6 Prepaid cards

Overview

73. This section provides assistance to *supervised persons* issuing prepaid cards in Jersey (**issuers**), whether directly or indirectly through an agent or a distributor. It covers:
    - what electronic money is and the features of prepaid cards
    - the various operators involved in a prepaid card programme
    - examples of risk factors inherently associated with prepaid cards
    - examples of how prepaid cards have been used in Jersey by *money launderers* and
    - the relevant regulatory and supervisory framework in place in Jersey in respect of the provision of prepaid cards.

3.3.6.1 Electronic money

Overview

74. Electronic money is defined at Paragraph 5(d)(15) of the Schedule to the *Wire Transfers Regulations* as "electronically (including magnetically) stored monetary value, as represented by a claim on the issuer, which is issued on receipt of funds for the purpose of making a payment transaction, and which is accepted by a person other than the issuer of the electronic money".

75. Examples of electronic money products and services include online payment services, card-based products (including prepaid cards), vouchers and mobile payment services.

76. Monetary value will be stored in an **online account** or held on a **stored-value card** (where the value is stored on a microchip embedded in the card). Both may be reloadable or non-reloadable. A **reloadable** account or stored-value card can be recharged after the initial funds have been loaded, usually for an unlimited number of times. A **non-reloadable** account or stored-value card can be charged only once and does not permit any other funds to be added.

77. Electronic money which is card-based uses the card for authentication in order to permit a *customer* to access their funds.

78. Where electronic money is not used it can instead be redeemed. **Redemption** is a process whereby a *customer* presents electronic money to the issuer and receives money in exchange at par value. Redemption should not be confused with the spending of electronic money when a prepaid card is used for purchase of goods or services from merchants.

79. Card-based electronic money may be used in an open or closed loop system. In an **open loop system** cards may be used to purchase goods and services from any merchant or withdraw cash at ATMs operated by any merchant that is participating in the payment network. These cards provide access to the global ATM and payment network through the logo that the card is branded with (e.g. VISA, MasterCard and American Express). In a **closed loop system**, cards may be used only to purchase goods and services from a single merchant or a limited, closed network of merchants (e.g. gift cards, gift vouchers and gift certificates). These cards typically do not provide access to the global ATM network, cannot be recharged and have no "cash back" function.

3.3.6.2 What is a prepaid card?

Overview

80. Prepaid cards are a type of electronic money. The *FATF* has classified such cards as a type of New Payment Products and Services (**NPPS**). These are considered to be new and innovative payment products and services that offer an alternative to traditional financial services. Other types of NPPS include mobile payment services and internet-based payment services – these are not covered by this section.

81. Prepaid cards provide the holder with an authenticated access to pre-loaded funds. These funds can be held in an online account or on a stored-value card.

82. Prepaid cards can be utilised for a range of purposes, including transactions in other countries or territories. Some cards can be funded by cash or other electronic payment instruments and can be used for online shopping or to receive "cash back". Newer prepaid card features that are becoming increasingly common include making onward transfers of money from a prepaid card account to other accounts (known as person-to-person transfers) and setting up standing orders.

83. Prepaid cards are considered to be a retail product and are mostly used for making small value payments. Despite this, the range of functions which prepaid cards currently offer can make them attractive to criminals.

3.3.6.3 Who is involved in a prepaid card programme?

Overview

84. A number of operators are normally involved in a prepaid card programme. These include:

Operator	Description
acquirer	The person which maintains the relationship with the retailer, provides the infrastructure needed for accepting a card payment (e.g. access to the point of sale (**POS**) terminal or the payment services supporting an e-commerce website) and normally operates the account in which the proceeds of the sale transaction are deposited.
distributor/ retailer	The person that sells, provides, or arranges for the sale of, prepaid cards on behalf of the issuer to *customers*. Distributors may also offer a separate range of services to these *customers*.
payment network operator	The person that provides the technical platform to perform transactions with the card at ATMs or points of sale at merchants.
issuer	The person that issues prepaid cards and against which the customer has a claim for redemption or withdrawal of funds.

programme manager	The person responsible for establishing and managing the prepaid card programme in cooperation with a bank or electronic money institution. The programme manager usually markets the prepaid cards and establishes relationships with banks and distributors or customers, and in many cases provides the data processing capability. Some prepaid card issuers manage their card programmes themselves (i.e. without using programme managers).
agent	For the purposes of this section, the agent is any person that issues prepaid cards on behalf of the issuer (the principal), whether by contract with, or under the direction of, the principal.

85. Article 1 of the EU Electronic Money Directive 2009 (defined in this section as the **Directive**) stipulates that the activity of issuing electronic money falls within the scope of the Directive. Categories of electronic money issuers include:

    › credit institutions

    › electronic money institutions (defined in Article 2 of the Directive as a legal person that has been granted authorisation to issue electronic money) and

    › post office giro institutions.

86. An issuer will be considered to carry on a *supervised business* in or from within Jersey where it does so through a physical presence on the island or through a Jersey-based agent.

3.3.6.4 Risks associated with prepaid cards

Overview

87. The *FATF* issued a guidance paper in June 2013 regarding the application of a risk-based approach towards prepaid cards, mobile payments and internet-based payment services. This paper highlights the importance of taking a more enhanced and focused approach in areas where there are higher risks.

88. Whilst prepaid cards do not automatically present a higher risk of *money laundering*, *terrorist financing,* or *proliferation financing*, issuers will need to consider the specific risk factors of each card issued and determine its risk assessment based on the same. The risk of a prepaid card being misused will also depend on the product design and use and the effectiveness of systems and controls (including policies and procedures). Issuers are expected to exercise greater caution and **apply *enhanced CDD measures*** in instances where there is a **greater** *money laundering, financing of terrorism,* or *financing of proliferation* risk or where a product is designed and used in a way that is similar to a bank account.

89. The risk assessment of a prepaid card issuer will need to cover all relevant risk factors (e.g. *customer* profile, product design and functionalities, geographical location of main card funding and card spending activities).

Guidance notes

90. Prepaid cards are mostly used for making small value payments and transactions. They leave an audit trail in the system, unlike cash transactions. However, if certain risk factors are not adequately or effectively managed and mitigated, prepaid cards can become attractive or susceptible to *money launderers*, *terrorist financiers* or *proliferators* of weapons of mass destruction.

91. The risk factors listed below do not constitute an exhaustive list and should not be considered in isolation. An accumulation of multiple risk factors will increase the overall risk level – such an accumulation is often seen in cases where prepaid cards have been used to facilitate criminal activities.

- Prepaid cards are **portable** and easily transported **cross-border**. The current definition of cash and bearer negotiable instruments in the Customs and Excise (Jersey) Law 1999 does not extend to prepaid cards and there is no requirement to report mailing or shipping such cards abroad. Furthermore, it can be difficult for law enforcement, customs or border guards to determine and potentially seize the monetary value stored on a prepaid card. This is particularly relevant when prepaid cards have high load limits and are used to transport the proceeds of criminal activities
- Ownership of the card may be transferred to an **unidentified bearer** (i.e. from the customer to another person)
- Prepaid cards may be purchased, and funds loaded, reloaded, redeemed, or withdrawn on a **non-face-to-face basis**
- Prepaid cards may be **funded by cash** which could be the proceeds of criminal activity. Cards also provide **access to cash** by way of ATMs, "**cash back**" functionality or redemption
- Prepaid cards may **be funded by unidentified third parties** and by other electronic products
- The card may have a **high transaction limit** or **no transaction limit** at all. Prepaid cards that allow high values to be loaded, have high or no transaction value limits and high or no transaction frequency limits increase the risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*
- Individual customers or groups of customers may hold, have access to, or control **multiple cards**. Multiple cards can be transported or sent across borders in an attempt to circumvent the usual controls of cross-border cash movements
- Prepaid cards may be used to make **frequent or high value cross-border transactions** by allowing customers to use funds loaded on their cards to be transferred onwards to other persons (person to person or business to business transfers)
- Most prepaid card programmes involve a number of agents which may be based in several different countries and territories. As a result of this segmentation there may be a **lack of consistent *CDD* measures** being applied across the issuer's business
- Prepaid card operators typically outsource business and compliance functions to overseas locations, where the legislation may not necessarily follow international standards.

3.3.6.5 Case Study – Use of prepaid cards to launder the proceeds of crime

Guidance notes

92. Prepaid currency cards have been used by individuals in Jersey to launder the proceeds of drug trafficking. For example, prosecutions in 2013 were connected with the laundering of criminal proceeds, amounting to £157,000, in Jersey through foreign currency exchange operators and through multiple loadings of criminal funds onto prepaid cards. In the case of the latter method, funds loaded locally were then withdrawn overseas, over a period of 34 months.

93. Evidence demonstrated that individuals hired by the drug dealer were asked to "bank" the proceeds of illicit drugs sales by obtaining prepaid cards (two individuals held two cards each in their own names), loading cash onto these prepaid cards in Jersey, and subsequently withdrawing these funds in the UK and Spain.

94. This case shows that criminals will exploit the different functionalities offered by prepaid cards. The ability to obtain multiple cards and load them with third party cash, the portability of such cards, and the ability to withdraw cash abroad have proved attractive to criminals.

3.3.6.6 Regulatory framework – prudential and conduct of business

Overview

95. There is currently no prudential or conduct of business regime in place in Jersey covering prepaid card issuers. However, in certain circumstances it is possible that prepaid card activity may fall within other regulatory regimes established, for example under the *BB(J) Law* (deposit-taking) or the *FS(J) Law* (where funds loaded on to a card are held by a card issuer in a trustee capacity).

3.3.6.7 Regulatory Framework – AML/CFT/CPF

Overview

96. The activity of issuing prepaid cards is listed in Paragraph 7(1)(e) of Part B of Schedule 2 to the *Proceeds of Crime Law*: "issuing and administering means of payment (such as credit and debit cards, cheques, travellers' cheques, money orders and bankers' drafts, and electronic money)".

97. As a result, any person issuing electronic money (including prepaid cards) in or from within Jersey (directly or through an agent) or through a legal person established under Jersey law:

- becomes a *supervised person* for the purposes of the *Money Laundering Order* and is required to apply *CDD* measures, keep records, appoint an *MLCO* and *MLRO*, and to have *policies and procedures* in place to prevent and detect *money laundering,* the *financing of terrorism,* and the *financing of proliferation*
- is required to register with the *JFSC* under the *Supervisory Bodies Law* or, where the person carries on a *regulated business* as defined in the *Supervisory Bodies Law*, to notify the *JFSC* that it is issuing prepaid cards and
- is subject to supervision by the JFSC under the Supervisory Bodies Law for compliance with the Money Laundering Order and AML/CFT/CPF Codes of Practice.

98. The *Money Laundering Order* therefore **applies to prepaid card issuers with no physical presence in Jersey** that issue cards through Jersey-based agents.

99. The *Money Laundering Order* does not provide for the application of simplified identification measures to prepaid card *customers*. Prepaid card issuers are required to apply *CDD* measures to each *customer* and each third party on whose behalf the *customer* acts.

100. Where a *business relationship* is established with a *customer*, a prepaid card issuer is required to monitor *customer* transactions undertaken throughout the course of that *business relationship*.

101. By virtue of Article 2(3) of the *EU Regulation*, payment cards (among other methods of transfer) are exempt from the scope of the *Wire Transfers Regulations* where they are used exclusively for the purchase of goods or services and the number of the card accompanies all transfers. However, Article 2(3) of the *EU Regulation* also states that the use of a payment card in order to effect a person-to-person transfer of funds falls within the scope of the *EU Regulation*.

102. This means that where they satisfy the conditions set out in Article 2(3) of the *EU Regulation*, a person carrying on activities listed in Paragraph 7(1)(e) of Part B of Schedule 2 to the *Proceeds of Crime Law* is exempt from the obligation to include information on the payer in a wire transfer.

3.4 On-going monitoring: ensuring that documents, data and information are up to date and remain relevant

Overview

103. Article 3(3)(b) of the *Money Laundering Order* explains that on-going monitoring includes ensuring that documents, data or information obtained under *identification measures* are kept up-to-date and relevant by undertaking reviews of existing records, particularly in relation to higher risk categories of *customers*, including reviews where any inconsistency has been disclosed as a result of scrutiny.

104. Among other things, where there is a change to information found out about the *customer*, the *customer* acts for a new third party, a new person purports to act for the *customer*, or the *customer* has a new *beneficial owner or controller*, Article 13(1)(c)(ii) of the *Money Laundering Order* requires that the identity of that person is found out and evidence obtained.

Guidance notes

105. A *supervised person* may demonstrate that documents, data or information obtained under *identification measures* are kept up-to-date and relevant under Article 3(3)(b) of the *Money Laundering Order* where the *customer* is requested to, and does provide, an assurance that they will update the information provided on a timely basis in the event of a subsequent change.

106. A *supervised person* may demonstrate that documents, data and information obtained under *identification measures* are kept up-to-date and relevant under Article 3(3)(b) of the *Money Laundering Order* where they are reviewed on a risk-sensitive basis, including where additional "factors to consider" occur which may impact the *customer* business and risk profile.

107. Trigger events, e.g. the opening of a new account, the purchase of a further product or a meeting with a *customer*, may also present a convenient opportunity to review documents, data and information obtained under *identification measures*.

3.5 Identification measures – taking on a book of business

Overview

108. Rather than establishing a *business relationship* directly with a *customer*, a *supervised person* may establish that relationship through the transfer of a block of *customers* from another business. The transfer may be effected through legislation or with the agreement of the *customer*.

Guidance notes

109. A *supervised person* may demonstrate that it has applied *identification measures* before establishing a *business relationship* taken on through the acquisition of a book of business where each of the following criteria are met:

- the vendor is a *supervised person* or carries on *equivalent business* (refer to Section 1.8 of this Handbook)
- the *supervised person* has concluded that the vendor's *CDD policies and procedures* are satisfactory. This assessment must either involve sample testing or alternatively an assessment of all relevant documents, data or information for the *business relationship* to be acquired
- before, or at the time of the transfer, the *supervised person* obtains from the vendor all of the relevant documents, data or information (or copy thereof) held for each *customer* acquired.

110. In cases where:

- the vendor is not a supervised person; **or**
- the vendor is not carrying on equivalent business (refer to Section 1.8 of this Handbook); **and**
- deficiencies are identified in the vendor's CDD policies and procedures (either at the time of transfer or subsequently)

a *supervised person* may demonstrate that it has applied *identification measures* before establishing a *business relationship* where it determines and implements a programme to apply *identification measures* on each *customer* and remediate any deficiencies, provided the programme is agreed in advance with the *JFSC*.

4 IDENTIFICATION MEASURES – FINDING OUT IDENTITY AND OBTAINING EVIDENCE

4.1 Overview of section

1. The purpose of this section of the *AML/CFT/CPF Handbook* is to explain what **information** on identity is to be found out when establishing a *business relationship* or carrying out a *one-off transaction* (or otherwise under Article 13 of the *Money Laundering Order*), and what **evidence** is to be obtained that is reasonably capable of verifying that the person to be identified is who they are said to be and satisfies a *supervised person* of the same.
2. This section does not address the information that must also be collected under Article 3(5) of the Money Laundering Order as part of *identification measures* in order to assess the risk that any *business relationship* or *one-off transaction* will involve *money laundering,* the *financing of terrorism,* or the *financing of proliferation*, which is covered by Stage 1.4 in Section 3.3 of this Handbook. Nor does it address the enhanced measures that will be required in order to address the case of a *customer* that is assessed as presenting a higher risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*, which is covered in Section 7.
3. Guidance is also given on the timing of obtaining evidence of identity and what to do where it is not possible to complete *identification measures*. This guidance covers all elements of *identification measures*, including, where appropriate, the collection of information under Article 3(5) of the *Money Laundering Order*.
4. The requirement to find out identity and obtain evidence (part of the *identification measures* referred to in Article 3 of the *Money Laundering Order*) applies:
   - at the outset of a business relationship or one-off transaction
   - where there is suspicion of money laundering, or the financing of terrorism
   - where there is some doubt as to the veracity or adequacy of documents, data or information that are already held (including the circumstances set out in Paragraph 5 below)
   - in respect of “existing customers”.
5. As stated in Section 3.4 of this Handbook, the requirement to find out identity and obtain evidence will also apply when there are changes, for example a:
   - change in information found out for a customer, e.g. a change of name or change of nationality
   - change in beneficial ownership and control of a customer
   - change in a third party (or parties), or *beneficial ownership or control* of a third party (or parties) on whose behalf a *customer* acts.
6. A customer may be an individual (or group of individuals) or a legal person. Section 4.3 deals with a customer who is an individual (or group of individuals), Section 4.4 deals with a customer (an individual or a legal person) who is acting for a legal arrangement, e.g. the trustee of an express trust, and Section 4.5 deals with a customer who is a legal person.
7. The term *customer* is defined in the Glossary above.

4.2 Obligation to find out identity and obtain evidence

Overview

8. Determining that a *customer* is the person they claim to be is a combination of being satisfied that:

   › a **person exists** - on the basis of information found out and

   › the *customer* **is that person** - by collecting from reliable and independent sources (documents, data or information), satisfactory confirmatory evidence of appropriate components of the *customer's* identity.

9. Evidence of identity can take a number of forms. In respect of individuals, identity documents (e.g. passports and national identity cards) are often the easiest way of providing evidence as to someone's identity. It is, however, possible to be satisfied as to a *customer's* identity by obtaining other forms of confirmation, including independent data sources, *E-ID* (see Section 4.3.5) and, in appropriate circumstances, written assurances from *obliged persons*.

10. When obtaining evidence of identity, a *supervised person* will need to be prepared to accept a range of documents.

Statutory requirements (paraphrased wording)

11. *Requirements for identification measures are summarised in Section 3. Among other things, identification measures must establish the persons who are concerned with a legal arrangement, and each beneficial owner and controller of a customer who is a legal person.*

12. *Under Article 3(2)(b) of the Money Laundering Order a relevant person must determine whether a customer is acting for a legal arrangement, and, if so, identify the legal arrangement.*

13. *Where a customer is acting for a legal arrangement, Article 3(2)(a) of the Money Laundering Order requires the customer, e.g. the trustee of a trust or general partner of a limited partnership, to be identified.*

14. *Article 3(2)(b)(iii) of the Money Laundering Order requires the identity of each person who falls within Article 3(7) to be found out and evidence of identity obtained, i.e.:*

    › *in the case of a trust, the settlor*

    › *in the case of a trust, the protector*

    › *having regard to risk, a person that has a beneficial interest in the legal arrangement, or who is the object of a trust power in relation to a trust*

    › *any other individual who otherwise exercises ultimate effective control over the third party.*

15. *In respect of each person falling within Article 3(7) who is not an individual, Article 3(2)(b)(iii) requires each individual who is that person's beneficial owner or controller to be identified.*

4.3 Obligation to find out identity and obtain evidence: individuals

Overview

16. The following paragraphs apply to situations where an individual is the *customer* or where the *customer* is more than one individual, such as spouses opening a joint account.

17. The provisions also apply to situations where an individual is:

- a person connected to a legal arrangement, because of a requirement in Article 3(2)(b)(iii) to identify each person who falls within Article 3(7) of the *Money Laundering Order*, and each individual who is that person's *beneficial owner or controller*
- the *beneficial owner or controller* of a *customer*, because of a requirement in Article 3(2)(c)(iii) of the *Money Laundering Order* to identify the individuals who are the *customer's beneficial owners or controllers*
- acting on behalf of a *customer* (e.g. is acting according to a power of attorney, or has signing authority over an account) because of a requirement in Article 3(2)(aa) of the *Money Laundering Order* or
- a third party on whose behalf a *customer* is acting, because of a requirement in Article 3(2)(b)(ii) of the *Money Laundering Order* to identify the individuals who are the third party's *beneficial owners or controllers*.

4.3.1 Finding out identity

Guidance notes

18. A *supervised person* may demonstrate that it has found out the identity of an individual who is a *customer* under Article 3(2)(a) of the *Money Laundering Order* where it collects all of the following:

- legal name, name(s) currently used, any former legal name(s), and name(s) formerly used
- principal residential address
- date of birth
- place of birth
- nationality
- gender identity and
- government issued personal identification number or other government issued unique identifier.

19. However, in the case of a **lower risk relationship**, a *supervised person* may demonstrate that it has found out the identity of an individual who is a *customer* under Article 3(2)(a) of the *Money Laundering Order* where it collects all of the following:

- legal name, any former legal name(s), and any other name(s) used
- principal residential address
- date of birth.

4.3.2 Obtaining evidence of identity

Overview

20. Evidence of identity may come from a number of sources, including one or more of the following:

- original documents (see Section 4.3.2);
- certified copies of documents (see Section 4.3.3);
- external data sources (see Section 4.3.4); and/or
- *E-ID* (see Section 4.3.5).

21. These sources may differ in their integrity, reliability and independence. For example, some identification documents are issued after due diligence on an individual's identity has been undertaken (e.g. passports and national identity cards). Others are issued on request, without any such checks being carried out. Furthermore, some documents are more easily forged than others. For E-ID applications, the technology used may not sufficiently mitigate the inherent risks associated with it. Therefore, a supervised person will need to ensure that its CDD systems and controls incorporate measures specifically designed to do so – see Section 4.3.5.
22. Additionally, documents incorporating photographic confirmation of *customer* identity provide a higher level of assurance that an individual is the person they claim to be.
23. Where a *supervised person* is not familiar with the form of evidence obtained, appropriate additional measures may be necessary to become satisfied that the evidence is genuine.
24. Where evidence of identity obtained subsequently expires, e.g. a passport, national identity card, or driving licence, it is not necessary to obtain further evidence under identification measures set out in Article 13 of the Money Laundering Order. However, a supervised person should keep in mind that updated evidence of identity may need to be requested at, for example, a trigger event or an increase in the level of money laundering/terrorist financing/proliferation financing risk (see Section 3.4 of this Handbook for more detail).

AML/CFT/CPF Codes of Practice

25. All key documents (or parts thereof) obtained as evidence of identity must be understandable (i.e. in a language understood by an employee of the *supervised person*), and must be translated into English at the request of the *JFCU* or the *JFSC*.

Guidance notes

26. A *supervised person* may demonstrate that it has **obtained evidence** under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that an individual to be identified is who they are said to be where that evidence covers the following components of identity and, where documentary evidence of identity is exclusively relied upon, uses at least **two** sources of evidence (see Paragraph 28):
    - legal name and name(s) currently used
    - principal residential address
    - date of birth
    - place of birth
    - nationality and
    - passport or national identity number.

27. However, in the case of a **lower risk relationship**, a *supervised person* may demonstrate that it has obtained evidence that is reasonably capable of verifying under Article 3(2)(a) of the *Money Laundering Order* that an individual to be identified is who they are said to be where that evidence covers the following components, using at least **one** source of evidence (see Paragraph 28):

- legal name and other names used and
- principal residential address (or, as an alternative, date of birth).

For the avoidance of doubt, this paragraph may be applied to *customers* who are resident outside of Jersey.

28. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that an individual to be identified is who they are said to be where that evidence is one of the following documents:

All elements of identity
› a current passport or copy of such a passport certified by a suitable certifier - providing photographic evidence of identity › a current national identity card or copy of such national identity card certified by a suitable certifier - providing photographic evidence of identity or › a current driving licence or copy of such driving licence certified by a suitable certifier - providing photographic evidence of identity - where the licensing authority carries out a check on the holder's identity before issuing.
Residential address:
› correspondence from a central or local government department or agency (e.g. States and parish authorities) › a letter of introduction confirming residential address from: o a *supervised person* that is regulated by the *JFSC* o a person carrying on a *supervised business* which is regulated and operates in a well-regulated country or territory or o a branch or subsidiary of a group headquartered in a well-regulated country or territory which applies group standards to subsidiaries and branches worldwide, and tests the application of and compliance with such standards › a bank statement or utility bill or › a tenancy contract or agreement.

29. However, in the case of a **lower risk relationship** with a *customer* who is **resident in Jersey**, a *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that an individual to be identified is who they are said to be where that evidence is a:

- jersey driving licence **or**
- birth certificate, in conjunction with:
  - a bank statement or
  - a utility bill or
  - a document issued by a government source or
  - a letter of introduction from a supervised person that is regulated by the JFSC.

30. A *supervised person* may also demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that an individual to be identified is who they are said to be where the data or information comes from an independent data source (see Section 4.3.4) or, in the case of a residential address, personal visit to that address.
31. Where an individual's residential address changes, a supervised person may demonstrate that it has obtained evidence under Article 3(2)(a) of the Money Laundering Order that is reasonably capable of verifying that an individual to be identified is who they are said to be where the data or information is collected through on-going correspondence with that customer at the changed address.
32. A *supervised person* may demonstrate that a country or territory is well-regulated for the purpose of a letter of introduction, where it has regard to:
    - the development and standing of the country or territory's regulatory framework
    - recent independent assessments of its regulatory environment, such as those conducted and published by the *IMF,* the *FATF* and other FATF-Style Regional Bodies.

4.3.2.1 Electronic bank statements and utility bills

Overview

33. It is now common for statements and utility bills to be delivered by e-mail or made available via an online portal (an **electronic statement**).
34. Common types of electronic statement include, but are not limited to;
    - a bank statement bearing the name and residential address of the individual
    - a bill for rates, council tax or utilities bearing the name and residential address of the individual.

Statutory requirements (paraphrased wording)

35. *Article 3(2)(a) of the Money Laundering Order states that identification measures are for identifying the customer.*
36. *Article 3(4)(b) of the Money Laundering Order states that for the purposes of Article 3(2), identification of a person includes obtaining evidence, on the basis of documents, data or information from a reliable and independent source, that is reasonably capable of verifying that the person to be identified is who they are said to be and satisfies the person responsible for the identification of a person that the evidence does establish that fact.*

Guidance notes

37. A *supervised person* wishing to accept an electronic statement as evidence of an individual's residential address is required to satisfy itself, through the application of a risk-based approach, that the document presented is sufficient to meet the requirements of Article 3(4)(b) of the *Money Laundering Order*.

38. A *supervised person* is also required to satisfy itself that the acceptance of an electronic statement is commensurate with the risk profile of its *customer*. For example, the use of an electronic statement alone may not be appropriate for a *customer* assessed as higher risk.

39. A *supervised person* should also consider that some types of electronic statement may be more susceptible than others to being stolen, intercepted, tampered with or otherwise amended, for example, a document sent by e-mail without any encryption.

40. If a *supervised person* becomes concerned regarding the integrity of an electronic statement, for example, if it becomes unsure whether a utility bill has been generated by the named utility company, the *supervised person* should take appropriate additional steps to seek to corroborate the validity of the document. Examples may include:

    › the use of an independent data source (see Section 4.3.4 below) to corroborate the address information. This may be achieved by using a third party database like a credit agency or an electoral roll. The additional corroboration should be sufficient to give the *supervised person* comfort as to the accuracy of the information contained within the electronic statement

    › requesting sight of the delivery mechanism (such as sight of or access to the customer portal, details of the document download or e-mail received) to the *customer* from the bank/utility provider, in which the document was attached

    › a telephone call to the provider of the electronic statement which is corroborated by an independent source to verify such provider exists.

41. If it is concluded that an electronic statement is not appropriate, such as in the case of a *supervised person* who is, or becomes, concerned or suspicious of the validity/authenticity of the electronic statement, an alternative form of residential address will need to be obtained.

42. Consideration should be given to whether concerns regarding the integrity of the electronic statement warrant a SAR.

4.3.3 Suitable certification

Overview

43. Suitable certification is a process where, rather than requesting a person to present evidence of identity directly to a *supervised person*, the person is called on to present themselves to a *suitable certifier* along with original documentation that supports that person's identity (and is current), specifically for the purpose of entering into a *business relationship* or *one-off transaction* with a *supervised person*. The effect of this is to create an environment in which *identification measures* in respect of a *customer* (or other person) are applied through a trusted external party and where the *customer* (or other person) is physically present.

44. *Suitable certification* is **not to be confused** with a case where a *supervised person* uses Article 16 of the *Money Laundering Order* - which allows **reliance** to be placed on *reliance identification measures* that have already been completed by an *obliged person* where evidence of identity that may subsequently be provided by that *obliged person* may now be out of date, and where the *obliged person* has a continuing responsibility to the *supervised person* in respect of record-keeping and access to records – in which case Section 5 is relevant.

45. **Nor** should the provisions in Section 4.4.5 and Section 4.5.7 for copy documentation to be provided by a **supervised *Trust and Company Services Provider*** be confused with ***suitable certification***.

Guidance notes

46. For *suitable certification* to be effective, an individual will need to personally present an original document to an acceptable *suitable certifier* who is subject to professional rules (or equivalent) providing for the integrity of the certifier's conduct.

47. Acceptable persons to certify evidence of identity (*suitable certifiers*) may include:

- a member of the judiciary, a senior civil servant, or a serving police or customs officer
- an officer of an embassy, consulate or high commission of the country of issue of documentary evidence of identity
- an individual who is a member of a professional body that sets and enforces ethical standards, for example an Advocate or Solicitor
- an individual that is qualified to undertake certification services under authority of the Certification and International Trade Committee (in Jersey this service is available through the Jersey Chamber of Commerce)
- a director, officer, or manager of either:
    - a person carrying on a financial services business which is regulated and operates in a well-regulated country or territory or
    - a branch or subsidiary of a group headquartered in a well-regulated country or territory which applies group standards to subsidiaries and branches worldwide, and tests the application of and compliance with such standards.

48. In determining whether a country or territory is well-regulated, a *supervised person* may have regard to:

- the development and standing of the country or territory's regulatory framework and
- recent independent assessments of its regulatory environment, such as those conducted and published by the IMF, the FATF and other *FSRBs*.

49. Best efforts should be exercised to secure a certified copy of photographic evidence of identity that is of adequate quality, e.g. the photograph is clear and any text is legible.

50. A higher level of assurance will be provided where the relationship between the certifier and the subject is of a professional rather than personal nature. A person **cannot** be a *suitable certifier* if they are:

- related to the person being identified by birth or marriage

› in a relationship or living with the person being identified.

Guidance notes

51. A *suitable certification* may take the following forms:

› a hand-written certification which meets the criteria as described in paragraphs 52 and 53; or

› an electronic certification which is produced using software as described in paragraph 54.

52. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a person to be identified is who they are said to be when it:

› obtains a true copy, signed and dated by the *suitable certifier*, of a document that is accompanied by the **confirmation** set out in Paragraph 58 and **adequate information** as set out in Paragraph 60 so that they may be contacted in the event of a query.

53. On a risk-based approach – for example where the *suitable certifier* is connected to a higher risk country or territory, based in a different country or territory to that of the person to be identified, or there is reason to believe that certification may not be effective – the *supervised person* should take additional steps in line with Paragraph 61 to **validate** the credentials of the suitable certifier.

54. **Electronic/digital signature** software is available that locks a certification into a pdf, or a similar file type, which cannot be tampered with. A *supervised person* must be aware of and comfortable with the reliability of the software used. The electronic/digital signature solution must lock the certification into the document in order for it to be acceptable.

    Article 9A of the Electronic Communications (Jersey) Law 2000 (the Electronic Communications Law) provides that a signature, seal, attestation or notarisation is not to be denied legal effect, validity or enforceability only because it is in electronic form.

55. Therefore, the certification does not need to be a handwritten signature on a document. It can be an electronic/digital signature which is technologically attached to the document. Article 9C(2) of the Electronic Communications Law provides that a person (Person A) may authorise another person to attach Person A's electronic signature to the document on Person A's behalf. It may not, however, simply be an electronic image/photocopy placed on that document (for example a handwritten signature copied onto a document (electronically or physically).

56. In the case of the affixation of an electronic signature to certify a document, we would expect that the suitable certifier is in receipt of the relevant original documentation (as described in 4.3.2) or an electronic statement. The suitable certifier may then produce an electronic copy of such original document and affix their electronic signature in line with the detail provided in Paragraphs 54 and 55. This would create an electronically-certified document.

57. It is not a requirement for a document which has been electronically certified to be received directly from the certifier.

58. The **confirmation** should state that the copy of the document is a true copy of an original document (or extract thereof) that includes information on the identity and/or residential address of an individual.

59. In a case where the document to be certified relates to a legal arrangement or legal person, then the *guidance notes* in this section apply, except that the documents to be certified will be those that provide evidence of identity of that arrangement or person.

60. An **adequate level of information** to be provided by a *suitable certifier* will include their name, position or capacity, their address and a telephone number, or email address, at which they can be contacted. This applies regardless of what method of certification is used.

61. The additional steps to be taken to **validate** the credentials of the *suitable certifier* may include considering factors such as:

- the stature and track record of the *suitable certifier*
- previous experience of accepting certifications from *suitable certifiers* in that profession or country or territory
- the adequacy of the framework to counter *money laundering,* the *financing of terrorism,* and the *financing of proliferation* in place in the country or territory in which the *suitable certifier* is located and
- the extent to which that framework applies to the *suitable certifier*.

4.3.3.1 Certification methods not considered to be suitable certification

Guidance notes

62. The following methods of certification **are not** considered to be *suitable certification*:

- "certification" of documents where the original document has not been presented to the suitable certifier;
- certification which does not include the **confirmation** set out in Paragraph 58 and **adequate information** as set out in Paragraph 60;
- certification which includes an image or photograph affixed to a document which is not an electronic signature as described within Paragraphs 54 and 55;
- production, viewing and screenshotting of documentation during a video call is not an appropriate method of certification due to:
    - the risk of 'deep fake' technology being utilised, whereby the video image and voice of an individual can be manipulated to look and sound like another individual. Biometric and similar matching/checking technology is considered necessary for this risk to be adequately mitigated.

63. The *JFSC* considers that certification by a *suitable certifier*, in line with the guidance set out at Section 4.3.3, provides assurances as to the authenticity of the document which the above-referenced methods are not able to do.

4.3.4 Obtaining Evidence of Identity – Independent Data Sources

Overview

64. Independent data sources can provide a wide range of confirmatory material on the identity of a *customer* and can be accessible, for example, through publically available information (such as registers of electors and telephone directories - to the extent permitted by data protection legislation) and commercially available data sources such as those provided by data services providers, e.g. credit reference agencies and business information service providers.

65. Where a *supervised person* is seeking to obtain reliable and independent evidence of identity using an independent data source, whether by accessing the source directly or by using a data services provider, an understanding of the depth, breadth and quality of the data or information is important in order to determine that the source does in fact provide satisfactory evidence of identity and that the process of obtaining evidence is sufficiently robust to be relied upon.

Guidance notes

66. A supervised person may demonstrate that it is satisfied that data or information it has accessed directly from data source(s) is sufficiently extensive, reliable and accurate under Article 3(2)(a) of the *Money Laundering Order* where:

- the source, scope and quality of the data or information accessed are understood
- the supervised person uses positive data or information source(s) that can be called upon to link a customer to both current and historical data and information and
- processes allow the *supervised person* to capture and record the data or information.

67. A *supervised person* may demonstrate that it is satisfied that data or information supplied by a data service provider is sufficiently extensive, reliable and accurate where:

- it understands the basis of the system used by the data service provider and is satisfied that the system is sufficiently robust, including knowing what checks have been carried out, knowing what the results of these checks were, and being able to determine the level of satisfaction provided by those checks
- the data services provider is registered with a data protection authority in Jersey, the *EEA*, or a country or territory that has similar data protection provisions to the *EEA*, e.g. Guernsey and the Isle of Man
- the data services provider either:
    - Accesses:
        - a range of positive data or information sources that can be called upon to link a customer to both current and historical data and information
        - negative data and information sources such as databases relating to fraud and deceased persons
        - a wide range of alert data sources
- or otherwise ensures that its source(s) are sufficiently extensive, reliable and accurate.
- processes allow the *supervised person* to capture and record the data information.

4.3.5 Use of electronic identification (E-ID)

Overview

68. With the ongoing development of remote working and circumstances where *customers* are not physically present, *supervised persons* are increasingly making use of smart phone and tablet applications to capture information, copy documents and take images, liveness checks (including micro streaming) or video recordings of *customers* as part of their *CDD* processes (defined in this Handbook as *E-ID*). this section will provide guidance and (where relevant) set out *AML/CFT/CPF Codes of Practice* in respect of:

- the relevant legal and regulatory obligations in relation to CDD
- the relevant legal and regulatory obligations in relation to new and developing technologies, outsourcing and customers who are not physically present
- risk factors inherently associated with the use of E-ID applications
- examples of risk mitigants to consider when assessing the potential use of a particular E-ID method or application and
- examples of practices or methods which are not considered to be *E-ID*.

69. The FATF has issued guidance on Digital Identity, March 2020 which *supervised persons* may find useful in developing their own procedures and controls.

70. The guidance in this section may also be relevant in situations where similar processes are undertaken but carried out through means other than smart phone and tablet applications, e.g. the use of self-service kiosks with similar document and image capturing and verification technology.

71. In order to adequately consider the risks associated with *E-ID*, the *supervised person's* Board/senior management should clearly identify, fully understand and document what the *E-ID* application does and does not do. For example:

- is it to be used only to collect information about an individual (finding out identity)?
- is it to be used to obtain evidence of that individual's identity?
- is it to be used to collect more general relationship information about an individual from that individual, e.g. source of funds?
- is it to be used to collect information about an individual from reliable and independent data sources? If so, where do these data sources originate and have they been assessed as to their reliability and/or independence?

72. Where it is identified that an *E-ID* application does not cover particular elements of *identification measures* (or more general *CDD* measures) then, in line with Article 13 of the *Money Laundering Order*, those elements should continue to be applied using a *supervised person's* existing *systems and controls* (including *policies and procedures*). For example, a *supervised person* could decide to use an *E-ID* application to find out and evidence identity, whilst, at the same time, employ a more traditional method to establish and verify a *customer's* address.

73. The *JFSC* is aware that a range of *E-ID* applications are commercially available for use by *supervised persons*. *Supervised persons* might also make use of *E-ID* applications which have been developed in-house or within their wider corporate group. The guidance provided in this section is not intended to express any preference or favour towards any particular method of *E-ID,* or any particular *E-ID* application. The *JFSC* does not endorse nor advise on specific methods or providers available to *supervised persons*. It remains the decision of the *supervised person* whether *E-ID* should be utilised in any given circumstance, and/or whether the *supervised person* will develop its own *E-ID* application for these purposes, or select an *E-ID* application that is commercially available. This choice may be determined, for example, based on the *supervised person's customer* base and how the *supervised person* conducts its business.

4.3.5.1 Legal and regulatory obligations relevant to E-ID

Statutory requirements (paraphrased wording)

74. *Article 3(4) of the Money Laundering Order explains that identification of a person means:*

- ***finding out the identity*** *of that person, including that person's name and legal status and*
- ***obtaining evidence*** *on the basis of documents, data or information from a reliable and independent source, that is reasonably capable of verifying that the person to be identified is who they are said to be, and satisfies the person responsible for the identification that the evidence does establish that fact.*

Overview

75. Using an *E-ID* application is one way of obtaining evidence of identity. Section 4.3.2 of this Handbook explains how a *supervised person* may demonstrate that it has **obtained evidence** that is reasonably capable of verifying that an individual to be identified is who they are said to be. Among other things, it states that use of the following documentary evidence will be reasonably capable of verifying an individual's identity:

- a current passport, or copy of such a passport certified by a suitable certifier
- a current national identity card, or copy of such a national identity card certified by a suitable certifier or
- a current driving licence, or copy of such a driving licence certified by a suitable certifier.

76. As an alternative to using documentary evidence, Section 4.3.4 of this Handbook permits, in certain circumstances, the use of **independent data sources** to verify that the person to be identified is who they are said to be. In practice, it may be possible to demonstrate compliance with Article 3(4) of the *Money Laundering Order* through a combination of documentary evidence and independent data sources.

77. A *supervised person* may use other tools and/or methods (including *E-ID* applications) to undertake *CDD* measures, so long as such methods comply with Article 3(4) of the *Money Laundering Order*.

Statutory requirements (paraphrased wording)

78. *Article 11 of the Money Laundering Order requires a relevant person to have policies and procedures for the identification and assessment of risks that arise in relation to the use of new or developing technologies for new or existing products or services.*

79. *Article 15(1)(b) of the Money Laundering Order requires a relevant person to apply enhanced CDD measures when the customer has not been physically present for identification purposes.*

Guidance notes

80. The requirements under Articles 11 and 15(3) of the *Money Laundering Order* and the *AML/CFT/CPF Codes of Practice* set out at Section 2.4.4 will apply in any circumstances where a part of the *CDD* process is undertaken by an independent third party or *supervised person* via the use of *E-ID* applications, where the *customer* is not physically present. Accordingly, when deciding whether to make use of a particular *E-ID* application, a *supervised person* is required to undertake a risk assessment comprising of the following:

- consider the risks involved in the use of the E-ID application and record the reasons why its use is appropriate
- consider the risks involved in outsourcing any part of the *CDD* process to an independent third party using the *E-ID* application and record the reasons why such outsourcing is appropriate
- consider whether the features of the *E-ID* application effectively mitigate the risks identified
- apply any additional measures to ensure that all risks are effectively managed
- apply, on a risk-sensitive basis, *enhanced CDD measures* to take account of the particular risks arising due to the fact that the *customer* has not been physically present for identification purposes.

81. A risk assessment as described in the paragraph above is not required to be undertaken by the *supervised person* on each occasion that the particular *E-ID* application is used, but rather when considering whether to incorporate the use of that *E-ID* application into its *CDD* measures.

82. When using technology to on-board a *customer* remotely, i.e. when a customer is not physically present, and conduct activities by digital or other non-physical present means, for example when interacting via a video call, mail or telephone, it is required that *enhanced CDD measures* be applied.

83. The approval by a *supervised person* of the use of one *E-ID* application should not be taken to constitute approval of the use of all *E-ID* applications. It is a requirement that each *E-ID* application be risk-assessed separately and on its own merits.

84. The *supervised person* is required to ensure that adequate and effective *policies and procedures* are in place to support the use of the *E-ID* application, and are catering for the technology that is being used, as well as for the *supervised person's* business practices.

85. The *supervised person* is required to ensure appropriate training is in place.

4.3.5.2 Risks of using E-ID

Overview

86. The use of *E-ID* applications to apply *identification measures* presents a number of inherent risks. Typically, an *E-ID* application will do one or more of the following:

- capture information, copy documents and capture an image (e.g. take a photograph) of the *customer* (for instance by way of a camera on a smart phone or tablet)

- transmit the information, documents or image (either to the supervised person or another party)
- compare the information, documents and image captured
- verify the information or documents against external data sources.

Guidance notes

87. A *supervised person* may demonstrate that it has considered the particular risks that arise when using *E-ID* applications to copy documents and take photographs for *CDD* purposes when it considers the risks set out below.

88. Risk: Documents are tampered with or forged:

- when original documents are not physically presented, it can be more difficult for a *supervised person* to detect that documents have been tampered with or forged. For example, it may be difficult to detect that another individual's photograph has been fraudulently inserted into a passport when simply viewing an electronic copy of that document.
- similarly, it may be difficult to detect the presence or absence of watermarks or other built-in security features on an identity document when simply viewing an electronic copy of the document.

89. Risk: Captured copies of documents or images are tampered with before or during transmission:

- when an electronic copy of a document or an image has been captured there may be opportunities for the *customer* (or another party) to use software to alter the copy of the document or image before transmitting it. For example, it may be possible for a *customer* to alter details (such as name and date of birth) on the copy of the passport prior to transmission. Similarly, it may be possible to use software to alter the photograph and other biometric data on a copy of an identity document.

90. Risk: Documents presented are stolen or their use unauthorised:

- when a *customer* is not physically presenting identification documents, it is more difficult for a *supervised person* to detect that the documents do not belong to the *customer*. For example, a customer may present stolen documentation when using the *E-ID* application.

91. Risk: External data sources used to verify information are not appropriate/sufficient:

- E-ID applications will often verify the information provided by a *customer* using external data sources. Those data sources may cover a specific geographical region, or a particular type of national identify documentation and may not provide full coverage over a *supervised person's* customer base.

4.3.5.3 Factors to consider when assessing E-ID applications

Overview

92. This section lists some potential features of *E-ID* applications (and wrap-around systems) that may be used to mitigate the risks listed at Section 4.3.5.2 above. Where the *E-ID* application (or connected system) does not sufficiently mitigate the risk, the *supervised person* will need to ensure that its *CDD systems and controls* (including *policies and procedures*) incorporate measures specifically designed to do so.

93. The features described in the *guidance notes* below do not represent an exhaustive list. A *supervised person* may consider other features, *systems and controls* (including *policies and procedures*) to be appropriate.

Guidance notes

94. Features of *E-ID* applications (and wrap-around systems) that may be used to mitigate the risk that documents have been tampered with or forged may include:

- the copy of the document is of a very high level of clarity and resolution, such that its contents can be adequately reviewed without undue difficulty (i.e. the clarity and resolution is still sufficient when zooming in to view a particular element of the document)
- the copy of the document is automatically matched to a pre-defined "template" for the particular form of identity document used
- the data in the main body of the document is compared to biometric or other data stored in the document's machine readable zone (MRZ) code
- data on the document is automatically examined for use of unauthorised print fonts and unexpected character spacing
- the copy of the document is automatically examined to enable detection of fraudulent documents on the basis of that documents' security features (e.g. watermarks, biographical data, photographs, lamination, UV sensitive ink lines holograms, micro-text, etc.) and the location of various elements in the document (i.e. optical character recognition).
- the copy of the document is examined by individuals specifically trained to detect tampering/forgery (e.g. ex-border agents), or the E-ID application has been designed with the characteristics of this training/expertise in mind.

95. Features of *E-ID* applications (and wrap-around systems) that may be used to mitigate the risk that a copy of a document or photograph has been tampered with or forged before or during transmission may include:

- the *E-ID* application itself controls the process of copying the document, taking photographs and transmitting the same, allowing no opportunity to tamper with or manipulate documents or photographs. This is in contrast with, for example, a prospective *customer* taking a photograph of a document and transmitting the PDF by e-mail, which presents multiple opportunities for interference
- a highly secure connection is used to transmit copies of documents and photographs
- the *E-ID* application's security is regularly tested in order to guard against hacking or other security breaches.

96. Features of *E-ID* applications (and wrap-around systems) that may be used to mitigate the risk that documents presented are stolen (or their use unauthorised) may include:

- a "selfie" photograph of the *customer* is taken **and** biometrically compared/matched to the photograph on the identity document presented, in order to verify that they relate to the same individual
- a video or a "micro-stream" of photographs is taken in order to identify facial movements, which may help to confirm that the *customer* is present at the time that the video/stream of photographs is taken. Use of anti-impersonation measures such as requiring the user to verbally repeat a word or phrase as dictated by the *supervised person* during a video or "micro-stream". This may also help to prevent the use of a video/stream of photographs which may have been stolen or use of which is unauthorised
- a code or password is sent to the *customer* who, immediately before the application of E-*ID*, is photographed while displaying the code or password - to confirm that the customer is present at the time that the photograph is taken - to avoid a photograph being taken of a photograph which may have been stolen or use of which is unauthorised
- use of location matching, where the *E-ID* application determines that information and copies of documents are captured and photographs taken at a location that is consistent with the *customer's* place (or country) of residence.
- the requirement that any image taken is adequately illuminated when using the E-ID solution.

4.3.5.4 Record-keeping requirements relevant to the use of E-ID

Guidance notes

97. Where a *supervised person* uses *E-ID* applications to capture information, copy documents and take photographs of *customers* as part of their *CDD* processes, adequate records are required to be kept in line with the record-keeping requirements set out in Part 4 of the *Money Laundering Order*.

98. Detailed *AML/CFT/CPF Codes of Practice* and *guidance notes* are provided at Section 10 of this Handbook regarding the requirements of Part 4 of the *Money Laundering Order*.

- Often E-ID systems will allow for *supervised persons* to meet these obligations by (1) providing them with access, on an ongoing basis, to the system which has verified a *customer* or (2) allowing them to download or integrate the documentary evidence which has verified a *customer* to or within their own systems. In either case, *supervised persons* should be confident that the evidence obtained from the E-ID system sets out:
    - details of the biometric checking undertaken
    - details of what third party data sources have been utilised to verify the *customer* (if any) and
    - details of the audit trail, sign-off or additional steps which have been undertaken commensurate with the risk profile of the *customer*.

4.3.5.5 Practices or methods not considered to be E-ID

Overview

99. Whilst there are a range of *E-ID* applications which incorporate features that the *JFSC* considers may allow a *supervised person* to comply with Article 3(4) of the *Money Laundering Order*, some other practices or methods are not currently deemed to sufficiently address the risks listed at Section 4.3.5.2 and are therefore **not** considered to be *E-ID*. Examples of these are set out in the guidance notes below.

100. Biometric and similar matching/checking technology is referred to in the guidance notes below. The *FATF* describes biometrics as an individual's personal biological or behavioural characteristics. *E-ID* applications may make use of the following biometrics as part of their verification processes:

- biophysical biometrics: attributes, such as fingerprints, iris patterns, voiceprints and facial recognition
- biomechanical biometrics: attributes, such as keystroke mechanics, are the product of unique interactions of an individual's muscles, skeletal system, and nervous system
- behavioural biometric patterns: attributes, based on the new computational social science discipline of social physics, consist of an individual's various patterns of movement and usage in geospatial temporal data streams, and include, for example, an individual's email or text message patterns, file access log, mobile phone usage, and geolocation patterns.

Guidance notes

101. Use of video calls where an identity document is produced during the call for comparison, but no biometric or similar matching/checking technology is employed, e.g. the *customer* just holds up their passport during a video call – this method is not considered to be appropriate due to:

- there being no independent authentication process alongside the identification document being produced, hence the process is not adequately robust.
- the risk of 'deep fake' technology being utilised, whereby the video image and voice of an individual can be manipulated to look and sound like another individual. Again, biometric and similar matching/checking technology is considered necessary for this risk to be adequately mitigated.

  Whilst a *supervised person* may wish to hold a video call in order to meet a potential customer and discuss elements of the proposed *business relationship* (including **finding out identity** or other customer information), that video call is not sufficient for the purposes of obtaining **evidence of identity**. An *E-ID* application, or other alternative method, may be used for that purpose, enabling the independent authentication process.

102. Using scanned copies of documents (i.e. re-productions of original documents which have not been suitably certified) as evidence of identity – this method is not considered to be appropriate due to:

- the risk that an identity document has been tampered with or forged not being mitigated through the use of specialist checks. The scanned copies in this case are in effect non-certified and non-authenticated. If scanned copies are to be used as evidence, they should be independently verified/authenticated. That verification process may include, for example,

the use of third party data sources or the use of an *E-ID* application in instances when such technology utilises automated verification technology in a robust and appropriate way. It may, for example, verify data embedded in the scanned document (barcodes, micro-lettering etc.).

103. Using a "selfie" photograph of the *customer* **without** it being biometrically compared/matched to the photograph on the identity document presented in order to verify that they relate to the same individual, e.g. the *customer* just takes a "selfie" photograph of themselves holding up their passport – this method is not considered to be appropriate due to:

- the risk that an identity document has been tampered with or forged not being mitigated through the use of specialist checks.

  If, however, such a "selfie" photograph is being uploaded to an *E-ID* application which then undertakes authenticity checks to verify identity, for example by extracting machine-readable text or hologram data, and verifying the data in an appropriate, independent way to ensure it is robust, then this is an acceptable method to evidence identity.

4.3.6 Guarding against the financial exclusion of Jersey residents

Overview

104. On occasions, an individual may be unable to provide evidence of identity using the sources set out at Section 4.3.2. Examples of such individuals may include:

- seasonal workers whose principal residential address is not in Jersey
- individuals living in Jersey in accommodation provided by their employer, with family, or in care homes, who may not pay directly for utility services
- Jersey students living in university, college, school, or shared accommodation, who may not pay directly for utility services
- minors.

AML/CFT/CPF Codes of Practice

105. A *supervised person* must determine that there is a valid reason for a *customer* being unable to provide more usual sources of evidence of identity, and must document that reason.

Guidance notes

106. In the case of a lower risk minor, whose parent or guardian is unable to produce more usual evidence of identity for the minor, and who would otherwise be excluded from accessing financial services, a *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a person to be identified is who they are said to be where that evidence is:

- the minor's birth certificate
- a letter from the parent or guardian confirming their status (i.e. "I am the parent or guardian of [name of minor]") and the residential address of the minor.

107. In the case of a lower risk individual who is resident in a Jersey nursing home or residential home for the elderly and has a valid reason for being unable to produce more usual evidence of identity, and would otherwise be excluded from accessing financial services, a *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a person to be identified is who they are said to be where that evidence is a letter from a Jersey nursing home or residential home for the elderly, which a *supervised person* is satisfied that it can place reliance on, confirming the identity of the resident.

108. In other cases, where a lower risk individual has a valid reason for being unable to produce more usual evidence of identity, and would otherwise be excluded from accessing financial services, a *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* of residential address that is reasonably capable of verifying that a person to be identified is who they are said to be where that evidence is:

- a letter from a Jersey employer, which a *supervised person* is satisfied that it can place reliance on, that confirms residence of an individual at a stated Jersey address, and, in the case of a seasonal worker, indicates the expected duration of employment and gives the worker's principal residential address in their country of origin
- a letter from the head of household at which the individual resides confirming that the individual lives at that Jersey address, setting out the relationship between the *customer* and the head of household, together with evidence that the head of household resides at the address or
- a letter from a principal of a university or college, which a *supervised person* is satisfied that it can place reliance on, that confirms residence of the individual at a stated address. In the case of a Jersey student studying outside the Island, a residential address in Jersey should also be collected.

109. Confirmatory letters should be written on appropriately headed paper.

4.3.7 Residential Address: Overseas Residents

Overview

110. On occasions, an individual that resides abroad may be unable to provide evidence of their principal residential address using the sources set out at Section 4.3.2. Examples include residents of countries without postal deliveries and few street addresses, who rely upon post office boxes or employers for delivery of mail, and residents of countries where, due to social restraints, evidence of a private address may not be obtained through a personal visit.

111. It is essential for law enforcement purposes that a record of an individual's residential address (or details of how that individual's place of residence may be reached) be recorded. As a result, it is not acceptable to only record a post office box number as an address.

AML/CFT/CPF Codes of Practice

112. A *supervised person* must determine that there is a valid reason for a *customer* being unable to provide more usual sources of evidence for an address and must document that reason.

113. Where alternative methods to obtain evidence for an address are relied on, a *supervised person* must consider whether enhanced monitoring of activity and transactions is appropriate.

Guidance notes

114. Where an individual has a valid reason for being unable to produce more usual evidence for a residential address, a *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a person to be identified is who they are said to be where it receives written confirmation from an individual satisfying the criteria for a *suitable certifier* that they have visited the individual at that address.

115. Where an individual has a valid reason for being unable to produce more usual evidence for a residential address, a *supervised person* may demonstrate that it has found out the identity of that person under Article 3(2)(a) of the *Money Laundering Order* where, in addition to principal residential address, it collects a "locator" address. In such a case, a *supervised person* may demonstrate that it has obtained evidence that is reasonably capable of verifying that a person to be identified is who they are said to be where it obtains evidence that the individual may normally be met or contacted at that address.

116. A "locator" address is an address at which it would normally be possible to physically meet or contact an individual (with or without prior arrangement), for example, an individual's place of work.

4.4 Obligation to find out Identity and obtain evidence: Legal Arrangements

Overview

117. Jersey law recognises two distinct forms of legal arrangement: the trust and the limited partnership.

118. Jersey trusts law comprises both the Trusts (Jersey) Law 1984, as amended and the Jersey customary law of trusts. Limited partnerships are established under the Limited Partnerships (Jersey) Law 1994. Limited Liability Partnerships, Separate Limited Partnerships and Incorporated Limited Partnerships all have legal personality and are therefore covered in Section 4.5.

119. There are a wide variety of trusts ranging from large, nationally and internationally active organisations subject to a high degree of public scrutiny and transparency, through to trusts set up under testamentary arrangements or established for wealth management purposes. Trusts may also be established as collective investment schemes – known as a *unit* trusts.

120. A legal arrangement cannot form a *business relationship* or carry out a *one-off transaction* itself. It is the trustee(s) of the trust or general partner(s) of the limited partnership who will enter into a *business relationship* or carry out the *one-off transaction* with a *supervised person* on behalf of the legal arrangement and who will be considered to be the *customer(s)*. In line with Article 3 of the Money Laundering Order, the trust or limited partnership will be considered to be the third party on whose behalf the trustee(s) or general partner(s) act(s).

121. In forming a *business relationship* or carrying out a *one-off transaction* with a trustee or general partner, a *supervised person* will be dependent on information provided by the trustee or general partner (a *supervised trust company business* or otherwise) relating to the legal arrangement and persons concerned with the legal arrangement (set out in Article 3(7) of the Money Laundering Order). When determining the risk assessment for a legal arrangement (Section 3.3), the risk factors set out in Section 3.3.4.1 and Section 7.15.1 will be relevant in deciding whether it is appropriate to use information provided by the trustee or general partner. In addition, the monitoring measures maintained by a *supervised person* (Section 6) may provide additional comfort that relevant and up to date information on identity has been found out.

122. In the case of a *unit* trust which is a third party, individual investors into the *unit* trust are not considered to be settlors for the purpose of Article 3(7)(a). However the investors may in certain circumstances be considered *beneficial owners and controllers* and are *customers* of the Fund (see Section 13).

123. The following provisions apply to situations where a trustee of an express trust or general partner of a limited partnership is the *customer* of a *supervised person*. Sector-specific sections for *trust company business* and funds and fund operators explain the *identification measures* to be applied by a trustee or general partner itself in respect of the legal arrangement. See Section 12 and Section 13.

124. The provisions will also assist with the identification of ultimate *beneficial owners and controllers* and will be relevant in situations where a legal arrangement (through the trustee or general partner) is:

- the owner or controller of a customer, because of a requirement in Article 3(2)(c)(iii) of the Money Laundering Order to identify the individuals who are the customer's beneficial owners or controllers or
- a third party on whose behalf a customer is acting, because of a requirement in Article 3(2)(b)(ii) of the Money Laundering Order to identify the individuals who are the third party's beneficial owners or controllers.

125. Where the trustee or general partner is a *supervised person* carrying on *regulated business* or is a person who carries on *equivalent business* to any category of *regulated business*, it may be possible to apply *CDD* exemptions under Article 17B and Article 18(3) of the *Money Laundering Order*. See Section 7 of this Handbook.

126. The measures that must be applied by a *supervised person* where a third party is a trust need not include a settlor of a trust who is deceased.

127. The measures that must be applied to obtain evidence of identity of **beneficiaries** and persons **who are the object of a power** and have been identified as **presenting higher risk** will necessarily reflect the verification methods that are available at a particular time to the trustee. For example, it may not be appropriate to request evidence directly from the beneficiary or object of a power.

128. Where a *supervised person* is not familiar with the form of evidence of identity obtained to verify identity, appropriate measures may be necessary to satisfy itself that the evidence is genuine.

129. Notwithstanding the requirement to find out identity and obtain evidence of identity in relation to the trustee, the trust and those individuals listed in Article 3(7) of the Money Laundering Order, a *supervised person* is not expected to collect information on the detailed terms of the trust, nor rights of the beneficiaries.

4.4.1 Finding out identity – Legal arrangement that is a trust

Guidance notes

130. A *supervised person* may demonstrate that it has found out the identity of a trust which is a third party under Article 3(2)(b)(i) of the *Money Laundering Order* where it collects all of the following components of identity:

- name of trust
- date of establishment
- official identification number (e.g. tax identification number or registered charity or non-profit organisation number)
- mailing address of trustee(s).

131. A *supervised person* may demonstrate that it has found out the identity of the settlor of a trust which is a third party under Article 3(2)(b)(iii)(B) of the *Money Laundering Order* where it finds out the identity of:

- the settlor (including any persons subsequently settling funds into the trust)
- any person who directly or indirectly provides trust property or makes a testamentary disposition on trust or to the trust and
- any other person exercising **ultimate effective control** over the trust, for example, a protector.

132. This information may be provided by the trustee.

133. A *supervised person* may demonstrate that it has found out the identity of persons having a beneficial interest in a trust (other than a *unit* trust) which is a third party under Article 3(2)(b)(iii)(B) of the *Money Laundering Order* where it finds out the identity of each beneficiary with a vested right. This information may be provided by the trustee.

134. A *supervised person* may demonstrate that it has found out the identity of persons having a **beneficial interest** in a trust (other than a *unit* trust) which is a third party under Article 3(2)(b)(iii)(B) of the *Money Laundering Order* where it finds out the identity of each beneficiary who has been identified as presenting higher risk. This information may be provided by the trustee.

135. A *supervised person* may demonstrate that it has found out the identity of persons having a **beneficial interest** in a *unit* trust (for example a Jersey Private Fund) which is a third party under Article 3(2)(b)(iii)(B) of the *Money Laundering Order* where, having regard to risk, it finds out the identity of investors holding a material interest in the capital of the *unit* trust. This information may be provided by the trustee.

136. A *supervised person* may demonstrate that it has found out the identity of persons who are the **object of a trust power** in a trust which is a third party under Article 3(2)(b)(iii)(B) of the *Money Laundering Order* where it finds out the identity of each person who is the **object of a power** and has been identified as **presenting higher risk**. This information may be provided by the trustee.

137. A *supervised person* may demonstrate that it has found out the identity of any other person who otherwise exercises **ultimate effective control** over the third party under Article 3(2)(b)(iii)(B) of the *Money Laundering Order* where it finds out the identity of each co-trustee. This information may be provided by the trustee.

138. In any case where a settlor, protector, beneficiary, object of a power, or other person referred to in paragraphs 131 to 137 (the "person") is not an individual, a *supervised person* may demonstrate that it has identified each individual who is the person's *beneficial owner or controller* under Article 3(2)(b)(iii)(C) of the *Money Laundering Order* where it has identified:

    i) **each** individual with a **material controlling ownership interest** in the capital of the person (through direct or indirect holdings of interests or voting rights) or who exerts **control through other ownership means**

    ii) **to** the extent that there is doubt as to whether the individuals exercising control through ownership are *beneficial owners*, or where no individual exerts control through ownership, any other individual exercising **control** over the person **through other means.** This effectively means that anyone exercising control through ownership and anyone exercising control through other means must be ascertained

    iii) where no individual is otherwise identified under sub-paragraphs (i) and (ii) above, individuals who exercise **control** of the person **through positions held** (e.g. those who have and exercise strategic decision-taking powers or have and exercise executive control through senior management positions).

    Refer to the flow-chart at Section 4.5.1 for a graphical explanation of the process described in the paragraph above.

139. For lower risk relationships, a general threshold of 25% is considered to indicate a **material controlling ownership interest** in capital. Where the distribution of interests is uneven, the percentage where effective control may be exercised (a material interest) may be less than 25% when the distribution of other interests is taken into account, i.e. interests of less than 25% may be material interests.

4.4.2 Obtaining Evidence of Identity – Legal Arrangement that is a Trust

AML/CFT/CPF Codes of Practice

140. All key documents (or parts thereof) obtained as evidence of identity must be understandable (i.e. in a language understood by an employee of the *supervised person*), and must be translated into English at the request of the *JFCU* or the *JFSC*.

141. A *supervised person* must obtain evidence that any person purporting to act as the trustee of a trust which is a third party has authority to act in such capacity.

Guidance notes

142. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(b)(i) of the Money Laundering Order that is reasonably capable of verifying that a trust which is a third party to be identified is what it is said to be where the evidence covers the following components of identity:

- name of trust
- date of establishment
- date of appointment of the trustee

› nature of the trustee's powers.

This need not involve a review of an existing trust instrument (or similar instrument) as a whole – reviewing or obtaining copies of relevant extracts of a trust instrument may suffice.

4.4.3 Finding out identity – Legal Arrangement that is a Limited Partnership

Guidance notes

143. A *supervised person* may demonstrate that it has found out the identity of a limited partnership which is a third party under Article 3(2)(b)(i) of the *Money Laundering Order* where it collects all of the following:

› name of partnership

› any trading names

› date and country/territory of registration/establishment

› official identification number

› registered office/business address

› mailing address (if different)

› principal place of business/operations (if different)

› names of all general partners and those limited partners that participate in management (if any).

144. A *supervised person* may demonstrate that it has found out the identity of a person who has a **beneficial interest** in a limited partnership which is a third party under Article 3(2)(b)(iii)(B) of the Money Laundering Order where it finds out the identity of limited partners holding a **material controlling ownership interest** in the capital of the partnership (through direct or indirect holdings of interests or voting rights) or any other person **exercising control through other ownership means**, e.g. partnership agreements, power to appoint senior management, or any outstanding debt that is convertible into voting rights.

145. To the extent that there is doubt as to whether the persons exercising control through ownership are *beneficial owners*, or where no person exerts control through ownership, a *supervised person* may demonstrate that it has found out the identity of a person who has a **beneficial interest** in a limited partnership which is a third party under Article 3(2)(b)(iii)(B) of the Money Laundering Order where it finds out the identity of those who exercise **control through other means**, e.g. those who exert control through personal connections, by participating in financing, because of close family relationships, historical or contractual associations or as a result of default on certain payments.

146. Where no person is otherwise identified under this section, a *supervised person* may demonstrate that it has found out the identity of a person who has a **beneficial interest** in a limited partnership which is a third party under Article 3(2)(b)(iii)(B) of the Money Laundering Order where it finds out the identity of persons who **exercise control through positions held** (e.g. those who have and exercise strategic decision-making powers or have and exercise executive control through senior management positions, e.g. general partner or limited partner that participates in management). This information may be provided by the general partner.

147. In any case where a partner (including a general partner) or other person referred to in paragraph 144 to 146 is not an individual, a *supervised person* may demonstrate that it has identified each individual who is that person's *beneficial owner or controller* under Article 3(2)(b)(iii)(C) of the Money Laundering Order where it has identified:

    i) each individual with a **material controlling ownership interest** in the capital of the partnership (through direct or indirect holdings of interests or voting rights) or who exerts control of the partnership through other ownership means

    ii) to the extent that there is doubt as to whether the individuals exercising control through ownership are *beneficial owners*, or where no individual exerts control through ownership, any other individual **exercising control** over the partnership **through other means.** This effectively means anyone exercising control through ownership and anyone exercising control through other means must be ascertained

    iii) where no individual is otherwise identified under sub-paragraphs (i) and (ii), individuals who **exercise control** of the partnership **through positions held** (e.g. those who have and exercise strategic decision-taking powers or have and exercise executive control through senior management positions).

    Refer to the flow-chart at Section 4.5.1 for a graphical explanation of the process described in the paragraph above.

148. In the case of a lower risk relationship, partners who have and exercise authority to operate a *business relationship* or *one-off transaction* will be considered to be individuals who **exercise control through positions held**.

149. For lower risk relationships, a general threshold of 25% is considered to indicate a **material controlling ownership interest** in the capital of a limited partnership. Where the distribution of interests is uneven the percentage where effective control may be exercised (a material interest) may be less than 25% when the distribution of other interests is taken into account, i.e. interests of less than 25% may be material interests.

4.4.4 Obtaining Evidence of Identity – Legal Arrangement that is a Limited Partnership

AML/CFT/CPF Codes of Practice

150. All key documents (or parts thereof) obtained as evidence of identity must be understandable (i.e. in a language understood by an employee of the *supervised person*), and must be translated into English at the request of the *JFCU* or the *JFSC*.

151. A *supervised person* must obtain evidence that any person purporting to act as general partner of a partnership which is a third party has authority to act in such capacity.

Guidance notes

152. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(b)(i) of the Money Laundering Order that is reasonably capable of verifying that a limited partnership which is a third party to be identified is what it is said to be where the evidence covers all of the following components of identity:

- name of partnership
- date and country/territory of registration/establishment
- official identification number
- registered office/business address
- principal place of business/operations (if different).

153. However, in the case of a lower risk relationship, a *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(b)(i) of the Money Laundering Order that is reasonably capable of verifying that a limited partnership which is a third party to be identified is what it is said to be where the evidence covers the following components of identity:

- name of partnership
- date and country/territory of registration/establishment
- official identification number.

154. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(b)(i) of the Money Laundering Order that is reasonably capable of verifying that a limited partnership which is a third party to be identified is what it is said to be where it obtains, in every case, the partnership agreement or a copy of such an agreement certified by a suitable certifier and one or more sources of further evidence (one source for lower risk customers):

- certificate of registration (where a partnership is registered) or copy of such a certificate certified by a suitable certifier
- latest audited financial statements or copy of such statements certified by a suitable certifier.

155. A *supervised person* may also demonstrate that it has obtained evidence under Article 3(2)(b)(i) of the Money Laundering Order that is reasonably capable of verifying that a partnership which is a third party is what it is said to be where the data or information comes from an independent data source (see *guidance notes* at Section 4.3.4) or (in the case of a principal place of business) personal visit to that address. An independent data source may include a registry search, which confirms that the partnership is not in the process of being dissolved, struck off, wound up or terminated.

156. Where a partner holds their role by virtue of their employment by (or position in) a business that is a *supervised* Jersey trust and company services provider, a *supervised person* may demonstrate that it has taken reasonable measures to find out the identity of that person and to obtain evidence under Article 3(2)(b)(iii)(B) of the Money Laundering Order where it obtains the following:

- the full name of the partner
- an assurance from the trust and company services provider that the individual is an officer or employee.

4.4.5 Copy documentation provided by regulated trust and company services provider

Guidance notes

157. Where information is provided by a trust and company service provider that is regulated by the *JFSC*, the Guernsey Financial Services Commission or the Isle of Man Financial Services Authority (referred to in this section as "a regulated trust and company services provider") on a person listed in Article 3(7) of the *Money Laundering Order* (following an assessment of risk in line with Paragraph 121), a *supervised person* may demonstrate that it has taken reasonable measures to obtain evidence of identity for that person under Article 13 of the *Money Laundering Order* where it obtains a copy of a document that is listed in Paragraph 28 from the *regulated trust and company services provider*, along with the confirmations set out in the paragraph below.

158. The confirmations to be obtained are that:

- the *regulated trust and company services provider* has seen the original document that it has copied to the *supervised person*, or the document that has been copied to the *supervised person* was provided to the *regulated trust and company services provider* by a suitable certifier, or the evidential report copied to the supervised person has been obtained by the *regulated trust and company services provider* as a result of utilising an E-ID system which meets the requirements of this Handbook,
- the *regulated trust and company services provider* is satisfied that the original document seen, or document provided to it by a suitable certifier, or documentary evidence permissible within an E-ID system, provides evidence that the individual is who they are said to be and
- the document provided to the supervised person is a true copy of a document (or evidential report) that is held by the *regulated trust and company services* provider.

159. This will be different to a case where a *supervised person* decides to make use of Article 16 of the Money Laundering Order - which allows reliance to be placed on *reliance identification measures* that have already been completed by an *obliged person* where evidence of identity may be held by the *obliged person*, and where the *obliged person* has a continuing responsibility to the *supervised person* in respect of record-keeping and access to records - see Section 5 of this Handbook.

160. In both cases, the risk of placing reliance on another person to have carried out *identification measures* must be considered – either as part of an assessment of *customer* risk under Article 13, or assessment of risk under Article 16 of the Money Laundering Order.

161. Nor should provision for copy documentation to be provided by a *regulated trust and company services provider* be confused with "suitable certification", which is explained in Section 4.3.3.

162. For the avoidance of doubt this is a very limited provision applying to *regulated trust and company services providers* and does not extend to other types of *supervised business*.

4.5 Obligation to find out identity and obtain evidence: Legal Persons

Overview

163. Jersey law recognises a number of distinct forms of legal person, in particular:

- companies, established under the Companies Law
- foundations, established under the Foundations Law
- limited liability partnerships, established under the Limited Liability Partnerships (Jersey) Law 2017
- separate limited partnerships, established under the Separate Limited Partnerships (Jersey) Law 2011
- incorporated limited partnerships, established under the Incorporated Limited Partnerships (Jersey) Law 2011.
- limited liability companies, established under the Limited Liability Companies (Jersey) Law 2018.

164. The following provisions apply to situations where a legal person is the *customer*.

165. The provisions will also assist with the identification of ultimate *beneficial owners and controllers* and will be relevant in situations where a legal person is:

- a person connected to a legal arrangement, because of a requirement in Article 3(2)(b)(iii) to identify each person who falls within Article 3(7) of the Money Laundering Order, and each individual who is that person's *beneficial owner or controller*
- the owner or controller of a *customer*, because of a requirement in Article 3(2)(c)(iii) of the Money Laundering Order to identify the individuals who are the *customer's beneficial owners or controllers*;
- acting on behalf of a *customer* (e.g. is acting according to a power of attorney, or has signing authority over an account)
- a third party on whose behalf a *customer* is acting, because of a requirement in Article 3(2)(b)(ii) of the Money Laundering Order to identify the individuals who are the third party's *beneficial owners or controllers*.

166. The Companies Law allows for the incorporation of cell companies: *ICCs* and *PCCs*. Each of these types of cell companies may establish one or more cells.

167. In the case of a *PCC*, each cell, despite having its own memorandum of association, shareholders and directors, as well as being treated for the purposes of the Companies Law as if it were a company, does not have a legal personality separate from the cell company. Accordingly, where a cell wishes to contract with another party, it does so through the cell company acting on its behalf. In order to ensure that creditors and third parties are aware of this position, a director of the cell company is under a duty to notify the counterparties to a transaction that the cell company is acting in respect of a particular cell.

168. Where a *supervised person* establishes a *business relationship* or enters into a *one-off transaction* with a cell of a *PCC*, because the cell does not have the ability to enter into arrangements or contract in its own name, for the purposes of Article 3 of the Money Laundering Order, the *PCC* will be taken to be a *customer* acting for a third party and the particular cell will be taken to be the third party that is a person other than an individual.

169. By contrast, in the case of an *ICC*, each cell has its own separate legal personality, with the ability to enter into arrangements or contracts and to hold assets and liabilities in its own name. Where a *supervised person* establishes a *business relationship* or enters into a *one-off transaction* with a cell of an *ICC*, the cell will be taken to be the *customer*.

170. In a case where the ownership structure of a legal person to be identified ("Legal Person A") includes other legal persons, the *beneficial owners and controllers* of Legal Person A will include those individuals **ultimately** holding a **material controlling ownership interest** in Legal Person A.

171. The *identification measures* to be applied to each type of person are set out in this Handbook as follows:

- a company: Sections 4.5.1 and 4.5.2
- a foundation: Sections 4.5.3 and 4.5.4.
- a partnership: Sections 4.5.5 and 4.5.6.

172. For the purpose of this section, provisions that are said to apply to a company are to be taken to apply, with appropriate modification, to:

- any other body that can establish a *business relationship* with a *supervised person* or otherwise own property
- an anstalt
- an incorporated or unincorporated association, club, society, charity, church body, or institute
- a mutual or friendly society
- a co-operative
- a provident society.

173. Where information relating to a legal person is not available from a public source, a *supervised person* will be dependent on the information that is provided by the legal person. When determining the risk assessment for a legal person (Section 3.3), the risk factors set out in Section 3.3.4.1 of this Handbook will be relevant. The risk factors set out in Section 7.15.1 will also be relevant in determining whether it is appropriate to use information on a legal person provided through, for example, a trust and company services provider. In addition, the monitoring measures maintained by a *supervised person* (Section 6) may provide additional comfort that relevant and up to date information on identity has been found out.

174. Where a director of a company holds their role by virtue of their employment by (or position in) a business that is a *supervised Jersey trust and company services provider*, separate provision is made for obtaining evidence of identity. Similar provision is made for a council member of a foundation and for a partner of a partnership.

175. Article 2 of the Money Laundering Order, which describes those persons considered to be *beneficial owners* of a body corporate or a limited liability company, provides that no individual is to be treated as a *beneficial owner* of a person that is a body corporate or a limited liability company, the securities of which are listed on a *regulated market*.

176. The measures that must be applied to obtain evidence of identity of beneficiaries and persons in whose favour the council of a foundation may exercise discretion and that have been identified as presenting higher risk will necessarily reflect the verification methods that are available at a particular time to the *supervised person*. For example, it may not be appropriate to request evidence directly from a person in whose favour discretion may be exercised.

177. Where a *supervised person* is not familiar with a document obtained to verify identity, appropriate measures may be necessary to satisfy itself that the evidence is genuine.

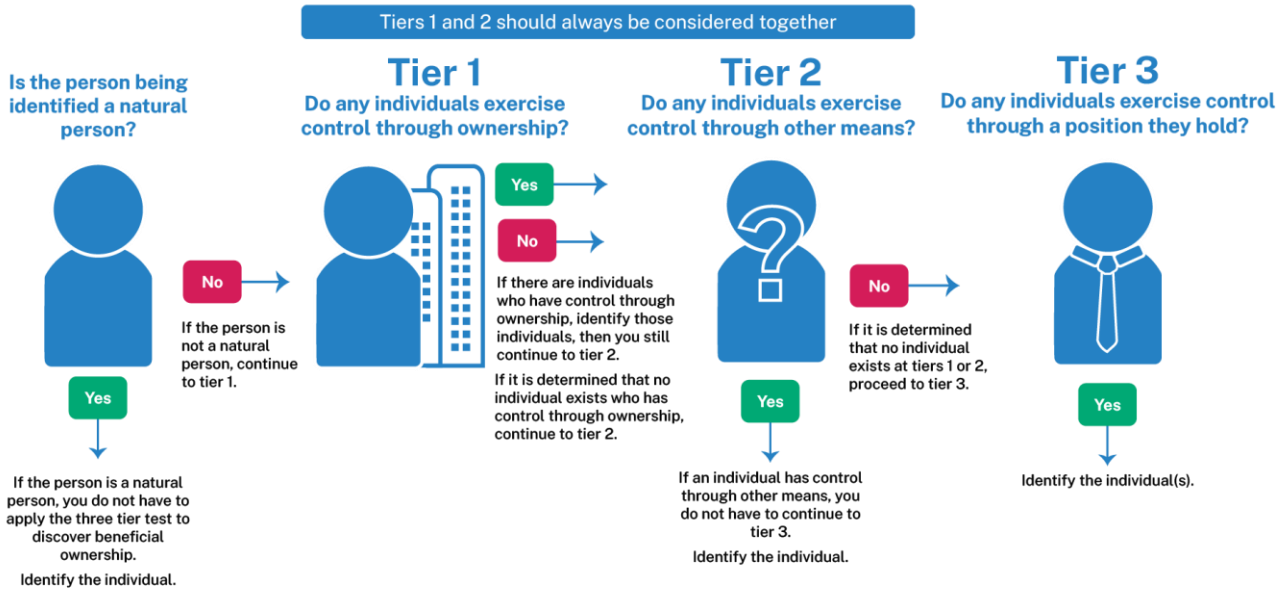
4.5.1 Finding out identity – Legal Person that is a company

Guidance notes

178. A *supervised person* may demonstrate that it has found out the identity of a company which is a *customer* under Article 3(2)(a) of the *Money Laundering Order* where it collects all of the following:

- name of company
- any trading names
- date and country/territory of incorporation/registration
- official identification number
- registered office address
- mailing address (if different)
- principal place of business/operations (if different)
- names of all persons holding a senior management position.

179. In order to ascertain whose identity must be found out i.e. who is/are the *customer's beneficial owner* or controllers under Article 3(2)(c)(iii) of the *Money Laundering Order*, a Supervised Person can use a tool that is commonly known as the "*Three Tier Test*". *The "Three Tier Test"* (explanatory text and flow-chart below) relates to legal persons (e.g. companies, incorporated partnerships etc). Individuals at tiers 1 and 2 should be identified, and only if there are no individuals at tiers 1 and 2 do the individuals at tier 3 need to be identified.



180. Tier 1: A *supervised person* may demonstrate that it has found out the identity of a person who is the *customer's beneficial owner or controller* under Article 3(2)(c)(iii) of the *Money Laundering Order* where it finds out the identity of persons holding a **material controlling ownership interest** in the capital of the company (through direct or indirect holdings of interests or voting rights) or who **exert control through other ownership interests**, e.g. shareholders' agreements, power to appoint *senior management*, or through holding convertible stock or any outstanding debt that is convertible into voting rights; and

    Tier 2: To the extent that there is doubt as to whether the persons exercising **control through ownership** are *beneficial owners*, or where no person exerts control through ownership, a *supervised person* may demonstrate that it has found out the identity of a person who is the *customer's beneficial owner or controller* under Article 3(2)(c)(iii) of the *Money Laundering Order* where it finds out the identity of those who exercise **control through other means**, e.g. those who exert control through personal connections, by participating in financing, because of close family relationships, historical or contractual associations or as a result of default on certain payments. This effectively means anyone exercising control through ownership and anyone exercising control through other means must be identified (Tier 1 and Tier 2); or

    Tier 3: Where no person is otherwise identified under Tier 1 or Tier 2 above, a *supervised person* may demonstrate that it has found out the identity of a person who is the *customer's beneficial owner or controller* under Article 3(2)(c)(iii) of the *Money Laundering Order* where it finds out the identity of persons who exercise **control through positions held** (e.g. those who have and exercise strategic decision-taking powers and exercise executive control through senior management positions). In the case of other bodies, anstalts, associations, clubs, societies, charities, church bodies, institutes, mutual or friendly societies, co-operatives and provident societies, 'senior management' will often include members of the governing body or committee plus executives.

181. The above information may be provided by the company.

182. In any case where a person identified is not an individual, a *supervised person* may demonstrate that it has identified each individual who is that person's *beneficial owner or controller* under Article 3(2)(c)(iii) of the Money Laundering Order where it has identified:

    i) each individual with a **material controlling ownership interest** in the capital of the company (through direct or indirect holdings of interests or voting rights) or who **exerts control** of the company **through other ownership means**

    ii) to the extent that there is doubt as to whether the individuals exercising control through ownership are beneficial owners, or where no individual exerts control through ownership, any other individual exercising **control** over the company **through other means.** This effectively means that anyone exercising control through ownership and anyone exercising control through other means must be identified

    iii) where no individual is otherwise identified under sub-paragraphs (i) and (ii), individuals who exercise **control** of the company **through positions held** (e.g. those who have and exercise strategic decision-taking powers and exercise executive control through senior management positions).

183. In the case of a lower risk relationship, person(s) holding a *senior management position* who have and exercise authority to operate a *business relationship* or *one-off transaction* will be those who exercise control through positions held.

184. For lower risk relationships, a general threshold of 25% is considered to indicate a **material controlling ownership interest** in the capital of a company. Where the distribution of interests is uneven, the percentage where effective control may be exercised (a material interest) may be less than 25% when the distribution of other interests is taken into account.

4.5.2 Obtaining evidence of identity – Legal person that is a company

AML/CFT/CPF Codes of Practice

185. All key documents (or parts thereof) obtained as evidence of identity must be understandable (i.e. in a language understood by an employee of the *supervised person*), and must be translated into English at the request of the *JFCU* or the *JFSC*.

Guidance notes

186. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a company which is a *customer* to be identified is who it is said to be where the evidence covers all of the following components of identity:

- name of company
- date and country/territory of incorporation/registration
- official identification number
- registered office address
- principal place of business/operations (where different to registered office).

187. However, in the case of a lower risk relationship, a *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the Money Laundering Order that is reasonably capable of verifying that a company which is a *customer* to be identified is who it is said to be where the evidence covers the following components of identity:

- name of company
- date and country/territory of incorporation/registration
- official identification number.

188. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the Money Laundering Order that is reasonably capable of verifying that a company which is a *customer* to be identified is who it is said to be where it obtains, in every case, the Memorandum and Articles of Association (or equivalent) or copy of such documents certified by a suitable certifier, and one or more sources of further evidence (one source for lower risk *customers*):

- certificate of incorporation (or other appropriate certificate of registration or licensing) or copy of such a certificate certified by a suitable certifier and/or
- latest audited financial statements or copy of such statements certified by a suitable certifier.

189. A *supervised person* may also demonstrate that it has obtained evidence under Article 3(2)(a) of the Money Laundering Order that is reasonably capable of verifying that a company which is a *customer* is who it is said to be where the data or information comes from an independent data source (see Section 4.3.4) or (in the case of a principal place of business) personal visit to that address. An independent data source may include a company registry search, which confirms that the company is not in the process of being dissolved, struck off, wound up or terminated.

190. Where a person in a senior management position holds their role by virtue of their employment by (or position in) a business that is a *supervised Jersey trust and company services provider*, a *supervised person* may demonstrate that it has taken reasonable measures to find out the identity of that person and to obtain evidence under Article 3(2)(c)(iii) of the Money Laundering Order where it obtains the following:

- the full name of the director
- an assurance from the trust and company service provider that the individual is an officer or employee.

4.5.3 Finding out identity – Legal person that is a foundation

Guidance notes

191. A *supervised person* may demonstrate that it has found out the identity of a foundation which is a *customer* under Article 3(2)(a) of the *Money Laundering Order* where it collects all of the following:

- name of foundation
- date and country/territory of incorporation
- official identification number
- business address. In the case of a foundation incorporated under the *Foundations Law*, this will be the business address of the qualified member of the council
- mailing address (if different)

- principal place of business/operations (if different)
- names of all council members and, if any decision requires the approval of any other person, the name of that person.

192. A *supervised person* may demonstrate that it has found out the identity of the foundation's *beneficial owners and controllers* under Article 3(2)(c)(iii) of the *Money Laundering Order* where it finds out the identity of:

- the founder, a person (other than the founder of the foundation) who has endowed the foundation (directly or indirectly), and, if any rights a founder of the foundation had in respect of the foundation and its assets have been assigned to some other person, that person
- the guardian (who takes such steps as are reasonable to ensure that the council of the foundation carries out its functions)
- the council members and, if any decision requires the approval of any other person, that person
- any beneficiary entitled to a benefit under the foundation in accordance with the charter or the regulations of the foundation
- any other beneficiary and person in whose favour the council may exercise discretion under the foundation in accordance with its charter or regulations and that have been identified as presenting higher risk
- any other person exercising ultimate effective control over the foundation

193. The above information may be provided by the foundation.

194. In any case where a founder, guardian, beneficiary or other person listed in paragraph 192 (the "person") is not an individual, a *supervised person* may demonstrate that it has identified each individual who is the person's *beneficial owner or controller* under Article 3(2)(c)(iii) of the Money Laundering Order where it has identified:

i) each individual with a **material controlling ownership interest** in the capital of the person (through direct or indirect holdings of interests or voting rights) or who exerts control through **other ownership means**

ii) to the extent that there is doubt as to whether the individuals exercising control through ownership are *beneficial owners*, or where no individual exerts control through ownership, any other individual exercising **control** over the person **through other means.** This effectively means that anyone exercising control through ownership and anyone exercising control through other means must be identified;

iii) where no individual is otherwise identified under sub-paragraphs (i) and (ii), individuals who exercise **control** of the person **through positions held** (e.g. those who have and exercise strategic decision-taking powers and exercise executive control through senior management positions).

Refer to the flow-chart at Section 4.5.1 for a graphical explanation of the process described in the paragraph above.

195. In the case of a lower risk relationship, as an alternative to finding out the identity of all council members (and, if any decision requires the approval of any other person, that person), a *supervised person* may find out the identity of council members who have and exercise authority to operate a *business relationship* or *one-off transaction*.

196. For lower risk relationships, a general threshold of 25% is considered to indicate a **material controlling ownership interest** in capital. Where the distribution of interests is uneven, the percentage where effective control may be exercised (a material interest) may be less than 25% when the distribution of other interests is taken into account.

4.5.4 Obtaining evidence of identity – Legal person that is a foundation

AML/CFT/CPF Codes of Practice

197. All key documents (or parts thereof) obtained as evidence of identity must be understandable (i.e. in a language understood by an employee of the *supervised person*), and must be translated into English at the request of the *JFCU* or the *JFSC*.

Guidance notes

198. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a foundation which is a customer is who it is said to be where the evidence covers all of the following components of identity:

- name of foundation
- date and country/territory of incorporation
- official identification number
- business address
- principal place of business/operations (if different).

199. However, in the case of a lower risk relationship, a *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a foundation which is a customer to be identified is who it is said to be where the evidence covers the following components of identity:

- name of foundation
- date and country/territory of incorporation
- official identification number.

200. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a foundation to be identified is who it is said to be where it obtains, in every case, the foundation Charter (or equivalent) or a copy of such document certified by a suitable certifier, and one or more sources of further evidence (one source for lower risk customers):

- latest audited financial statements or copy of such statements certified by a suitable certifier.

201. A *supervised person* may also demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a foundation which is a customer is who it is said to be where the data or information comes from an independent data source (see Section 4.3.4) or (in the case of a principal place of business) personal visit to that address. An independent data source may include a registry search on the *JFSC's* website (for the business address of the qualified member of the council).

202. Where a council member who is an individual holds their role by virtue of their employment by (or position in) a business that is a *supervised Jersey trust and company services provider*, a *supervised person* may demonstrate that it has taken reasonable measures to find out the identity of that person and to obtain evidence under Article 3(2)(c)(iii) of the *Money Laundering Order* where it obtains the following:

- the full name of the council member and
- an assurance from the trust and company services provider that the individual is an officer or employee.

4.5.5 Finding out identity – Legal Person that is a partnership

Guidance notes

203. A *supervised* person may demonstrate that it has found out the identity of a partnership which is a customer under Article 3(2)(a) of the Money Laundering Order where it collects all of the following:

- name of partnership
- any trading names
- date and country/territory of incorporation/registration
- official identification number
- registered office/business address
- mailing address (if different)
- principal place of business/operations (if different)
- names of all partners (except any limited partners that do not participate in management).

204. A *supervised person* may demonstrate that it has found out the identity of a person who is the *customer's beneficial owner or controller* under Article 3(2)(c)(iii) of the Money Laundering Order where it finds out the identity of limited partners holding a **material controlling ownership interest** in the capital of the partnership (through direct or indirect holdings of interests or voting rights) or any other person exercising **control through other ownership means**, e.g. partnership agreements, power to appoint senior management, or any outstanding debt that is convertible into voting rights.

205. To the extent that there is doubt as to whether the persons exercising control through ownership are *beneficial owners*, or where no person exerts control through ownership, a *supervised person* may demonstrate that it has found out the identity of a person who is the *customer's beneficial owner or controller* under Article 3(2)(c)(iii) of the Money Laundering Order where it finds out the identity of those who exercise **control through other means**, e.g. those who exert control through personal connections, by participating in financing, because of close family relationships, historical or contractual associations or as a result of default on certain payments. This effectively means that anyone exercising control through ownership and anyone exercising control through other means must be identified (the paragraph above and this paragraph).

206. Where no person is otherwise identified under the two paragraphs above, a *supervised person* may demonstrate that it has found out the identity of a person who is the *customer's beneficial owner or controller* under Article 3(2)(c)(iii) of the Money Laundering Order where it finds out the identity of persons who exercise **control through positions held** (e.g. those who have and exercise strategic decision-taking powers and exercise executive control through senior management positions, such as a general partner or limited partner that participates in management).

207. This information may be provided by the partnership.

208. In any case where a partner or other person referred to in paragraphs 204 to 206 is not an individual, a *supervised person* may demonstrate that it has identified each individual who is that person's *beneficial owner or controller* under Article 3(2)(c)(iii) of the Money Laundering Order where it has identified:

    i) each individual with a **material controlling ownership interest** in the capital of the partnership (through direct or indirect holdings of interests or voting rights) or who exerts **control** of the partnership **through other ownership means**

    ii) to the extent that there is doubt as to whether the individuals exercising control through ownership are beneficial owners, or where no individual exerts control through ownership, any other individual exercising **control** over the partnership **through other means.** This means that anyone exercising control through ownership and anyone exercising control through other means must be identified

    iii) where no individual is otherwise identified under sub-paragraphs (i) and (ii), individuals who **exercise control** of the partnership **through positions held** (e.g. those who have and exercise strategic decision-taking powers and exercise executive control through senior management positions).

    Refer to the flow-chart at Section 4.5.1 for a graphical explanation of the process described in the paragraph above.

209. In the case of a lower risk relationship, partners who have and exercise authority to operate a *business relationship* or *one-off transaction* will be those who exercise control through positions held.

210. For lower risk relationships, a general threshold of 25% is considered to indicate a **material controlling ownership interest** in the capital of a partnership. Where the distribution of interests is uneven, the percentage where effective control may be exercised (a material interest) may be less than 25% when the distribution of other interests is taken into account.

4.5.6 Obtaining evidence of identity – Legal person that is a partnership

AML/CFT/CPF Codes of Practice

211. All key documents (or parts thereof) obtained as evidence of identity must be understandable (i.e. in a language understood by an employee of the *supervised person*), and must be translated into English at the request of the *JFCU* or the *JFSC*.

Guidance notes

212. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the Money Laundering Order that is reasonably capable of verifying that a partnership which is a *customer* to be identified is who it is said to be where the evidence covers all of the following components of identity:

- name of partnership
- date and country/territory of incorporation/registration
- official identification number
- registered office/business address
- principal place of business/operations (if different).

213. However, in the case of a lower risk relationship, a *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the Money Laundering Order that is reasonably capable of verifying that a partnership which is a *customer* to be identified is who it is said to be where the evidence covers the following components of identity:

- name of partnership
- date and country/territory of incorporation/registration and
- official identification number.

214. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the Money Laundering Order that is reasonably capable of verifying that a partnership which is a *customer* to be identified is who it is said to be where it obtains, in every case, the Partnership agreement or a copy of such an agreement certified by a suitable certifier, and one or more sources of further evidence (one source for lower risk customers):

- certificate of registration (where a partnership is registered) or copy of such a certificate certified by a suitable certifier and/or
- latest audited financial statements or copy of such statements certified by a suitable certifier.

215. A *supervised person* may also demonstrate that it has obtained evidence that is reasonably capable of verifying that a partnership which is a *customer* is who it is said to be under Article 3(2)(a) of the Money Laundering Order where the data or information comes from an independent data source (see Section 4.3.4) or (in the case of a principal place of business) personal visit to that address. An independent data source may include a registry search, which confirms that the partnership is not in the process of being dissolved, struck off, wound up or terminated.

216. Where a partner holds their role by virtue of their employment by (or position in) a business that is a *supervised Jersey trust and company services provider*, a *supervised person* may demonstrate that it has taken reasonable measures under Article 3(2)(c)(iii) of the Money Laundering Order to find out the identity of that person and to obtain evidence where it obtains the following:

- the full name of the partner
- an assurance from the trust and company services provider that the individual is an officer or employee.

4.5.7 Copy documentation provided by regulated trust and company services provider

Guidance notes

217. Where information is provided by a trust and company service provider that is regulated by the *JFSC*, the Guernsey Financial Services Commission or the Isle of Man Financial Services Authority (referred to in this section as "a *regulated trust and company services provider*") on a person who is a beneficial owner or controller of a legal person (following an assessment of risk in line with Paragraph 173), a *supervised person* may demonstrate that it has taken reasonable measures to obtain evidence of identity for that person under Article 13 of the *Money Laundering Order* where it obtains a copy of a document that is listed in Paragraph 28 from the *supervised trust and company services provider*, along with the confirmations set out in the paragraph below.

218. The confirmations to be obtained are that:

- the *regulated trust and company services provider* has seen the original document that it has copied to the *supervised person*, or the document that has been copied to the *supervised person* was provided to the *regulated trust and company services provider* by a suitable certifier, or the evidential report copied to the supervised person has been obtained by the *regulated trust and company services provider* as a result of utilising an E-ID system which meets the requirements of this Handbook,
- the *regulated trust and company services provider* is satisfied that the original document seen, or document provided to it by a suitable certifier, or documentary evidence permissible within an E-ID system, provides evidence that the individual is who they are said to be and
- the document provided to the supervised person is a true copy of a document (or evidential report) that is held by the *regulated trust and company services* provider.

219. Alternatively, a *supervised person* may decide to make use of Article 16 of the *Money Laundering Order* - which allows reliance to be placed on *reliance identification measures* that have already been completed by an *obliged person* where evidence of identity may be held by the *obliged person*, and where the *obliged person* has a continuing responsibility to the *supervised person* in respect of record-keeping and access to records - see Section 5 of this Handbook.

220. In both cases, the risk of placing reliance on another person to have carried out *identification measures* must be considered – either as part of an assessment of *customer* risk under Article 13, or assessment of risk under Article 16 of the *Money Laundering Order*.

221. Nor should provision for copy documentation to be provided by a *regulated trust and company services provider* be confused with "suitable certification", which is explained in Section 4.3.3.

222. For the avoidance of doubt this is a very limited provision applying to *regulated trust and company services providers* and does not extend to other types of *supervised business*.

4.6 Obligation to find out identity and obtain evidence: Person purporting to act for the customer

Statutory requirements (paraphrased wording)

223. *Under Article 3(2)(aa) of the Money Laundering Order, a relevant person must identify any person purporting to act on behalf of the customer and verify the authority of any person purporting so to act.*

224. *Article 13 of the Money Laundering Order requires a relevant person to find out the identity of persons purportedly authorised to act on behalf of a customer that is a legal person and to take reasonable measures to obtain evidence of identity of such persons. This will include account signatories and those to whom powers of attorney have been granted In addition, Article 13 requires a relevant person to verify the authority of any person purporting to so act.*

225. *Article 18 of the Money Laundering Order allows this particular* identification measure *(or part of the* identification measure*) to be simplified in some limited cases.*

AML/CFT/CPF Codes of Practice

226. In a case where another person purports to act on behalf of a *customer*, a *supervised person* must obtain a copy of the power of attorney or other authority or mandate that provides the persons representing the *customer* with the right to act on its behalf.

227. In the case of a legal arrangement that is a trust, a *supervised person* must obtain evidence that any person purporting to act as the trustee has authority to act in such capacity.

228. In the case of a legal arrangement that is a limited partnership, a *supervised person* must obtain evidence that any person purporting to act as general partner has authority to act in such capacity.

Guidance notes

229. Evidence of authority to act may include:

- obtaining a certified copy of the power of attorney
- obtaining a certified copy of the limited partnership agreement or
- checking records held in the companies registry regarding the identity of the general partner

230. A *supervised person* may demonstrate that it has taken reasonable measures to obtain evidence of identity where it takes into account factors such as the risk posed by the relationship and the materiality of the authority delegated to individuals.

231. In the case of a lower risk relationship, a *supervised person* may demonstrate that it has taken reasonable measures to obtain evidence of identity where it does so for a minimum of two individuals that have purported authority to act on behalf of a customer.

4.7 Timing of Identification Measures

Statutory requirements (paraphrased wording)

Initial

232. *Article 13(1) of the Money Laundering Order requires identification measures to be applied before the establishment of a relationship or before carrying out a one-off transaction.*

233. *However, Article 13(4) of the Money Laundering Order permits evidence of identity to be obtained after the establishment of a business relationship in three cases.*

234. *The first – set out in Article 13(6) and (7) of the Money Laundering Order – is a business relationship that relates to a life insurance policy if the identification measure relates to a beneficiary under the policy and the relevant person is satisfied that there is a little risk of money laundering or the financing of terrorism occurring. Where identification measures are not completed before the establishment of a business relationship, they must be completed before any payment is made under the policy or any right vested under the policy is exercised.*

235. *The second – set out in Article 13(8) and (9) of the Money Laundering Order – is a business relationship that relates to a trust or foundation if the identification measure relates to a person who has a beneficial interest in the trust or foundation by virtue of property or income having been vested and the relevant person is satisfied that there is a little risk of money laundering or the financing of terrorism occurring. Where identification measures are not completed before the establishment of a business relationship, they must be completed before any distribution of trust property or income is made.*

236. *The third – set out in Article 13(4) of the Money Laundering Order – is where:*

- *it is necessary not to interrupt the normal course of business*
- *there is little risk of money laundering or the financing of terrorism occurring as a result of obtaining evidence of identity after establishing the relationship*
- *the risk of money laundering and the financing of terrorism is effectively managed*
- *Evidence of identity is obtained as soon as reasonably practicable.*

237. *Under Articles 11(3)(fa) and (fb) of the Money Laundering Order, policies and procedures must be in place to:*

- *assess the risk of money laundering or financing of terrorism and to manage the risks in relation to the conditions under which a customer may utilise a business relationship with the relevant person before the identification of the customer has been completed, as referred to in Article 13(4)*
- *ensure that there is periodic reporting to senior management to allow it to assess that appropriate arrangements are in place to address risk and to ensure that identification measures are completed as soon as reasonably practicable.*

During Business Relationship

238. *Article 13(1)(c)(i) of the Money Laundering Order requires a relevant person to apply identification measures where it suspects money laundering or financing of terrorism.*

239. *In addition, where a relevant person has doubts about the veracity or adequacy of documents, data or information previously obtained under customer due diligence measures, Article 13(1)(c)(ii) of the Money Laundering Order requires that person to apply identification measures.*

Existing Customers

240. *Article 13(2) of the Money Laundering Order states that, where a relevant person has a business relationship with a customer that commenced before the Money Laundering Order came into force, a relevant person must apply CDD measures that are in line with the Money Laundering Order to that relationship at appropriate times.*

241. *Article 13(3) of the Money Laundering Order states that for the purposes of Article 13(2) "appropriate times" means -*

for the application of identification measures:

- *times that are appropriate having regard to the degree of risk of money laundering or the financing of terrorism, taking into account the type of customer, business relationship, product or transaction concerned*
- *any time when a relevant person suspects money laundering or the financing of terrorism (unless agreed otherwise with the JFCU).*

242. *Article 13(3A) of the Money Laundering Order states that an appropriate time for finding out identity (as required by Article 3(4)) is a date no later than 31 December 2014, or such later date as may be agreed by the JFSC on application by relevant person on or before 31 December 2014.*

243. *Article 13(3B) of the Money Laundering Order explains that a person may be considered to have found out the identity of a customer where the information that it holds in relation to a customer is commensurate to the relevant person's assessment of risk.*

All cases

244. *Article 14(6) of the Money Laundering Order provides that a relevant person is not required to apply any identification measures if the relevant person:*

- *suspects money laundering in respect of any business relationship or transaction with a person*
- *reasonably believes that the application of identification measures is likely to alert the person to the relevant person's suspicions of money laundering*
- *has made a report under procedures maintained under Article 21 to a designated police officer or a designated customs officer*
- *acting with the consent of that officer, terminates or does not establish that business relationship or does not complete or carry out that transaction.*

Overview

245. Article 13(4) of the Money Laundering Order allows, in certain circumstances, a *supervised person* a reasonable timeframe to undertake the necessary enquiries for obtaining evidence of identity after the initial establishment of a *business relationship*. No similar concession is available for finding out identity. Where a reasonable excuse for the continued delay in obtaining evidence of identity cannot be provided, in order to comply with Article 14(2) of the *Money Laundering Order*, a *supervised person* must terminate the relationship (see Section 4.8).

246. Lawyers, Accountants and certain other professional advisers will also need to consider Sections 15.5.3 and 16.4.4, which provide sector-specific concessions for those who are in the course of ascertaining the legal position for their *customer* or performing the task of defending or representing their *customer* in legal proceedings.

247. A *business relationship* is considered to be established as soon as a *supervised person* undertakes to act in respect of that relationship, for example by receiving and accepting signed terms of business from the *customer*, or by carrying out the instructions of the *customer*, such as investing in a financial product. Funds may be received from a *customer* during the course of establishing a *business relationship*.

AML/CFT/CPF Codes of Practice

248. In a case where Article 13(4) of the *Money Laundering Order* applies, a *supervised person* may obtain evidence of identity after the initial establishment of a *business relationship* if, in addition, the following conditions are met:

- it highlights to its *customer* its obligation to terminate the *business relationship* at any time on the basis that evidence of identity is not obtained; and
- money laundering, financing of terrorism, and financing of proliferation risk is effectively managed.

249. In any event, a *supervised person* must not pay away funds to an external party, other than to invest or deposit the funds on behalf of the *customer*, until such time as evidence of identity has been obtained.

Guidance notes

250. A *supervised person* may demonstrate that it has highlighted to a *customer* the obligation to terminate a *business relationship* where terms of business, which govern its relationship with its customer:

- encompass the termination of *business relationships* when evidence of identity is either not obtained, or the results are unsatisfactory
- clearly state that termination may lead to a *customer* suffering losses – e.g. where funds have been invested in a *collective investment scheme* where a forced redemption is necessary.

251. A *supervised person* may demonstrate that *money laundering, financing of terrorism,* and *financing of proliferation* risk is effectively managed where:

- policies and procedures establish timeframes for obtaining evidence of identity
- the establishment of any *business relationship* benefiting from this concession has received appropriate authorisation, and such relationships are appropriately monitored so that evidence of identity is obtained as soon as is reasonably practicable and
- appropriate limits or prohibitions are placed on the number, type and amount of transactions over an account for such relationships.

252. A *supervised person* may demonstrate that periodic reporting is in line with Article 11(3)(fa) of the *Money Laundering Order* where it highlights to the Board:

- the number of *customers* for which evidence of identity has not been obtained during a reporting period (also expressed as a percentage of the total number of *business relationships* established during the reporting period) and summarises reasons
- in any case where the delay is for more than a particular period of time, the name of the *customer*, the reason for the delay, the extent to which evidence of identity has not been obtained, the risk rating given to that *customer*, and action that is to be taken to obtain evidence or terminate the *business relationship* (and by when).

253. Guidance as to appropriate steps to take where a *supervised person* is unable to complete *identification measures* is provided in Section 4.8 of this Handbook.

4.7.1 Timing of identification measures during business relationship – Obtaining evidence

Guidance notes

254. In the course of a *business relationship* between a *supervised person* and a *customer* that is a **trustee**, a *supervised person* may demonstrate that it has obtained evidence that is reasonably capable of verifying the identity of each beneficiary with a vested right where:
    - it does so at the time of, or before, distribution of trust property or income and
    - it is satisfied that there is little risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* occurring as a result of obtaining evidence after entitlement is conferred.
255. In the course of a *business relationship* between a *supervised person* and a *customer* that is a **trustee**, a *supervised person* may demonstrate that it has obtained evidence that is reasonably capable of verifying the identity of a beneficiary or person who is the object of a trust power where it does so at the time that the person is identified as presenting a higher risk.
256. In the case of a *business relationship* between a *supervised person* and a *customer* that is a **foundation**, a *supervised person* may demonstrate that it has obtained evidence that is reasonably capable of verifying the identity of each beneficiary entitled to benefit under the foundation where:
    - it does so at the time of, or before, distribution of property or income
    - it is satisfied that there is little risk of money laundering, the financing of terrorism, or the financing of proliferation occurring as a result of obtaining evidence after conferring entitlement.
257. In the course of a *business relationship* between a *supervised person* and a *customer* that is a **foundation**, a *supervised person* may demonstrate that it has obtained evidence that is reasonably capable of verifying the identity of any beneficiary or person in whose favour the council may exercise discretion under the foundation where it does so at the time that the person is identified as presenting a higher risk.

4.7.2 Timing for “Existing Customers”

Overview

258. *FATF Recommendation* 10 states that "financial institutions" should be required to apply that *Recommendation* (which deals with *CDD* measures) to "existing customers" on the basis of materiality and risk, and should conduct *CDD* measures on such existing relationships at appropriate times. This is based on the presumption that *identification measures* applied historically to existing customers will have been less effective than those to be applied in line with *FATF Recommendation* 10.

259. For the purposes of the Money Laundering Order the meaning of existing customer depends on the sector. In the case of a *supervised business*, this means a *business relationship* established before the *Money Laundering Order* came into force on **4 February 2008** and which continues. In the case of Estate Agents, High Value Dealers, Accountants and Lawyers this means a *business relationship* established before the *Money Laundering Order* came into force on **1 May 2008** and which continues.

260. For the avoidance of doubt, the *identification measures* (finding out identity and obtaining evidence) to be applied to existing customers include the collection of information that is necessary to assess the risk that a *business relationship* involves *money laundering* or the *financing of terrorism* (in line with Article 3(5) of the Money Laundering Order). This is likely to be self-evident for an existing customer on the basis that a *business relationship* will have been established on or before the dates stated in the sector-specific sections below. In the case of a *supervised business*, for example, this means on or before **3 February 2008**.

261. Except with the agreement of the *JFSC* (in relation to an application from the *supervised person* made on before 31 December 2014), the effect of Article 13(3A) of the *Money Laundering Order* is to require the identity of a *customer* to have been found out by 31 December 2014. There is no similar deadline for obtaining evidence of identity.

262. Once an existing relationship has been "remediated", then Article 13(1)(c)(ii) of the *Money Laundering Order* will apply to such a relationship in the same way as a relationship established on or after the dates referred to in paragraph 259 above, on the basis that documents, data or information will have been obtained under the *CDD* measures prescribed in Article 3.

263. In line with Article 13(3)(a)(ii) of the Money Laundering Order, *identification measures* must always be applied to an existing customer as soon as a *supervised person* suspects *money laundering* or the *financing of terrorism*.

264. A *supervised person* may meet its obligation to apply *identification measures* by placing reliance on an *obliged person*. See Section 5 of this Handbook.

AML/CFT/CPF Codes of Practice

265. A *supervised person* must review its "existing customer" base in order to determine a risk assessment for each customer that has still to be remediated.

Guidance notes

266. Where it does not suspect *money laundering* or the *financing of terrorism*, a *supervised person* may demonstrate that it has **found out identity** at an appropriate time for a **higher risk** existing customer where it does so at the earlier of the following dates:

- as soon as is practicable after the date that a supervised person has assessed a customer to present a higher money laundering, the financing of terrorism, or the financing of proliferation risk or
- 31 December 2014 (or later date agreed with the JFSC on application by the supervised person on or before 31 December 2014).

267. Where it does not suspect *money laundering* or the *financing of terrorism*, a *supervised person* may demonstrate that it has **found out identity** at an appropriate time for a **standard** or **lower risk** existing customer where it does so at the earlier of the following dates:

- the date when a transaction of significance takes place
- the date when a supervised person's customer documentation standards change substantially or
- 31 December 2014 (or later date agreed with the JFSC on application by the supervised person on or before 31 December 2014).

268. Where it does not suspect *money laundering* or the *financing of terrorism*, a *supervised person* may demonstrate that it has obtained **evidence of identity** at an appropriate time for an existing customer where it does so as soon as is practicable after the *customer* has been assessed as presenting a **higher risk** of *money laundering* or the *financing of terrorism*.

269. A *supervised person* may demonstrate that it has applied *identification measures* where it does so in accordance with measures applied to **new** *business relationships* and *one-off transactions*, taking into account any factors that are relevant to an existing relationship. Such factors could include existing knowledge of the *customer* built up through the historical conduct of the relationship, etc.

4.8 Failure to Complete Identification Measures

Statutory requirements (paraphrased wording)

270. *If a relevant person is unable to apply identification measures before the establishment of a business relationship or before carrying out a one-off transaction (except in the circumstances set out in Article 13(4) of the Money Laundering Order), Article 14(1) of the Money Laundering Order requires that a relevant person shall not establish that business relationship or carry out that one-off transaction.*

271. *Article 14(2) of the Money Laundering Order requires a relevant person that is unable to apply identification measures in the circumstances described in Article 13(4), to terminate the relationship.*

272. *Article 14(5) of the Money Laundering Order requires a relevant person to terminate a business relationship where it cannot apply on-going identification measures.*

273. *Article 14(7) of the Money Laundering Order states that, if a relevant person is unable to apply identification measures to an existing customer at the appropriate time, it must terminate that particular business relationship.*

274. *Article 14(11) of the Money Laundering Order provides that a business relationship or one-off transaction may proceed or continue where a relevant person is acting with the consent of the JFCU.*

Guidance notes

275. Where *identification measures* cannot be completed, a *supervised person* must not establish a *business relationship* or carry out a *one-off transaction*. In the case of an established *customer* relationship, that relationship must be terminated.

276. The timing of the termination of an established relationship will depend on the underlying nature of the *business relationship*. For example, whereas a bank can close an account relatively easily and return deposited funds to a *customer*, it may be problematic to effect a compulsory redemption of a holding of units in a *collective investment scheme*, particularly where it is closed ended, or where valuation dates are infrequent.

277. Wherever possible, when terminating a *business relationship* where *customer* money or other assets have been received, a *supervised person* should return said assets directly to the *customer*, i.e. by returning money to the account from which it was received.

278. In a case where the *customer* requests that assets or funds be transferred to an external party, or to a different account in the *customer's* name, a *supervised person* should assess whether this provides grounds for knowledge or suspicion, or reasonable grounds for knowledge or suspicion, of *money laundering* or the *financing of terrorism*.

279. Where contact has been lost with a *customer* so that it is not possible to complete termination of a *business relationship*, assets or funds held should be "blocked" or placed on a "suspense" account until such time as contact is re-established.

5 IDENTIFICATION MEASURES – RELIANCE ON OBLIGED PERSONS

5.1 Overview of section

1. In some strictly limited cases, a *supervised person* may meet its obligation to comply with Article 13(1)(a) or (c)(ii) (*CDD*); Article 15(1)(a), (b), (d), (e) or (g) (*Enhanced CDD measures*); or Article 15A (*Enhanced CDD Measures* in relation to *PEPs*) of the *Money Laundering Order*, and *AML/CFT/CPF Codes of Practice* by placing reliance on measures that have already been applied by an *obliged person* to find out the identity of a mutual *customer* and to obtain evidence of identity.
2. In order to consider what reliance might be placed on an *obliged person*, a *supervised person* will first need to determine what elements of identity must be found out and what evidence of identity is to be obtained for its *customer*. It will do so in accordance with Article 3 of the *Money Laundering Order* and the *AML/CFT/CPF Codes of Practice* set out in Sections 3, 4 and 7, and will also take into account its risk assessment for the *customer*. Once it has determined what *identification measures* it is to apply, a *supervised person* can then consider whether those measures have already been applied by an *obliged person*.
3. Where an *obliged person* has met its *customer*, who is resident in the same country or territory as the *obliged person*, the measures that it has taken to find out identity and to obtain evidence of identity will be different to the *identification measures* that must be applied by the *supervised person* in a case where the *supervised person* is resident in a different country or territory to the *obliged person* and *customer*, and where it has not met its *customer*. Even in a case where the *supervised person* and *obliged person* have met a *customer* and are resident in the same country or territory, the measures taken by the *obliged person* may still differ to those to be applied by the *supervised person* to the extent that other factors are different, for example the nature of the product or service to be provided.
4. The effect of this is that the *obliged person* may not have found out all of the same information on identity as the *supervised person* needs, and may have obtained evidence of identity using different documents, data or information. This means that, in practice, the scope to place reliance may sometimes be quite limited, and that it may be necessary for a *supervised person* to find out more information on identity and obtain evidence for that aspect of identity itself.
5. However, it is not necessary for the *obliged person* to have found out identity or obtained evidence of identity exactly in line with *policies and procedures* applied by the *supervised person*, since *guidance notes* in Section 4 provide that there are different ways in which to apply *identification measures*. Also, where the *obliged person* is outside Jersey, different requirements and guidance will be applicable.
6. Where an *obliged person* meets the requirements outlined in Article 16 of the *Money Laundering Order*, a *supervised person* is permitted to place reliance on the *obliged person* to have found out the identity and to have obtained evidence of the identity of:

› the supervised person's customer

› any beneficial owner or controller of that customer

› any third party for which that customer is acting

› any beneficial owner or controller of a third party for whom that customer is acting

› any person purporting to act on behalf of that customer.

7. It is not possible to place reliance on an *obliged person* to obtain information on the purpose and intended nature of a *business relationship* or *one-off transaction*, nor to apply on-going monitoring during a *business relationship*.

8. As noted above, overall CDD is always required to be undertaken by the supervised person. However, set out below are two tables summarising the elements of *CDD* that, in the absence of other provisions, the *supervised person* is required to undertake itself:

CDD Element	**Always required to be undertaken by the supervised person**
Identification measures	Risk assessment
	Obtain information on purpose/nature
On-going monitoring	Scrutinising transactions/activity
	Keep documents/information up-to-date

CDD Element	**Article 16(2) allows reliance upon an obliged person**	
Identification measures	ID *customer*	
	ID third parties	
	ID person acting for *customer*	Verify authority to act
	Where *customer* not individual:	Understand ownership/control structure
		ID *beneficial owners/controllers*

9. Further, Article 16 of the Money Laundering Order cannot be applied in any case where:

› a supervised person suspects money laundering or the financing of terrorism

› a *supervised person* considers that there is a higher risk of *money laundering* or the *financing of terrorism* on the basis of a risk assessment carried out under Article 16(4) of the *Money Laundering Order* (see Section 5.1.1) or

› the *obliged person* has a relevant connection to an *enhanced risk state* (see Section 7.5).

10. Whilst the information on **identity found out** by the *obliged person* must be provided to the *supervised person* immediately before establishing a *business relationship* or carrying out a *one-off transaction*, a *supervised person* is not also required to immediately obtain **evidence of identity**. Evidence of identity may be held by an *obliged person*, so long as the *supervised person* is satisfied that the *obliged person* will provide the evidence that it holds on request and without delay. However, it is not uncommon for evidence of identity to be called for at the same time as information on identity is provided by the *obliged person*.

11. **Examples of *obliged persons*** include, but are not limited to:

› an investment advisor who arranges for a *customer* to invest in a financial product provided by a *supervised person*, where the investment is to be held in the name of the *customer* and not that of the investment advisor

› a trust company business who establishes a bank or investment account for a client company, trust or foundation

› a law firm that is a supervised person carrying on specified Schedule 2 business

› an accountancy firm that is a supervised person carrying on specified Schedule 2 business.

12. A *supervised person* will remain responsible for the satisfactory performance of all elements of *reliance identification measures*. As noted in the Glossary above, in this Handbook *reliance identification measures* has the meaning set out in Article 16(1) of the *Money Laundering Order*.
13. However, where the measures taken by a *supervised person* are reasonable, it will have a defence should the *obliged person* fail to have performed satisfactory measures.
14. Outsourcing arrangements are not included within the scope of this section, as these are distinct from circumstances in which reliance is placed on an *obliged person*. In an outsourcing arrangement, the *customer* will have a direct relationship with a *supervised person* and not with the provider of the outsourced services. Although the provider of the outsourced services may have substantial contact with the *customer*, the *customer* is a *customer* of the *supervised person* and not of the provider of the outsourced services. The provider of the outsourced services will be carrying on the outsourced activity for the *supervised person* according to the terms of a contract with the *supervised person*. An example of a typical outsourcing arrangement is where a trustee of a *collective investment scheme* outsources the management of the scheme to an external party.
15. Where information on identity found out or evidence of that identity is passed by an *obliged person* to a *supervised person* in order to comply with requirements to counter *money laundering* and the *financing of terrorism*, the Data Protection (Jersey) Law 2018 restricts the use of the information to that purpose, except where another condition for processing personal data applies.
16. A *customer* may be an individual (or group of individuals) or legal person. Section 4.3 of this Handbook deals with a *customer* who is an individual (or group of individuals), Section 4.4 deals with a *customer* (an individual or legal person) who is acting for a legal arrangement, and Section 4.5 deals with a *customer* who is a legal person. The Glossary above provides a definition of *customer* for the purposes of this Handbook.
17. Under Article 16(1) of the *Money Laundering Order*, in this section "customer of the obliged person" means:

› a customer of the obliged person

› a beneficial owner or controller of that customer

› a third party for whom that *customer* is acting

› a *beneficial owner or controller* of a third party for whom that *customer* is acting

› a person purporting to act on behalf of that *customer*.

Statutory requirements (paraphrased wording)

18. *In some strictly limited circumstances, Article 16(2) of the Money Laundering Order provides that a relevant person may be considered to have applied the reliance identification measures where such measures have already been applied by an obliged person. Obliged person means a person who the relevant person knows or has reasonable grounds for believing is:*

› *a relevant person in respect of whom the JFSC discharges supervisory functions that is overseen for AML/CFT compliance in Jersey*

- *a person who carries on equivalent business (refer to Section 1.8).*

19. *Reliance must always be subject to a number of conditions.*
20. *The **first condition** (Article 16(2)(a) of the Money Laundering Order) is that the obliged person consents to being relied upon.*
21. *The **second condition** (Article 16(4) of the Money Laundering Order) is that identification measures have been applied by the obliged person in the course of an established business relationship or one-off transaction.*
22. *The **third condition** (Article 16(4)(a),(b),(c) and (d) of the Money Laundering Order) is that the relevant person obtains adequate assurance in writing that the obliged person:*

› has applied reliance identification measures in relation to the customer

› has not itself relied upon another party to have applied any reliance identification measures

› has not, in reliance on any provision in Part 3A (or if the obliged person is not in Jersey, a provision of similar effect), applied measures that are less than equivalent to the reliance identification measures

› is required to keep, and does keep, evidence of the identification as described in Article 3(4)(b) of the Money Laundering Order relating to each of the obliged person's customers, including a record of such evidence.

23. *The **fourth condition** (Article 16(2)(b) of the Money Laundering Order) is that the obliged person immediately provides the relevant person with the information obtained from applying the reliance identification measures.*
24. *To the extent that reliance is placed on an obliged person to keep hold of the evidence obtained under reliance identification measures, the **fifth condition** (Article 16(5) of the Money Laundering Order) is that the relevant person obtains adequate assurance in writing that the obliged person will:*

- *keep that evidence until the evidence has been provided to the relevant person, or until notification is received from the relevant person that the evidence is no longer required to be kept*
- *provide that evidence to the relevant person at its request, and without delay.*

25. *The **sixth condition** (Article 16(3) of the Money Laundering Order) is that, immediately before placing reliance, the relevant person assesses the risk of placing reliance and makes a written record as to the reason why it is appropriate for it to place reliance on the obliged person, having regard to:*

- *the higher risk of money laundering or the financing of terrorism should the obliged person fail to carry out any action specified in the assurances obtained under Paragraphs 22 and 24 above*
- *the risk that an obliged person will fail to provide the relevant person with evidence without delay if requested to do so by the relevant person. See Section 5.1.1 below.*

26. *Under Article 16(8) of the Money Laundering Order a relevant person who relies on an obliged person under this Article must conduct tests in such manner and at such intervals as the relevant person considers appropriate in all the circumstances in order to establish whether:*

- *the obliged person has appropriate and consistent policies and procedures in place to apply reliance identification measures*

- *if the obliged person has not already provided the evidence to the relevant person, the obliged person does keep the evidence they have obtained during the course of applying reliance identification measures in respect of a person*
- *the obliged person will provide that evidence without delay if requested to do so.*

27. *Under Article 16(8)(c) of the Money Laundering Order, testing should take into consideration whether the obliged person may be prevented, by application of law, from providing information or evidence, e.g. secrecy legislation.*
28. *If, as a result of carrying out any such test, a relevant person is not satisfied that the obliged person has appropriate and consistent policies and procedures in place, keeps evidence, or will provide it without delay if requested to do so, in that particular case, Article 16(9) of the Money Laundering Order requires the relevant person to apply reliance identification measures immediately.*
29. *Article 16(6)(a) of the Money Laundering Order provides that a written assurance will be adequate if it is reasonably capable of being regarded as reliable and a relevant person is satisfied that it is reliable.*
30. *Article 16(6)(b) of the Money Laundering Order provides that written assurances may be provided each time that reliance is placed or through a more general arrangement with an obliged person that has an element of duration, e.g. terms of business.*
31. *Article 16(7) states that a relevant person (including a person who was formerly a relevant person) who has given an assurance to another person under Article 16 (5) (or under an equivalent provision that applies outside Jersey) must, if requested by the other person, provide the person with the evidence obtained from applying the reliance identification measures.*
32. *Article 16(11) of the Money Laundering Order states that nothing in this Article permits a relevant person to rely on the reliance identification measures of an obliged person if:*
    - *the relevant person suspects money laundering or the financing of terrorism*
    - *the relevant person considers that there is a higher risk of money laundering on the basis of the assessment made under Article 16(3) of the Money Laundering Order*
    - *the obliged person is a person having a relevant connection with an enhanced risk state (within the meaning of Article 15 of the Money Laundering Order).*
33. *Notwithstanding that reliance may be placed on an obliged person, Article 16(10) of the Money Laundering Order states that a relevant person is liable for any failure to apply reliance identification measures.*

AML/CFT/CPF Codes of Practice

34. To the extent that reliance is placed on an *obliged person*, a *supervised person* must be able to demonstrate that the conditions required by the Money Laundering Order are met.
35. All evidence of identity passed by the *obliged person* to a *supervised person* (on request) must be confirmed by the *obliged person* as being a true copy of either an original or copy document held on its file.

Guidance notes

Assurance in writing about *reliance identification measures*

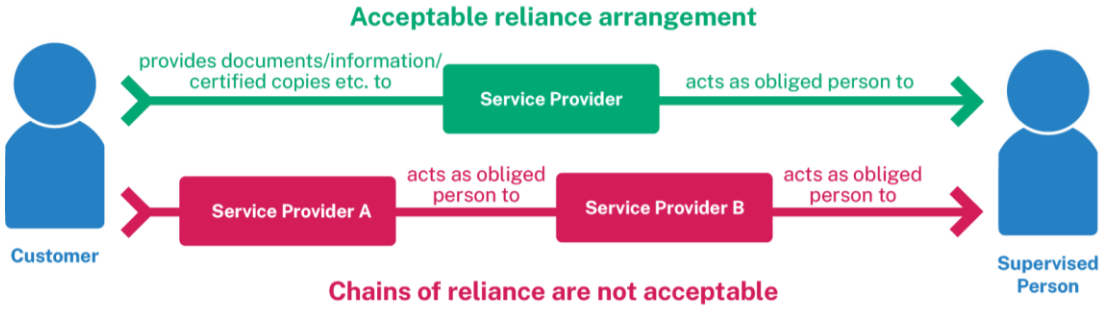
36. A *supervised person* may demonstrate that it has obtained adequate assurance in writing from an *obliged person* under Article 16(4)(a) of the Money Laundering Order that it has applied *reliance identification measures* to the *customer*, where the *obliged person*:

› provides information on **identity** that it has **found out** using an information template and

› explains what **evidence of identity** it has obtained.

37. An assurance that addresses the matters listed in Paragraph 36 above will be considered to be reasonably capable of being regarded as reliable under Article 16(6)(a) of the Money Laundering Order.

38. As stated at Article 16(4)(b) of the *Money Laundering Order* and referenced in the *statutory requirements* section above, a *supervised person* must not rely on an *obliged person* who is in turn relying on someone else (also known as a chain of reliance). See the diagram below for a graphical explanation of this point.



39. Where, as a result of Article 16(6)(b) of the Money Laundering Order, a *supervised person* has a more general arrangement with an *obliged person*, such as terms of business, that more general arrangement may be used to explain what **evidence of identity** will routinely be obtained by the obliged person.

Access to evidence of identity

40. A *supervised person* will have demonstrated that an *obliged person* is providing evidence of identity without delay if it is provided within **two working days**. If it is provided later than **five working days**, it is not provided without delay. If it is provided **between two and five working days**, the *supervised person* must be able to show why this constitutes provision without delay based on the nature of its *customer* base. In order to demonstrate that it has adequately assessed a delay, the *supervised person* is expected to provide detail of the reasons for the delay, how many days evidence remained outstanding, how many times a delay has occurred previously across the *supervised person's* practice, as well as the Board/*senior management's* considerations.

5.1.1 Assessment of Risk

Overview

41. The risk factors that are set out in this section will also be relevant to a *customer* risk assessment that is conducted under Section 3.3.4.1 in the cases highlighted at Section 4.4 and Section 4.5.

Statutory requirements (paraphrased wording)

42. *Before relying upon the obliged person, the relevant person must assess the risk of doing so and make a written record of the reasons the relevant person considers that it is appropriate to do so, having regard to two risks.*

43. *The **first** is the higher risk of money laundering or the financing of terrorism should an obliged person fail to carry out any actions specified in the assurances obtained under Articles 16(4) and (5) of the Money Laundering Order.*

44. *The **second** is the risk that an obliged person will fail to provide the relevant person with evidence without delay if requested to do so by the relevant person.*

45. *Article 16(3) of the Money Laundering Order requires a relevant person to prepare a written record of the reason why it is appropriate to place reliance on an obliged person.*

AML/CFT/CPF Code of Practice

46. In a case where, for a particular *Business Relationship*, testing under Articles 16(8) and (9) of the Money Laundering Order highlights that an *obliged person*:

› has not applied the necessary reliance identification measures

› does not provide adequate, accurate and current information

› does not keep evidence of identity for as long as is necessary or

› will not provide that evidence without delay when requested to do so,

a *supervised person* must review the basis upon which it has placed reliance on that *obliged person* for other relationships (if any) in order to determine whether it is still appropriate to do so.

Guidance notes

47. Immediately before relying upon an *obliged person*, a *supervised person* may demonstrate that it has had regard for the higher risk of *money laundering,* the *financing of terrorism,* and the *financing of proliferation*, and risk that an *obliged person* will fail to provide the *supervised person* with evidence of identity without delay if requested to do so, where it considers the following factors:

› the stature and regulatory track record of the *obliged person*

› the risks posed by the country/territory in which the *obliged person* is based. Factors to consider include those found at Section 3.3.4.1 of this Handbook

› the adequacy of the framework to combat *money laundering,* the *financing of terrorism,* and the *financing of proliferation* in place in the country/territory in which the *obliged person* is based and the period of time that the framework has been in place

› the adequacy of the supervisory regime to combat *money laundering,* the *financing of terrorism,* and the *financing of proliferation* to which the *obliged person* is subject

› the adequacy of identification measures applied by the obliged person to combat money laundering, the *financing of terrorism,* and the *financing of proliferation*.

48. A *supervised person* may demonstrate that it has considered the adequacy of *identification measures* applied by an *obliged person* where it takes one or more of the following steps:

- reviews previous experience (if any) with the *obliged person*, in particular the adequacy and accuracy of information on identity found out by the *obliged person* and whether that information is current
- makes specific enquiries, e.g. through use of a questionnaire or series of questions
- reviews relevant policies and procedures to combat *money laundering,* the *financing of terrorism,* and the *financing of proliferation* in place at the *obliged person*
- where the *obliged person* is a member of a *financial group*, makes enquiries concerning the extent to which group standards are applied to and assessed by the group's internal audit function.

5.2 Group Reliance

Overview

49. In some strictly limited cases, a *supervised person* may meet its obligation to comply with Article 13(1)(a) or (c)(ii) (*CDD*); Article 15(1)(a), (b), (d), (e) or (g) (*Enhanced CDD Measures*); or Article 15A (*Enhanced CDD Measures* in relation to *PEPs*) of the Money Laundering Order, and the *AML/CFT/CPF Codes of Practice* by placing reliance on *similar identification measures* that have already been applied by a party outside Jersey who is a member of the same financial group as the *supervised person,* but is not also an *obliged person*.
50. The effect of Article 16A of the Money Laundering Order is therefore to extend the application of Article 16 to an 'external person' who could not otherwise be relied on, and the six conditions and provisions for testing outlined in Section 5.1 apply to an external person in the same way as to an *obliged person*.
51. Under the definitions provided in Article 16A(1) of the Money Laundering Order, in this section 'external person' means a person outside Jersey, who:

- is not an obliged person
- is a member of the same financial group as the *supervised person* and
- carries on a business which, if that business were carried on in Jersey, would be a *supervised business*.

Statutory requirements (paraphrased wording)

52. *In some strictly limited circumstances, Article 16A of the Money Laundering Order provides that a relevant person may be considered to have applied similar identification measures specified in Article 3(2)(a), (aa), (b) and (c) of the Money Laundering Order where such measures have already been applied by an external person.*
53. *Under Article 16A(2)(c-f) of the Money Laundering Order, in order to place reliance on an external person, the financial group to which the relevant person and external person belong must:*

- *apply CDD measures and record-keeping requirements in line with the Money Laundering Order or in line with FATF Recommendations 10, 11 and 12*

- *maintain a programme against money laundering and the financing of terrorism which includes policies and procedures by which every member of the group who carries on a financial services business (or equivalent) shares information that is appropriate for the purpose of preventing and detecting money laundering and the financing of terrorism (an AML/CFT programme)*
- *adequately mitigate any higher risk of money laundering and the financing of terrorism through its policies and procedures*
- *be supervised by an overseas regulatory authority in its implementation of CDD measures and record-keeping requirements, and its AML/CFT programme.*

54. *Article 16(A)(2), (3), (4), (5) and (6) of the Money Laundering Order states that reliance is always subject to a number of conditions. These are outlined at Paragraphs 20 to 25 above, where references to "obliged person" should be read as referring to "external person".*
55. *Articles 16(A)(7) and (8) of the Money Laundering Order state that reliance must always be subject to testing. Provisions in this respect are outlined at Paragraphs 26 to 28 above, where references to "obliged person" should be read as referring to "external person".*
56. *Article 1(5) of the Money Laundering Order explains that a person is a member of the same financial group as another person if there is, in relation to the group, a parent company or other legal person that exercises control over every member of that group for the purposes of applying group supervision under:*

- *the Core Principles for Effective Banking Supervision published by the Basel Committee*
- *the Objectives and Principles for Securities Regulation issued by IOSCO or*
- *the Insurance Supervisory Principles issued by the IAIS.*

AML/CFT/CPF Codes of Practice

57. A *supervised person* may not rely on an 'external person' where it suspects *money laundering,* the *financing of terrorism,* or the *financing of proliferation*, considers that there is a higher risk of *money laundering* or the *financing of terrorism* on the basis of a risk assessment carried out under Article 16(3) of the *Money Laundering Order*, or where the *external person* has a relevant connection to an *enhanced risk state*.
58. Despite a *supervised person's* reliance on an 'external person' under Article 16A(9) of the *Money Laundering Order*, a *supervised person* is liable for any failure to apply similar identification measures.

6 ONGOING MONITORING – SCRUTINY OF TRANSACTIONS & ACTIVITY

6.1 Overview of section

1. This section outlines the statutory provisions concerning on-going monitoring. On-going monitoring consists of:

› scrutinising transactions undertaken throughout the course of a business relationship and

› keeping documents, data or information up-to-date and relevant.

2. The obligation to monitor a *business relationship* finishes at the time that it is terminated. In a case where a relationship has been terminated, but where payment for a service remains outstanding, a *supervised person* will still need to consider reporting provisions summarised in Section 8 of this Handbook. For example where there is suspicion that payment for the service is made out of the proceeds of criminal conduct or instrumentalities.

3. This section explains the measures required to demonstrate compliance with the requirement to scrutinise transactions and sets a requirement to scrutinise *customer* activity.

4. The requirement to keep documents, data or information up-to-date and relevant is covered at Section 3.4 of this Handbook.

6.2 Obligation to perform on-going monitoring

Statutory requirements (paraphrased wording)

5. Article 3(3) of the Money Laundering Order sets out what on-going monitoring is to involve:

› *scrutinising transactions undertaken throughout the course of a business relationship to ensure that the transactions being conducted are consistent with the relevant person's knowledge of the customer, including the customer's business and risk profile. See Article 3(3)(a) of the Money Laundering Order*

› *keeping documents, data or information up-to-date and relevant by undertaking reviews of existing records, particularly in relation to higher risk categories of customers. See Article 3(3)(b) of the Money Laundering Order.*

6. *Article 13 of the Money Laundering Order requires a relevant person to apply on-going monitoring throughout the course of a business relationship.*

7. Article 11 of the Money Laundering Order requires a relevant person to maintain appropriate and consistent policies and procedures for the application of CDD measures, having regard to the degree of risk of money laundering and the financing of terrorism. The policies and procedures referred to include those:

› *which provide for the identification and scrutiny of:*

a. complex or unusually large transactions

b. unusual patterns of transactions, which have no apparent economic or lawful purpose or

c. any other activity, the nature of which causes the relevant person to regard it as particularly likely to be related to money laundering or the financing of terrorism.

› *which determine whether:*

a. business relationships or transactions are with a person connected with a country or territory in relation to which the FATF has called for the application of enhanced CDD measures or

b. business relationships or transactions are with a person:

i. subject to measures under law applicable in Jersey for the prevention and detection of money laundering

ii. connected with an organization that is subject to such measures or

iii. connected with a country or territory that is subject to such measures.

8. Article 11(3A) of the Money Laundering Order explains that, for the purposes of Article 11(3)(a), "scrutiny" includes scrutinising the background and purpose of transactions and activities.

6.2.1 Scrutiny of transactions and activity

Overview

9. **Scrutiny** may be considered as two separate, but complimentary processes.

10. **Firstly**, a *supervised person* **monitors** all *customer* transactions and activity in order to **recognise** notable transactions or activity, i.e. those that:

- are inconsistent with the *supervised person's* knowledge of the customer (unusual transactions or activty)
- are complex or unusually large
- form part of an unusual pattern or
- present a higher risk of money laundering, the financing of terrorism, or the financing of proliferation.

11. **Secondly**, such notable transactions and activity, including their background and purpose, are then **examined** by an appropriate person.

12. In addition to the scrutiny of **transactions** as required by the *Money Laundering Order*, *AML/CFT/CPF Codes of Practice* in this section also require a *supervised person* to scrutinise *customer* **activity**. This is not just relevant to transaction-based business relationships, but also to business relationships that do not involve transactions, e.g. where a *supervised person* gives investment advice, or acts as a director to a company.

13. A *supervised person* must therefore, as a part of its **scrutiny** of transactions/activity, establish appropriate *procedures* to **monitor** all of its *customers'* transactions/activity, and to **recognise** and **examine** notable **transactions/activity**.

14. Sections 3 and 4 of this Handbook address the capturing of sufficient information about a *customer,* allowing a *supervised person* to record a ***customer* business and risk profile** which provides a basis for recognising notable transactions/activity, which may indicate *money laundering,* the *financing of terrorism,* or the *financing of proliferation*.

15. Additional or more frequent monitoring is required for relationships that have been designated as carrying a higher risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*.

16. With reference to what has been recorded in the *customer* business and risk profile, **unusual transactions/activity**, **unusually large transactions/activity**, and **unusual patterns of transactions/activity** may be recognised where transactions or activity are inconsistent with:

› the expected pattern of transactions

› the expected activity for a particular *customer* or

› the normal business activities for the type of product or service that is being delivered.

17. Where a *supervised person's customer* base is homogeneous, and where the products and services provided to *customers* result in uniform patterns of transactions or activity, it may be easier to establish parameters to identify usual transactions/activity. For example when dealing with local property transactions being passed before the Royal Court or undertaking deposit-taking activities.

18. Where each *customer* is unique, and where the product or service is bespoke, a *supervised person* will need to tailor monitoring systems to the nature of its business and facilitate the application of additional judgement and experience to the recognition of unusual transactions and activity.

19. For some *customers*, additional information may only become evident **during** the course of the *business relationship* (i.e. whilst acting for the *customer*), leading to a revised profile and risk assessment. This requires particular diligence and care when updating documents, data or information and when scrutinising and monitoring *customer* activity and transactions. In these cases, appropriate staff training in the recognition of unusual transactions and activity is vital, as are relevant *systems and controls*.

20. **Higher risk transactions/activity** may be recognised by developing a set of 'red flags' or indicators which may indicate *money laundering,* the *financing of terrorism,* or the *financing of proliferation*, based on a *supervised person's* understanding of its business, products and *customers* (i.e. the outcome of its business risk assessment – Section 2.3.1).

21. **Complex transactions/activity** may be recognised by developing a set of indicators, based on a *supervised person's* understanding of its business, its products and its *customers* (i.e. the outcome of its business risk assessment – Section 2.3.1).

22. External data sources and media reports may also assist with the identification of notable transactions and activity.

23. Where notable transactions or activity are **recognised**, they will need to be **examined**. The purpose of this examination is to determine whether there is an **apparent economic** or **visible lawful purpose** for the transactions or activity. It is not necessary (nor will it be possible) to conclude with certainty that a transaction or activity has an economic or lawful purpose. Sometimes, it may be possible to make such a determination on the basis of an existing customer business and risk profile and on occasion this examination will involve requesting additional information from a *customer*.

24. Notable transactions or activity may indicate *money laundering,* the *financing of terrorism,* or the *financing of proliferation* where there is no apparent economic or visible lawful purpose for the transaction or activity, i.e. they are no longer just unusual, but may also be suspicious. **Reporting** of knowledge, suspicion, or reasonable grounds for knowledge or suspicion of *money laundering* or the *financing of terrorism* is addressed in Section 8 of this Handbook.

25. Practical guidance on financial sanctions implementation matters, including an explanation of reporting obligations under the *Sanctions and Asset-Freezing Law*, is provided on the JFSC's website. See also Section 8.8 of this Handbook.

26. **Scrutiny** may involve both **real time** and **post event** monitoring. Real time monitoring will focus on transactions and activity when information or instructions are received from a *customer*, before or as the instruction is processed. Post event monitoring may involve end of day, weekly, monthly or annual reviews of *customer* transactions and activity. Real time monitoring of transactions and activity will more effectively reduce a *supervised person's* exposure to *money laundering,* the *financing of terrorism,* and the *financing of proliferation*. Post event monitoring may be more effective at identifying unusual patterns.

27. Monitoring may involve **manual** and **automated procedures**. Automated monitoring procedures may add value to manual procedures by recognising transactions or activity that fall outside set parameters. This will be particularly so where a *supervised person* processes large volumes of *customer* transactions which are not subject to day-to-day oversight. However, where automated monitoring procedures are not in place, monitoring is likely to be most effective when undertaken on a case-by-case basis by *customer* facing staff, administration and accounts staff, whom may be expected to spot and highlight notable transactions or activity.

28. The **examination** of notable transactions or activity may also be conducted either by *customer* facing employees, or by an independent reviewer. In any case, the examiner must have access to all *customer* records.

29. The results of an examination should be recorded and appropriate action taken. Refer to Section 10 of this Handbook for record-keeping requirements in relation to the examination of notable transactions and activity.

30. In order to **recognise** *money laundering,* the *financing of terrorism,* and the *financing of proliferation*, employees will need to have a good level of awareness of each, and to have received training. Refer to Section 9 of this Handbook for raising of awareness and training.

31. Where on-going monitoring indicates possible *money laundering* or the *financing of terrorism* activity, an internal *SAR* is required to be made to the *MLRO*. Reporting of knowledge, suspicion, or reasonable grounds for knowledge or suspicion, of *money laundering* and the *financing of terrorism* is addressed in Section 8 of this Handbook.

AML/CFT/CPF Codes of Practice

32. In addition to the **scrutiny** of **transactions**, on-going monitoring must also involve **scrutinising activity** in respect of a business relationship to ensure that the activity is consistent with the *supervised person's* knowledge of the *customer*, including the *customer's* business and risk profile.

33. A *supervised person* must establish and maintain appropriate and consistent *policies and procedures* which provide for the **identification** and **scrutiny** of:

- complex or unusually large activity
- unusual patterns of activity, which have no **apparent economic** or **visible lawful** purpose and
- any other activity, the nature of which causes the *supervised person* to regard it as particularly likely to be related to *money laundering,* the *financing of terrorism,* or the *financing of proliferation*.

34. As part of its examination of the above transactions, a *supervised person* must **examine**, as far as possible, their background and purpose and set forth its findings in writing.

Guidance notes

35. A *supervised person* may demonstrate that *CDD policies and procedures* are appropriate where **scrutiny** of transactions and activity has regard to the following factors:

› its business risk assessment (including the size and complexity of its business)

› the nature of its business and services

› whether it is practicable to monitor transactions or activity in real time (i.e. before customer instructions are put into effect)

› whether it is possible to establish appropriate standardised parameters for automated monitoring and

› the monitoring procedures that already exist to satisfy other business needs.

36. A *supervised person* may demonstrate that *CDD policies and procedures* are appropriate where the following are used to **recognise** notable transactions or activity:

› *customer* business and risk profile – see Section 3.3.5 of this Handbook

› 'red flags' or indicators of higher risk – that reflect the risk that is present in the *supervised person's customer* base – based on its business risk assessment (refer to Section 2.3.1 of this Handbook), information published from time to time by the *JFSC* or *JFCU*, e.g. findings of supervisory and themed examinations and typologies, and information published by reliable and independent third parties and

› 'red flags' or indicators of complex transactions and activity – based on its business risk assessment (refer to Section 2.3.1 of this Handbook), information published from time-to-time by the *JFSC* or *JFCU*, e.g. findings of supervisory and themed examinations and typologies, and information published by reliable and independent third parties.

37. A *supervised person* may demonstrate that *CDD policies and procedures* are appropriate if **examination** of notable transactions or activity includes:

› reference to the *customer's* business and risk profile

› as far as possible, a review of the background and purpose of a transaction or activity (set in the context of the business and risk profile) and

› where necessary, the collection of further information needed to determine whether a transaction or activity has an **apparent economic** or **visible lawful purpose**.

Case study:

› A *supervised person* may have a business relationship with a *customer* who previously advised that they had a modest *source of funds*.

› The *customer* then instructs the *supervised person* to purchase an asset, the value of which appears to be outside the means of the *customer's source of funds,* as currently understood.

› While the *supervised person* may be satisfied that it still knows the identity of the *customer*, as part of its on-going monitoring obligations, it would be appropriate to ask about the

source of funds for this purchase. Depending on the *customer's* willingness to provide such information, and the answer that is provided, the *supervised person's staff* should also consider whether they:

› are satisfied with the response

› want further proof of the *source of funds* and/or

› need to submit an internal *SAR* to the *supervised person's MLRO*.

38. A *supervised person* may demonstrate that *CDD* and reporting *policies and procedures* are effective if, in **post-examination** of notable transactions or activity, it:

› revises, as necessary, its *customer's* business and risk profile

› adjusts, as necessary, its monitoring system, e.g. it refines monitoring parameters, enhances controls for more vulnerable products/services/business units

› considers if it knows, or has reasonable cause to suspect, that a person:

  - a designated person, or
  - has committed, is committing or intends to commit and offence under the Sanctions and Asset-Freezing Law, and

› considers whether it knows, suspects or has reasonable grounds for suspecting that another person is engaged in *money laundering* or the *financing of terrorism*, or that any property constitutes or represents:

  - the proceeds of criminal conduct; or
  - property used in or intended to be used in criminal conduct.

6.2.2 Monitoring and recognition of business relationships and transactions – Person connected with an enhanced risk state or sanctioned country

Overview

39. The risk that a *business relationship* is tainted by funds that are the proceeds of criminal conduct or instrumentalities, or are used to finance terrorism, is increased where the *business relationship* or *one-off transaction* is with a person or entity connected with a country or territory:

› in relation to which the *FATF* has called for the application of *enhanced CDD* measures (an *enhanced risk state*) or

› that is subject to measures for purposes connected with the prevention and detection of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*, such measures being imposed by one or more countries or sanctioned by the UK, *EU* (in limited circumstances) or the *UN.*

40. Similarly, the risk that a *business relationship* is tainted by funds that are the proceeds of criminal conduct or instrumentalities, or are used to finance terrorism, is increased where the *business relationship* or *one-off transaction* is with a person connected with an organisation subject to such measures or who is themselves subject to such measures.

41. As a part of its on-going monitoring procedures, a *supervised person* will establish and maintain appropriate *policies and procedures* to **monitor** all *customer* transactions and activity in order to **recognise** whether any business relationships or one-off transactions are directly or indirectly with such sanctioned persons, organisations or other parties.

42. There is not a separate requirement to **examine**, or have *policies and procedures* in place to examine, *business relationships* with an *enhanced risk state* once they are recognised. This is because enhanced *CDD* measures must be applied in line with Article 15(1)(c) of the Money Laundering Order. See Section 7.5 of this Handbook.

43. There is not a statutory requirement to **examine**, or have *policies and procedures* in place to examine, *business relationships* or *one-off transactions* with a *designated person* once they are recognised. This is because provisions in financial sanctions legislation must be followed. Among other things, such provisions may prohibit certain activities or require the property to be frozen. Further guidance is published on the *JFSC's* website.

AML/CFT/CPF Codes of Practice

44. On-going monitoring must involve **examining** transactions and activity recognised as being with a person connected with an *enhanced risk state*.

45. A *supervised person* must establish and maintain appropriate and consistent *policies and procedures* which provide for the **examination** of transactions and activity recognised as being with a person connected with an *enhanced risk state*.

46. As part of its **examination** of the above transactions and activity, a *supervised person* must examine, as far as possible, their background and purpose and set forth its findings in writing.

Guidance notes

47. A *supervised person* may demonstrate that *CDD policies and procedures* are appropriate where **scrutiny** of transactions and activity has regard to the following factors:

- its business risk assessment (including the size and complexity of its business)
- the nature of its business and services
- whether it is practicable to monitor transactions or activity in real time (i.e. before *customer* instructions are put into effect)
- whether it is possible to establish appropriate standardised parameters for automated monitoring and
- the monitoring procedures that already exist to satisfy other business needs.

48. A *supervised person* may demonstrate that *CDD policies and procedures* are appropriate where the following are used to **recognise** connections with persons connected to *enhanced risk states* and *sanctioned countries*:

- all *customers* – Business and risk profile in line with Section 3.3.5 of this Handbook
- all *customers* – Adopting the Sanctions designations lists as a comprehensive listing of sanctions measures applicable in Jersey

- all *customers* – Considering methods of identifying possible indirect associations and connections that may exist between the *supervised person's customer* and any sanctioned parties, and/or enhanced risk states, that will not immediately be obvious from screening of the UK's consolidated list
- *enhanced risk states* - Appendix D1 of the *AML/CFT/CPF Handbook* and
- sanctioned countries and territories - Appendix D2 of the *AML/CFT/CPF Handbook* (Source 6 only).

49. A *supervised person* may demonstrate that *CDD policies and procedures* are appropriate if **examination** of transactions or activity recognised as being with a person connected with an *enhanced risk state* includes:

- reference to the *customer's* business and risk profile
- as far as possible, a review of the background and purpose of a transaction or activity (set in the context of the business and risk profile) and
- where necessary, the collection of further information needed to determine whether a transaction or activity has an **apparent economic** or **visible lawful** purpose.

50. A *supervised person* may demonstrate that *CDD* and reporting *policies and procedures* are appropriate if **post-examination** of transactions or activity recognised as being with a person connected with an *enhanced risk state* it:

- revises, as necessary, its *customer's* business and risk profile
- adjusts, as necessary, its monitoring system e.g. refines monitoring parameters, enhances controls for more vulnerable products/services/business units
- considers if it knows, or has reasonable cause to suspect, that a person:
    - a designated person, or
    - has committed, is committing or intends to commit and offence under the Sanctions and Asset-Freezing Law and
- considers whether it knows, suspects or has reasonable grounds for suspecting that another person is engaged in *money laundering* or the *financing of terrorism*, or that any property constitutes or represents:
    - the proceeds of criminal conduct; or
    - property used in or intended to be used in criminal conduct.

6.3 Automated monitoring methods

Overview

51. Automated monitoring methods may be effective in recognising notable transactions and activity, and *business relationships* and *one-off transactions* with persons connected to *enhanced risk states* and sanctioned countries, territories and other sanctioned parties.

52. **Exception reports** can provide a simple but effective means of monitoring all transactions to or from particular geographical locations or accounts and any activity that falls outside of pre-determined parameters, based on thresholds that reflect a *customer's* business and risk profile.

53. Large or more complex *supervised persons* may also use automated monitoring methods to facilitate the monitoring of significant volumes of transactions, or – such as in an e-commerce environment – where the opportunity for human scrutiny of individual transactions is limited.

54. What constitutes unusual behaviour by a *customer* is often defined by the automated monitoring system selected by the *supervised person*. It is important that the system selected has an appropriate definition of 'unusual' and is in line with the nature of business conducted by the *supervised person*.

55. Where an automated monitoring method (group or otherwise) is used, a *supervised person* will need to understand:

› how the system works and when it is changed

› its coverage (who or what is monitored and what external data sources are used)

› how to use the system, e.g. making full use of guidance and

› the nature of its output (exceptions, alerts etc.).

56. Use of automated monitoring methods does not remove the need for a *supervised person* to otherwise remain vigilant. Factors such as staff intuition, direct contact with a *customer* and the ability, through experience, to recognise transactions and activity that do not seem to make sense, cannot be automated.

57. In the case of **screening** of a business relationship (before establishing that relationship and subsequently) and transactions, the use of electronic external data sources to screen *customers* may be particularly effective. However, where a *supervised person* uses group screening arrangements, it will need to be satisfied that it provides adequate mitigation of risks applicable to the Jersey business. In all cases, it is important that a *supervised person*:

› understands which business relationships and transaction types are screened

› understands the system's capacity for **fuzzy matching** (a technique used to recognise names that do not precisely match a target name but which are still potentially relevant)

› sets clear procedures for dealing with potential matches, driven by risk considerations rather than resources and

› records the basis for **discounting** alerts (e.g. false positives) to provide an audit trail.

58. By way of example, **fuzzy matching** arrangements can be used to identify the following variations:

Variation	Example
Different spelling of names	"Jon" instead of "John" "Abdul" instead of "Abdel"
Name reversal	"Adam, John Smith" instead of "Smith, John Adam"

Shortened names	"Bill" instead of "William"
Insertion/removal of punctuation and spaces	"Global Industries Inc" instead of "Global-Industries, Inc."
Name variations	"Chang" instead of "Jang"

59. Further information on screening practices may be found in reports published by the *JFSC* in August 2014 and May 2021. Additional guidance is also available on the JFSC's website.

6.4 Money laundering warning signs

Overview

60. Article 13 of the *Money Laundering Order* requires a *supervised person* to apply on-going monitoring throughout the course of a business relationship and take steps to be aware of transactions with heightened *money laundering* and the *financing of terrorism* risks. The *Proceeds of Crime Law* requires a *supervised person* to report suspicious transactions and activity (see Section 8 of this Handbook).

61. This section highlights a number of general warning signs for *supervised persons* to help them decide whether there may be reasons for concern or the basis for a reportable suspicion.

62. In relation to on-going monitoring, a *supervised person* should have regard both to the warning signs contained in the relevant sector-specific sections of this Handbook and the general indicators set out below, where they may become vulnerable to *money laundering,* the *financing of terrorism,* or the *financing of proliferation*. These warning signs apply to on-going relationships just as much as to circumstances that may arise at the start of a business relationship.

63. Because money launderers, terrorist financers, and proliferators of weapons of mass destruction are always developing new techniques, no list of examples can be fully comprehensive. However, the following are some key factors indicating activity or transactions which might heighten a *customer's* risk profile or give cause for concern.

6.4.1 Secretive customers

64. Whilst face-to-face contact with *customers* is not always possible, an excessively obstructive or secretive *customer* may be a cause for concern. Consideration should be given as to whether *customers* who demand strict confidentiality relating to their financial and business affairs, or are reluctant to answer due diligence questions are evading tax or seeking to mask the true beneficial ownership of their assets.

6.4.2 Unusual instructions

65. Instructions that are unusual in themselves, or that are unusual for the *supervised person* or the *customer* may give rise to concern, particularly where no rational or logical explanation can be given. Be wary of:

- loss-making transactions where the loss is avoidable
- dealing with money or property when there are suspicions that it is being transferred to avoid the attention of either a trust in a bankruptcy case, a revenue authority (e.g. HMRC, Revenue Jersey etc), or a law enforcement agency
- complex or unusually large transactions, particularly where underlying beneficial ownership is difficult to ascertain and/or where the underlying transactions have been conducted in cash

- unusual patterns of transactions which have no apparent economic purpose particularly those where a number of jurisdictions and different entities are involved for no logical business reason
- funds that are being switched between investments or jurisdictions for no apparent reason
- use of shell companies, blind trusts or other structures that are merely being used as a front for other activities
- excessive use of off-balance sheet transactions or activity.

6.4.2.1 Instructions outside the *supervised person's* area of expertise

66. Taking on work which is outside the *supervised person's* normal range of expertise can present additional risks because a money launderer, terrorist financer or proliferator might be using the *supervised person* to avoid answering too many questions. A *supervised person* inexperienced in the provision of a particular product or service might be influenced into taking steps which a more experienced business would not contemplate. *Supervised persons* should be wary of highly paid niche areas of work in which they have no background, but in which the *customer* claims to be an expert.

67. If the *customer* is not resident in Jersey, *supervised persons* should satisfy themselves that there is a genuine legitimate reason why they have been approached. For example, have the *supervised person's* services been recommended by another *customer*? Making these types of enquiries makes good business sense, as well as being a sensible *AML/CFT/CPF* check.

6.4.2.2 Changing instructions

68. Instructions that change unexpectedly or significantly might be suspicious, especially if there seems to be no logical reason for the changes. This may also be the case where the person making the instruction changes. The obligation to re-conduct *CDD* may well arise.

69. The following situations could give rise to cause for concern:

- a *customer* deposits funds into a *supervised person's* client account for a transaction, but then ends the transaction for no apparent reason
- a *customer* advises that funds are coming from one source and at the last minute the source changes and
- a *customer* unexpectedly requests that money received into a *supervised person's* client account be sent back to its source, to the *customer* or to a third party.

6.4.3 Use of client accounts

70. Client accounts should only be used to hold *customer* money for legitimate transactions for *customers*, or for another proper legal purpose. Putting criminal money through a *supervised person's* client account can make it appear clean, whether the money is sent back to the *customer*, on to a third party, or invested in some way. Introducing cash into the banking system can become part of the placement stage of *money laundering*. Therefore, the use of cash for non-cash based businesses is often a warning sign.

6.4.3.1 Source of funds

71. If funding is from a source other than the *customer*, *supervised persons* may need to make further enquiries, especially if the *customer* has not previously advised that a third party would be involved. When considering whether to accept funds from a third party, *supervised persons* should ask how and why the third party is helping with the funding.

72. *A supervised person* must always be alert to warning signs and in some cases will need to seek more information.

6.4.4 Money laundering offences factors

6.4.4.1 Intent

73. Except for certain strict liability offences, criminal conduct requires an element of criminal intent which means that an offender must know or suspect that an action or property is criminal. Conduct which is an innocent error or mistake may be criminal where it constitutes a strict liability offence, but will not also be *money laundering*.

74. If an individual or *supervised person* knows or believes that a *customer* is acting in error, the *customer* may be approached and the situation and legal risks explained to them. However, once the criminality of the conduct is explained to the *customer*, they must bring their conduct (including past conduct) promptly within the legislation to avoid a *money laundering* offence being committed. Where there is uncertainty about the legal issues that are outside the competence of the *supervised person*, *customers* should be referred to an appropriate specialist or legal adviser.

75. If there are reasonable grounds to suspect that a *customer* knew or suspected that their actions were criminal, a report must be made. Even if the *customer* does not have the relevant intent, but the *supervised person* is aware that there is criminal property, consideration needs to be given to whether a report has to be made to the *JFCU*.

76. In all circumstances, *supervised persons* should be mindful of committing a 'tipping-off' offence as set out at Article 35(4) of the Proceeds of Crime Law. See Section 8.5 of this Handbook for more information.

6.4.4.2 Holding of funds

77. *Supervised persons* who choose to hold funds on behalf of a *customer* should consider the checks to be made about the funds they intend to hold before the funds are received. Consideration should be given to conducting *CDD* measures on all those on whose behalf the funds are being held.

78. Particular consideration should be given to any proposal that funds are collected from a number of individuals whether for investment purposes or otherwise. This could lead to wide circulation of client account details and payments being received from unknown sources.

6.4.4.3 Factors arising from action by the *customer* or its controllers

79. Where a *customer* is actively involved in *money laundering*, the signs may include:

- unusually complex corporate structure where complexity does not seem to be warranted
- complex or unusual transactions, possibly with related parties

- transactions with little commercial logic taking place in the normal course of business (such as selling and re-purchasing the same asset)
- transactions conducted outside of the normal course of business or where the method of payment/receipt is not usual business practice, such as wire transfers or payments in foreign currency
- transactions where there is a lack of information or explanation, or where explanations are unsatisfactory
- transactions that are undervalued or overvalued, including double billing
- transactions with companies whose identity or beneficial ownership is difficult to establish
- abnormally extensive or unusual related party transactions
- unusual numbers of cash transactions for substantial amounts or a large number of small transactions that add up to a substantial amount
- payment for unspecified services or for general consultancy services and
- long delays in the production of company or trust accounts for no apparent reason.

6.4.4.4 Where the *customer* may unknowingly be a party to money laundering, the financing of terrorism, or the financing of proliferation

80. There may be occasions where **the *customer* has been duped by its own customer** into providing assistance or a vehicle for *money laundering,* the *financing of terrorism,* or the *financing of proliferation*. Warning signs may be:

- unusual transactions without an explanation, or a pattern of trading with a customer of the *supervised person's customer* that is different from the norm
- request for settlement of sales in cash
- the *customer's* customer setting up a transaction that appears to be of no commercial advantage or logic
- the *customer's* customer requesting special arrangements for vague purposes
- unusual transactions with companies registered in other jurisdictions
- request for settlement to bank accounts or jurisdictions which would be unusual for a normal commercial transaction or
- excessive overpayment of accounts, subsequently requesting a refund.

6.4.5 Administration of estates

81. A deceased person's estate is very unlikely to be actively utilised by criminals as a means for laundering their funds; however, there is still a risk of *money laundering* for those working in this area.

82. When winding up an estate, there is no blanket requirement that *supervised persons* should be satisfied about the history of all of the funds which make up the estate under administration. However, *supervised persons* should be aware of the factors which can increase *money laundering* risks and consider the following:

- where estate assets have been earned in a foreign jurisdiction, *supervised persons* should be aware of the wide definition of criminal conduct in Article 1 of the Proceeds of Crime Law and
- where estate assets have been earned or are located in a *higher risk country or territory*, *supervised persons* may need to make further checks about the source of those funds.

83. *Supervised persons* should be alert from the outset and **monitor** throughout so that any disclosure can be considered as soon as knowledge or suspicion is formed and problems of delayed consent can be avoided.

84. *Supervised persons* should bear in mind that an estate may include criminal property. An extreme example would be where the *supervised person* knows or suspects that the deceased person was accused or convicted of acquisitive criminal conduct during their lifetime.

85. If *supervised persons* know or suspect that the deceased person improperly claimed welfare benefit or had evaded the due payment of tax during their lifetime, criminal property will be included in the estate and so a *money laundering* disclosure may be required.

86. Relevant local laws will apply before assets can be released. For example, a grant of probate will normally be required before UK assets can be released. *Supervised persons* should remain alert to warning signs, for example if the deceased or their business interests are based in a *higher risk country of territory*.

87. If the deceased person is from another jurisdiction and a lawyer is dealing with the matter in the home country, *supervised persons* may find it helpful to ask the lawyer for information about the deceased to gain some assurances that there are no suspicious circumstances surrounding the estate. The issue of the tax payable on the estate may depend on the jurisdiction concerned.

6.4.6 Charities

88. While the majority of charities are used for legitimate reasons, they can be used as vehicles for *money laundering,* the *financing of terrorism,* or the *financing of proliferation*.

89. *Supervised persons* acting for charities should consider their purpose and the organisations they are aligned with. If money is being received on the charity's behalf from an individual or a company donor, or a bequest from an estate, *supervised persons* should be alert to unusual circumstances, such as receipt of unexpectedly large sums of money.

6.4.7 Taxation matters

90. There are a number of tax offences which can give rise to the proceeds of crime and therefore require the submission of a *SAR* to the *JFCU*. A *supervised person* is not required to be an expert in criminal law, but they would be expected to recognise activity which might suggest the *customer* is involved in tax evasion.

91. There will, however, be no question of criminality where the *customer* has adopted in good faith, honestly and without mis-statement, a technical position with which a revenue authority disagrees.

92. The main areas where offences may arise in relation to direct tax are:

- tax evasion, including making false returns (including supporting documents), accounts or financial statements or deliberate failure to submit returns and
- deliberate refusal to correct known errors.

6.4.7.1 Innocent or negligent error

93. Where a *customer* indicates that they are unwilling, or refuse, to disclose an innocent mistake or negligent act to the *competent authority* in order to avoid paying the tax due, the *customer* appears to have formed a criminal intent and therefore a reporting obligation arises. The *supervised person* should also consider whether they can continue to act for the *customer*. This paragraph applies equally to potential *customers* for whom the *supervised person* has declined to act.

6.4.7.2 Intention to underpay

94. C*ustomers* may suggest that they will, in the future, underpay tax. This would be tax evasion and also a *money laundering* offence when it occurs. A *supervised person* can and should investigate whether the *customer* has understood their obligations under the relevant legislation. Should the *customer's* intention in this regard still remain in doubt, the *supervised person* should consider carefully whether they can commence or continue to act, and if in doubt should seek specialist legal advice. A *SAR* may well be required in such cases.

6.4.8 Observation of unlawful conduct

95. It should be borne in mind that for property to be criminal property, not only must it constitute a person's benefit from criminal conduct, but the alleged offender must know or suspect that the property constitutes such a benefit. This means, for example, that if someone has made an innocent error, even if such an error resulted in benefit and constituted a strict liability criminal offence, then the proceeds are not criminal property and no *money laundering* offence has arisen until the offender becomes aware of the error.

96. Examples of unlawful behaviour which may be observed, but which are not reportable as *money laundering*, are set out below:

- offences where no proceeds or benefit results, such as the late filing of company accounts. However, *supervised persons* should be alert to the possibility that persistent failure to file accounts could represent part of a larger offence with proceeds, such as fraudulent trading or credit fraud involving the concealment of a poor financial position
- mis-statements in tax returns, for whatever cause, but which are corrected before the date when the tax becomes due
- attempted fraud where the attempt has failed and so no benefit has accrued (although this may still be an offence in some jurisdictions e.g. the UK) and
- where a *customer* refuses to correct, or unreasonably delays in correcting, an innocent error that gave rise to proceeds and which was unlawful, firms should consider what that indicates about the client's intent and whether the property has now become criminal property.

7 ENHANCED AND SIMPLIFIED CDD MEASURES AND EXEMPTIONS

7.1 Overview of section

1. This section explains the circumstances in which *CDD* measures must be enhanced under Articles 15, 15A and 15B of the Money Laundering Order and explains the exemptions from *CDD* requirements under Part 3A of the *Money Laundering Order*. It also sets out circumstances where simplified measures can be applied in relation to low risk products or services.

2. In addition to any case where a *supervised person* determines that a *customer* presents a higher risk of *money laundering* or the *financing of terrorism*, Articles 15, 15A and 15B of the Money Laundering Order also requires enhanced *CDD* measures to be applied in the following specified scenarios:

- *customer*, or some other person, is not physically present for identification purposes – Section 7.4
- *customer* has a relevant connection to an *enhanced risk state* – Section 7.5
- *customer*, or some other prescribed person, is a *PEP* – Section 7.6
- *customer* is a non-resident – Section 7.7
- *customer* is provided with private banking services – Section 7.8
- *customer* is a personal asset holding vehicle – Section 7.9
- *customer* is a company with nominee shareholders or issues bearer shares – Section 7.10
- correspondent Banking or similar relationships – Section 7.11

3. It may be that *CDD* measures routinely applied under Article 13 of the Money Laundering Order already address some of the risk characteristics of these *customers* (for instance identification of *beneficial owner(s)* and understanding the nature and purpose of the relationship) and significantly reduce the risk of *money laundering* and the *financing of terrorism*. Therefore any additional measures may be quite limited.

4. Nevertheless, the enhanced measures required under Articles 15, 15A and 15B must be in addition to the measures to be taken in circumstances presenting a lower or standard risk, as set out in Section 4 and Section 6 of this *Handbook* and must address the particular risk presented. This section provides some (non-exhaustive) examples for each category of *customer*.

5. As noted in the Glossary above, a *customer* may be an individual (or group of individuals) or a legal person. Section 4.3 of this Handbook deals with a *customer* who is an individual (or group of individuals), Section 4.4 deals with a *customer* (an individual or legal person) who is acting for a legal arrangement, and Section 4.5 deals with a *customer* who is a legal person.

6. As noted in the Glossary above, references to a *customer* include, where appropriate, a prospective *customer* (an applicant for business) with whom a *business relationship* is to be established or a *one-off transaction* carried out.

7.2 Requirement to apply enhanced CDD measures

Statutory requirements (paraphrased wording)

7. *Article 11(3)(c) of the Money Laundering Order requires a relevant person to maintain appropriate and consistent policies and procedures to determine whether:*

(i) a customer

(ii) a beneficial owner or controller of a customer;

(iii) a third party for whom a customer is acting;

(iv) a beneficial owner or controller of a third party described in (iii);

(v) a person acting, or purporting to act, on behalf of a customer is a PEP; or

(vi) a beneficiary under a life insurance policy.

8. *Article 11(3)(d) of the Money Laundering Order requires a relevant person to maintain appropriate and consistent policies and procedures to determine whether a business relationship or one-off transaction is with a person connected with a country or territory that does not apply, or insufficiently applies, the FATF Recommendations.*

9. *Article 15(1) of the Money Laundering Order requires a relevant person to apply enhanced CDD measures on a risk-sensitive basis in the following circumstances:*

a) if a customer has, or proposes to have, a business relationship or proposes to carry out a one-off transaction with the relevant person and the relevant person is not resident in the customer's country of residence or in the same country as the country from which, or from within which, the customer is carrying on business

b) if a customer has not been physically present for identification purposes

c) if the relevant person has or proposes to have a business relationship or proposes to carry out a one-off transaction with a customer having a relevant connection with a country or territory (an "enhanced risk state") in relation to which the FATF has called for the application of enhanced customer due diligence measures

d) if the customer of the relevant person is a company with nominee shareholders or that issues shares in bearer form

da) if the customer of the relevant person is a limited liability company with nominee LLC interest holders

e) if the customer of the relevant person is:

i) a legal person established by an individual for the purpose of holding assets for investment purposes or

ii) a person acting on behalf of a legal arrangement established for an individual for the purpose of holding assets for investment.

f) if the relevant person provides or proposes to provide a customer with private banking services

g) any situation which by its nature can present a higher risk of money laundering.

7.3 Higher risk customer

Overview

10. Section 3.3 of this Handbook explains the risk-based approach to *identification measures*. It explains that a *supervised person* must, on the basis of information collected, assess the risk that a *business relationship* or *one-off transaction* will involve *money laundering,* the *financing of terrorism,* or the *financing of proliferation*.

11. Enhanced *CDD* measures must be applied where a *supervised person's* assessment is that there is a higher risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* (i.e. a situation which by its nature can present a higher risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*).

12. There are a number of reasons why a *business relationship* or *one-off transaction* might be assessed as presenting a higher risk. For this reason, there are a number of possible measures listed in this section to address that risk.

Guidance notes

13. A *supervised person* may demonstrate that it has applied enhanced *identification measures* to an individual who is a higher risk *customer* under Article 15 of the *Money Laundering Order* where it obtains evidence that verifies a:

› former name (if applicable) or

› passport or national identity card number.

14. A *supervised person* may demonstrate that it has applied enhanced *identification measures* to a higher risk *customer* under Article 15(1)(g) of the *Money Laundering Order* where it takes reasonable measures to find out the ***source of funds*** and ***source of wealth*** at the time that a *business relationship* is established or *one-off transaction* carried out which are commensurate with risk and include one or more of the following:

› commissioning an independent and reliable report from a specialist security agency about the *source of funds* involved and/or *customer's source of wealth*

› where a *supervised person* is part of a group, obtaining reliable information from the group's internal security department or business intelligence unit (or equivalent) about the *source of funds* involved and/or *customer's source of wealth*

› where a *supervised person* is part of a group, obtaining reliable information from a part of the group which has an office in the country or territory with which the *customer* has a connection about the *source of funds* involved and/or *customer's source of wealth*

› obtaining reliable information directly from the *customer* concerned, for instance during (or subsequent to) a face to face meeting inside or outside Jersey, or via a telephone "welcome call" on a home or business number which has been verified or by obtaining certified copies of corroborating documentation such as contracts of sale, property deeds, salary slips, etc

› obtaining reliable information from an external party (for instance a solicitor, accountant or tax advisor) which has an office in the country or territory with which the *customer* has the connection about the *source of funds* involved and/or *customer's source of wealth*

› obtaining reliable information from a person eligible to be an *obliged person* (for instance a solicitor, accountant or tax advisor) about the *source of funds* involved and/or *customer's source of wealth*

› where information is publicly available or available through subscription databases, obtaining reliable information from a public or private source about the *source of funds* involved and/or *customer's source of wealth*

› obtaining reliable information through financial statements that have been prepared in accordance with generally accepted accounting principles and audited in accordance with generally accepted auditing standards.

15. Where a connection is established during the course of an existing relationship, a *supervised person* may also demonstrate that it has taken reasonable measures to find out the *source of funds* and/or *source of wealth* where it reviews the relationship information that it already holds and concludes that it is reliable.

16. Where the measures set out in Paragraph 13 to 15 above are not sufficient to mitigate the risk associated with the *customer*, a *supervised person* may demonstrate that it has applied enhanced *identification measures* where it does one or more of the following in a way that is commensurate with risk:

› in a case where a document that has been used to obtain evidence of identity for a higher risk *customer*, e.g. a passport, subsequently expires, a *supervised person* may demonstrate that documents, data or information obtained under identification measures are kept up to date and relevant where a copy of the document that replaces that originally used to obtain evidence of identity is requested and obtained

› in a case where a *business relationship* is to be established making use of a suitable certifier, it obtains confirmation that a photograph contained in the document certified bears a true likeness to the individual requesting certification (or words to that effect).

17. A *supervised person* may demonstrate that it has applied enhanced on-going monitoring to a higher risk *customer* where it:

› reviews the *business relationship* on at least an annual basis, including all documents, data and information obtained under *identification measures* in order to ensure that they are kept up to date and relevant

› where monitoring thresholds are used, sets lower thresholds for transactions connected with the *business relationship*.

7.4 Customer not physically present for Identification Measures

Overview

18. Frequently, business relationships will be established and one-off transactions carried out where there is no face to face contact with the *customer* to be identified or its *beneficial owners or controllers*, for example:

› relationships established with individuals by mail, telephone or via the internet where external data sources are used to obtain evidence of identity

› where identity is found out on persons who fall within Article 3(7) of the Money Laundering Order through a trustee or general partner, or on *beneficial owners and controllers* of a legal person through that legal person.

19. There may also be circumstances where there is face to face contact with a *customer*, but where documentary evidence is to be provided at a time when the *customer* is not present.

20. Such circumstances may increase the risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* as it may be easier for criminals to conceal their true identity when there is no face to face contact with the *supervised person*. They may also increase the risk of impersonation or identity fraud being used to establish a *business relationship* or conduct a *one-off transaction* for illegitimate purposes.

21. For the avoidance of doubt, this section does not cover a person whose identity has been verified through a suitable certifier, (e.g. **where the certifier has met the person at the time the documents are certified**).

Statutory requirements (paraphrased wording)

22. *Under Article 15(1)(b) of the Money Laundering Order, if a customer has not been physically present for identification purposes, a relevant person must apply enhanced CDD measures on a risk-sensitive basis.*

AML/CFT/CPF Codes of Practice

23. A *supervised person* must apply enhanced *CDD* measures on a risk-sensitive basis where a person who falls within Article 3(7) of the Money Laundering Order, or who is the *beneficial owner or controller* of a *customer*, or is a person who must otherwise be identified under Article 3 of the *Money Laundering Order* is not physically present for identification purposes.

Guidance notes

24. A *supervised person* may demonstrate that it has applied enhanced identification measures:

› under Article 15 of the *Money Laundering Order* and

› under the *AML/CFT/CPF Code of Practice* set at Paragraph 23 above

Where it finds out further information on a person (in this example, “Person A”), obtains an additional form of evidence of identity for Person A, or carries out some other additional measure in respect of Person A.

25. Additional forms of evidence of identity may include use of a further source listed in Section 4 (including independent data sources).

26. Other additional measures may include:

› where a *supervised person* is part of a group, confirmation from another part of that group that Person A has been met face-to-face

› confirmation from a *supervised person* that carries on a *regulated business* or a person who carries on an *equivalent business* that Person A has been met face to face

› confirmation from a *supervised person* that carries on *Trust Company Business* or a person who carries on an *equivalent business* that Person A is known to the trust and company services provider, and the trust and company services provider is satisfied that the particular individual is the person whose identity is to be found out

› a combination of other checks that adequately take into account the *supervised person’s* risk assessment for Person A, including:

- requiring the first payment for the product or service to be drawn on an account in the *customer's* name at a bank that is a *regulated person* or carries on *equivalent business* (refer to Section 1.8)
- telephone contact with the *customer* prior to establishing a relationship on a home or business number which has been verified, or a "welcome call" to the *customer* before transactions are permitted, using the call to verify additional components of identity found out
- internet sign-on following verification measures where the *customer* uses security codes, tokens, and/or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address
- specific card or account activation measures.

7.5 Customer with relevant connection to an enhanced risk state

Overview

27. The *FATF* has identified a number of countries and territories which have failed to address their own *money laundering*, *financing of terrorism,* and *proliferation financing* risks and/or have in place insufficient *AML/CFT/CPF* regimes, in relation to which it has called for the application of countermeasures. These countries or territories are referred to in the Money Laundering Order as *enhanced risk states* and that definition is reflected in the Glossary above. A person with a *relevant connection* to these countries or territories presents a higher risk of being involved in *money laundering*, the *financing of terrorism,* or the *financing of proliferation*, and doing business with such a person also poses an increased risk.

28. For the purpose of applying Article 15(1)(c) of the Money Laundering Order, *enhanced risk states* are those listed in Appendix D1 of this Handbook.

7.5.1 Application of enhanced CDD measures to a customer with a relevant connection to an enhanced risk state

Statutory requirements (paraphrased wording)

29. *Under Article 15(1)(c) of the Money Laundering Order, if the relevant person has or proposes to have a business relationship or proposes to carry out a one-off transaction with a customer having a relevant connection with a country or territory (an "enhanced risk state") in relation to which the FATF has called for the application of enhanced customer due diligence measures, a relevant person must apply enhanced CDD measures on a risk-sensitive basis.*

30. *Under Article 15(2)(a) of the Money Laundering Order, for the purpose of the Article 15(1)(c), a "customer" includes any of the following:*

a) a beneficial owner or controller of the customer

b) a third party for whom the customer is acting

c) a beneficial owner or controller of a third party described above

d) a person acting, or purporting to act, on behalf of the customer.

31. *Under Article 15(2)(b) of the Money Laundering Order a person has a relevant connection with an enhanced risk state if the person is:*

a) the government or a public authority of that state

b) in relation to that state, a foreign PEP (within the meaning of Article 15A)

c) a person resident in that state

d) a person having an address for business in that state

e) A customer, where the source of the customer's funds is or derives from assets held in that state by the customer or by any person on behalf of the customer or income arising in that state.

AML/CFT/CPF Codes of Practice

32. The *enhanced CDD measures* applied to a *customer* with a *relevant connection* to an *enhanced risk state* must include:

› requiring any new *business relationship* (and continuation thereof) or *one-off transaction* to be approved by the senior management function

› where there is a *relevant connection* because a *customer's source of funds* is, or derives, from:

- assets held in the state by the *customer* or by any person on behalf of the *customer* or
- income arising in the state

Taking reasonable measures to find out the *customer's source of wealth*.

Guidance notes

33. A *supervised person* may demonstrate that it has taken reasonable measures to find out the *source of wealth* at the time that a *business relationship* is established or *one-off transaction* carried out, where the measures taken are commensurate with risk and include one or more of the measures listed in Paragraph 14 above.

34. Where a *relevant connection* is established during the course of an existing relationship, a *supervised person* may also demonstrate that it has taken reasonable measures to find out the *source of wealth* where it reviews the relationship information that it already holds and concludes that it is reliable.

35. A *supervised person* may demonstrate that it has otherwise applied *enhanced CDD measures* where it does all of the following:

› in a case where a document that has been used to obtain evidence of identity for a higher risk *customer*, e.g. a passport, subsequently expires, a *supervised person* may demonstrate that documents, data or information obtained under *identification measures* are kept up to date and relevant where a copy of the document that replaces that originally used to obtain evidence of identity is requested and obtained

› in a case where a relationship is to be established making use of a suitable certifier, it obtains confirmation that a photograph contained in the document certified bears a true likeness to the individual requesting certification (or words to that effect)

› reviews the *business relationship* on at least an annual basis, including all documents, data and information obtained under *identification measures* in order to ensure that they are kept up to date and relevant

› where monitoring thresholds are used, sets lower thresholds for transactions connected with the *business relationship*.

7.6 Customer who is a Politically Exposed Person (PEP)

Overview

36. Corruption by *PEPs* will inevitably involve serious crime, such as theft or fraud, and is of global concern. The proceeds of such corruption are often transferred to other countries and territories and concealed through private companies, trusts or foundations, frequently under the names of relatives or close associates of the perpetrator.

37. By their very nature, *money laundering* investigations involving the proceeds of corruption generally gain significant publicity and are therefore very damaging to the reputation of both the businesses and countries/territories concerned. This is in addition to the possibility of criminal charges.

38. Indications that a *customer* may be connected with corruption include excessive revenue from "commissions" or "consultancy fees" or involvement in contracts at inflated prices, where unexplained "commissions" or other charges are paid to external parties.

39. The risk of handling the proceeds of corruption, or becoming engaged in an arrangement that is designed to facilitate corruption, is greatly increased where the arrangement involves a *PEP*. Where the *PEP* also has connections to countries or business sectors where corruption is widespread, the risk is further increased.

40. The nature of *enhanced CDD measures* applied will be commensurate with the risk that is identified and nature of the *PEP* connection. In particular, the measures to be applied by a *supervised person* to a PEP:

› who is the Minister of Finance in a country that is prone to corruption may be very different to the measures to be applied to a senior politician with a limited portfolio in a country or territory that is not prone to corruption

› as another example, the measures to be applied to a company that is a *collective investment scheme*, the securities of which are traded on a recognised market, and which has an investor who is a *PEP* with a 1% holding in the scheme, may be very different to a private company established exclusively to hold investments for a *PEP*.

41. As a result, there is no "one-size fits all" approach to applying *enhanced CDD measures* for *PEPs*.

42. Whilst *PEP* status does not in itself incriminate individuals or entities, it will mean that the *customer* may be subject to *enhanced CDD measures*. The nature and scope of a *supervised person's* activities will generally determine whether the existence of *PEPs* in its *customer* base is a practical issue for the *supervised person*.

7.6.1 Determining whether a customer is a PEP

Statutory requirements (paraphrased wording)

43. *Article 15A(3) of the Money Laundering Order provides the following definitions of PEP categories, which include an immediate family member or a close associate of the person:*

"domestic politically exposed person" *means a person who is an individual who is or has been entrusted with a prominent public function in Jersey including but not limited to:*

- *heads of state, heads of government, senior politicians*
- *senior government, judicial or military officials*
- *senior executives of state owned corporations*
- *important political party officials.*

"foreign politically exposed person" *means a person who is an individual who is or has been entrusted with a prominent public function in a country or territory outside Jersey including but not limited to:*

- *heads of state, heads of government, senior politicians*
- *senior government, judicial or military officials*
- *senior executives of state owned corporations*
- *important political party officials.*

"prominent person" *means a person who is an individual who is or has been entrusted with a prominent public function by an international organisation.*

"immediate family member" *includes any of the following:*

- *a spouse*
- *a partner, that is someone considered by their national law as equivalent or broadly equivalent to a spouse*
- *children and their spouses or partners (as defined above)*
- *parents*
- *grandparents and grandchildren*
- *siblings.*

"close associate" *of a person includes any person who is known to maintain a close business relationship with the person, including a person who is in a position to conduct substantial financial transactions on behalf of the person.*

44. *Under Article 15A(4) of the Money Laundering Order, for the purpose of deciding whether a person is a close associate of a person, a relevant person need only have regard to information which is in that person's possession or is publicly known.*

7.6.2 Enhanced customer due diligence measures in relation to PEPs

Statutory requirements (paraphrased wording)

45. *Article 15A of the Money Laundering Order applies to a relevant person:*

› *who has or proposes to have a business relationship with, or proposes to carry out a one-off transaction with, a foreign politically exposed person or*

› *who has or proposes to have a high risk business relationship, or proposes to carry out a high risk one-off transaction with, a domestic politically exposed person or prominent person or*

› *if any of the following is a foreign politically exposed person or, in the case of a high risk business relationship or one-off transaction, a domestic politically exposed person or prominent person:*

i) a beneficial owner or controller of the customer of the relevant person

ii) a third party for whom the customer of the relevant person is acting

iii) a beneficial owner or controller of a third party described in clause (ii) above

iv) a person acting or purporting to act on behalf of the customer of the relevant person.

46. *A relevant person to whom Article 15A applies must apply enhanced customer due diligence measures on a risk-sensitive basis including:*

› *unless the relevant person is a sole trader, measures requiring a new business relationship or continuation of a business relationship or a new one-off transaction to be approved by the senior management of the relevant person*

› *measures to establish the source of the wealth of the politically exposed person and source of the funds involved in the business relationship or one-off transaction*

› *measures to conduct the enhanced ongoing monitoring of that relationship and*

› *if the relevant business relationship relates to a life insurance policy, measures requiring the senior management to be informed before any payment is made under the policy or any right vested under the policy is exercised.*

In Article 15A:

***"enhanced ongoing monitoring"** means ongoing monitoring that involves specific and adequate measures to compensate for the higher risk of money laundering.*

***"high risk"**, in relation to a business relationship or one-off transaction, means any situation which by its nature can present a higher risk of money laundering.*

***"source of the wealth"** means the source generating the total net worth of funds of the politically exposed person, whether those funds are used in the business relationship or one-off transaction.*

AML/CFT/CPF Codes of Practice

47. *Policies and procedures* maintained in line with Article 11 of the Money Laundering Order must recognise that customers may subsequently acquire *PEP* status.

Guidance notes – Foreign *PEPs*

48. Where the existence of foreign *PEPs* is considered to be a practical issue, a *supervised person* may demonstrate that it has appropriate *policies and procedures* for determining whether a *customer* or prescribed person is a *PEP* where it:

› assesses those countries and territories to which *customers* are connected, which pose the highest risk of corruption. See Section 3.3.4.1 of this Handbook

- finds out who the current and former holders of prominent public functions are within those higher risk countries and territories and determines, as far as is reasonably practicable, whether or not *customers* have any connections with such individuals (including through immediate family or close associates). In determining who the current and former holders of prominent public functions are, it may have regard to information already held by the *supervised person* and to external information sources such as the *UN*, the European Parliament, the UK Foreign, Commonwealth & Development Office, the Group of States against Corruption, and other external data sources (see Section 3.3.4.2 of this Handbook) and

- exercises vigilance where *customers* are involved in business sectors that are vulnerable to corruption such as (but not limited to) oil or arms sales.

49. Where a *supervised person* runs the details of all its *customers* and prescribed persons through an external data source (e.g. a screening package) to determine whether any of them are *PEPs*, it should nevertheless also assess those countries and territories to which *customers* are connected, which pose the highest risk of corruption, and exercise particular vigilance where *customers* are involved in business sectors that are vulnerable to corruption.

50. In a case where a *PEP* is a director (or equivalent) of a *customer*, or person acting or purporting to act for a *customer*, and where no property of that *PEP* is handled in the particular *business relationship* or *one-off transaction*, a *supervised person* may demonstrate that it applies specific and adequate measures under Article 15A(2) of the *Money Laundering Order* where it considers the nature of the *PEP's* connection and reason why the *PEP* has such a connection.

51. Similarly, where a *PEP* is a trustee or a general partner that is a *customer*, or is a beneficiary or object of a power of a trust, and where no property of that *PEP* is handled in the particular *business relationship* or *one-off transaction*, a *supervised person* may demonstrate that it applies specific and adequate measures under Article 15A(2) of the *Money Laundering Order* where it considers the nature of the *PEP's* connection and reason why the *PEP* has such a connection.

Guidance notes – Domestic *PEPs*

52. In determining whether someone is a domestic *PEP*, a *supervised person* should consider the criterion set out at Article 15A(3) of the Money Laundering Order – namely that a *PEP* is an individual who is or has been entrusted with a prominent public function, for example:

- heads of state, heads of government, senior politicians

- senior government, judicial or military officials

- senior executives of state owned corporations

- important political party officials.

53. In the context of Jersey, this will include (but is not limited to) the following positions:

- Lieutenant-Governor

- Ministers (but not necessarily deputy Ministers)

- Chief Executive of the States of Jersey

- Director-Generals of the States of Jersey

- HM Attorney-General
- HM Solicitor-General
- Commissioners of the *JFSC*
- Director General of the *JFSC*
- Registrar of Companies
- Information Commissioner
- Comptroller and Auditor-General
- Bailiff
- Deputy Bailiff
- Judicial Greffier
- Comptroller of Taxes
- HM Receiver General
- Senior Executives of State Owned Body Corporates (or similar)

54. Note that this will also include immediate family members and close associates of individuals listed above.

7.6.2.1 Higher Risk Domestic PEPs

55. As set out in Article 15A(1)(b) of the Money Laundering Order, mandatory *enhanced CDD measures* are only required in relation to *business relationships* or *one-off transactions* with domestic *PEPs* which are assessed as higher risk.

56. Individuals entrusted with a prominent public function in Jersey may be considered to pose a low risk, unless a *supervised person* considers that other specific risk factors indicate a higher risk. Particular consideration should be given to the following characteristics that might indicate a higher risk:

- responsibility for, or ability to influence, large public procurement exercises
- responsibility for, or ability to influence, allocation of government licenses (or similar)
- personal wealth or lifestyle inconsistent with known legitimate sources of income or wealth
- credible allegations of financial misconduct.

57. Similarly, immediate family or close associates of individuals entrusted with a prominent public function in Jersey may be considered to pose a low risk, unless a *supervised person* considers that other specific risk factors indicate a higher risk. Particular consideration should be given to the following characteristics that might indicate a higher risk:

- wealth or lifestyle inconsistent with known legitimate sources of income or wealth
- credible allegations of financial misconduct

› wealth derived from the granting of government licences (or similar)

› wealth derived from preferential access to the privatisation of former state assets.

7.7 Non-resident customer

Overview

58. *Customers* who are not resident in a country or territory but who nevertheless seek to form a *business relationship* or conduct a *one-off transaction* with a *supervised person* in that country or territory will typically have legitimate reasons for doing so. Some *customers* will, however, pose a risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* and may be attempting to move illicit funds away from their country or territory of residence or attempting to further conceal funds sourced from that country or territory.

Statutory requirements (paraphrased wording)

59. *Under Article 15(1)(a) of the Money Laundering Order, if a customer has, or proposes to have, a business relationship or proposes to carry out a one-off transaction with the relevant person and the relevant person is not resident in the customer's country of residence or in the same country as the country from which, or from within which, the customer is carrying on business, a relevant person must apply enhanced customer due diligence measures on a risk-sensitive basis.*

Guidance notes

60. A *supervised person* may demonstrate that it has applied *enhanced CDD measures* under Article 15(1)(a) of the Money Laundering Order, where it has applied additional measures that are commensurate with risk. Additional measures may include one or more of the following:

› determining the reasons why the *customer* is looking to establish a *business relationship* or carry out a *one-off transaction* other than in their home country or territory and/or

› the use of external data sources to collect information on the *customer* and the country risk of the *customer's* home country or territory (see Section 3.3.4.1) in order to build a *customer* business and risk profile similar to that available for a resident *customer*.

7.8 Customer provided with private banking services

Guidance notes

61. Private banking is generally understood to be the provision of banking and investment services to high net worth *customers* in closely managed relationships. It often involves complex, bespoke arrangements and high value transactions across multiple countries and territories. Such *customers* may therefore present a higher risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*.

62. For the avoidance of doubt, a trustee who may from time to time facilitate such banking or investments services as part of carrying on *trust company business* is not considered to be providing private banking services, where such facilitation is ancillary to the core business of acting as a trustee.

Statutory requirements (paraphrased wording)

63. *Under Article 15(1)(f) of the Money Laundering Order, if the relevant person provides or proposes to provide a customer with private banking services, a relevant person must apply enhanced CDD on a risk-sensitive basis.*

64. *Under Article 15(3), a service is a "private banking service" if the service is offered, or it is proposed to offer the service, only to persons identified by the service provider as being eligible for the service, having regard to the person's net worth, and the service:*

a) involves a high value investment

b) is a non-standard banking or investment service tailored to the person's needs, or uses corporate or trust investment structures, tailored to the person's needs or

c) offers opportunities for investment in more than one jurisdiction.

Guidance notes

65. A *supervised person* may demonstrate that it has applied *enhanced CDD measures* under Article 15(1)(f) of the *Money Laundering Order* in respect of a private banking relationship, where it has applied additional measures that are commensurate with risk. Additional measures may include:

› taking reasonable measures to find out the *source of funds* and *source of wealth*

› reviewing the *business relationship* on at least an annual basis, including all documents, data and information obtained under *identification measures* in order to ensure that they are kept up to date and relevant

› where monitoring thresholds are used, setting lower thresholds for transactions connected with the *business relationship*.

7.9 Customer that is a personal asset holding vehicle

Overview

66. Personal asset holding vehicles are legal persons or legal arrangements established by individuals for the specific purpose of holding assets for investment. The use of such persons or arrangements may make identification of *ultimate beneficial owners* more difficult since layering of ownership may conceal the true source or controller of the investment.

67. Article 15(1)(e) of the Money Laundering Order is intended to apply in two specific scenarios:

› where the personal asset holding vehicle is the *customer* or

› where the personal asset holding vehicle is the third party for whom a trustee or general partner (the *customer*) is acting.

Guidance notes

68. A *supervised person* may demonstrate that it has applied *enhanced CDD measures* under Article 15(1)(e) of the Money Laundering Order, where it has applied additional measures that are commensurate with risk. Additional measures may include:

› understanding the structure of the vehicle, determining the purpose and rationale for making use of such a vehicle, and being satisfied that the *customer's* use of such an investment vehicle has a genuine and legitimate purpose

› taking reasonable measures to find out and document the *source of funds* and *source of wealth*.

7.10 Customer that is a company with nominee shareholders or issues bearer shares

Overview

69. Companies with nominee shareholders or bearer shares (or the ability to issue bearer shares in the future) may present a higher risk because such arrangements make it possible to hide the identity of the *beneficial owner(s)* and/or changes in beneficial ownership by separating legal and beneficial ownership, or because there is no trail of ownership, which introduces a degree of anonymity.

70. Nevertheless, nominee shareholders are often used for good and legitimate reasons, e.g. to ease administration and reduce client costs by enabling a nominee to take necessary corporate actions, such as the passing of resolutions, in the day to day administration of a corporate structure.

71. Where one or more of the following circumstances apply, the *customer* **should not** be considered to be a *customer* that issues bearer for the purpose of Article 15(1) of the Money Laundering Order:

› the bearer shares are issued by a company in a country or territory that has fully enacted appropriate legislation to require bearer shares to be registered in a public registry and the bearer shares are so registered or

› the bearer shares are traded on an approved stock exchange or

› all issued bearer shares are held in the custody of the *supervised person*, the *customer* or trusted external party along with an undertaking from that trusted external party or *customer* to inform the *supervised person* of any transfer or change in ownership.

Statutory requirements (paraphrased wording)

72. *Under Article 15(1)(d) of the Money Laundering Order, if a customer of a relevant person is a company with nominee shareholders or that issues shares in bearer form, a relevant person must apply enhanced CDD measures on a risk-sensitive basis.*

Guidance notes

73. A *supervised person* may demonstrate that it has applied *enhanced CDD measures* under Article 15(1)(d) of the Money Laundering Order, where it has applied additional measures that are commensurate with risk.

74. In the case of *customers* who are companies with nominee shareholders, additional measures may include:

› determining and being satisfied with the reasons why the *customer* is making use of nominees

› using external data sources to collect information on the fitness and propriety of the nominee (such as its regulated status and reputation) and the particular country risk.

75. In the case of *customers* who are companies with bearer shares (or the ability to issue bearer shares in the future), additional measures may include:

- determining and being satisfied with the reasons why the *customer* has issued bearer shares or retains the ability to do so
- ensuring that any new or continued business relationship or any one-off transaction is approved by the senior management of the supervised person
- reviewing the *business relationship* on at least an annual basis, including all documents, data and information obtained under *identification measures* in order to ensure that they are kept up to date and relevant.

7.11 Correspondent banking and similar relationships

Overview

76. "Correspondent banking" is a term given to the provision of banking services by a *supervised person* (i.e. the **correspondent**) to another overseas financial institution (i.e. the **respondent**) for the benefit of the *customers* of the respondent. As a result, the *correspondent* indirectly makes its services available to the *customers* of the *respondent*. In doing so, the *correspondent* potentially exposes itself to additional risk. This section sets out the additional *CDD* measures required where a *correspondent* enters into a *correspondent relationship* with a *respondent* to appropriately manage the risk presented by that relationship.
77. *FATF* standards also require financial institutions to apply enhanced measures in relation to **other similar relationships**, for example, those established for securities transactions or funds transfers, whether for the cross-border financial institution as principal or for its *customers*.
78. *Supervised persons* that are registered under the BB(J)L are prohibited by the *Money Laundering Order* from entering into banking relationships with "**shell banks"**.

Statutory requirements (paraphrased wording)

79. *Article 15B of the Money Laundering Order applies to a relevant person who has or proposes to have a banking or similar relationship with an institution whose address for that purpose is outside Jersey.*
80. *Under Article 15B(2) of the Money Laundering Order a relevant person must apply enhanced customer due diligence measures on a risk-sensitive basis including:*
    - *gathering sufficient information about the institution to understand fully the nature of its business*
    - *determining the reputation of the institution and the quality of its supervision, including whether it has been subject to any money laundering investigation or regulatory action*
    - *assessing the institution's systems and controls to combat money laundering in order to determine whether they are consistent with the requirements of the FATF recommendations and their effectiveness*
    - *requiring any new relationship to be approved by the senior management of the relevant person*
    - *ensuring that both the relevant person and the institution clearly understand their respective responsibilities to prevent and detect money laundering and recording those responsibilities*

› *being satisfied that, in respect of customers of the institution who have services provided directly by the relevant person, that the institution has applied customer due diligence measures at least equivalent to those set out in this Order and is able to provide a copy, at the request of the relevant person, of the evidence, documents, data and information obtained when applying such measures.*

81. *Article 23A(1) of the Money Laundering Order provides that a relevant person that is a correspondent bank must not enter into a correspondent banking relationship, or continue an existing correspondent banking relationship, with a respondent that is a shell bank.*

82. *Article 23A(2) of the Money Laundering Order provides that a relevant person that is a correspondent bank must take appropriate measures to ensure that it does not enter into a correspondent banking relationship, or continue an existing correspondent banking relationship, with a bank that is known to permit its accounts to be used by a shell bank.*

83. *Article 23A(4)(b) defines "shell bank" as a bank incorporated in a jurisdiction in which it has no physical presence involving meaningful decision-making and management, and which is not subject to supervision by the JFSC or by an overseas regulatory authority by reason of that bank's connection with any other institution or person.*

Guidance notes

84. This part applies to all *supervised persons* that have *banking or similar relationships* with an overseas *Institution*.

85. Banking or similar relationships include:

    a) the provision of banking services by a *supervised person* to an Overseas Financial *Institution* including providing a current or other liability account and related services, such as cash management, international funds transfers, cheque clearing, providing customers of the *Institution* with direct access to accounts with the *supervised person* (and vice versa) and providing foreign exchange services; or
    b) other relationships whereby similar services are provided by a *supervised person* to an *Institution*, including relationships established for securities transactions or funds transfer.

86. An institution's address for this purpose should be considered to be overseas unless the transaction is with the Jersey office of a business.

87. A *supervised person* may demonstrate that it has gathered sufficient information about the institution to fully understand the nature of its business where it obtains information concerning the following:

› the geographic location of its *customer* base

› the general nature of its *customer* base

› the nature of the services which the *Institution* provides to its *customers*

› whether relationships are conducted by the *Institution* on a non-face to face basis

› the extent to which the *Institution* relies on third parties to identify and hold evidence of identity or to conduct other *CDD* measures on *customers*.

88. A *supervised person* may determine the institution's reputation by assessing its stature from publicly-available information from credible sources on the reputation of the institution and the quality of the supervision to which the institution is subject.

89. A *supervised person* may determine that an institution's *systems and controls* are consistent with the requirements of the *FATF Recommendations* where the institution carries on *equivalent business* (see Section 1.8 of this Handbook).

90. Where *customers* of the *Institution* have direct access to the services of the *supervised person*, a *supervised person* may satisfy itself as to the adequacy of an institution's *CDD* measures, and its ability to provide relevant *CDD* information and documents on request where either:

    a) It obtains a written assurance from the institution to this effect; or

    b) The correspondent bank may also satisfy itself as to the adequacy of the *CDD* measures of the respondent and its ability to produce information and documentation on request by periodically requesting relevant *CDD* information and documents from the institution.

91. Regarding the definition of a shell bank, "physical presence" means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.

7.12 Enhanced CDD measures – transitional arrangements

Overview

92. Where amendments to the *Money Laundering Order* introduce new *CDD* requirements applicable to *business relationships* and *one-off transactions*, these requirements do not apply retrospectively and no remediation project is required.

93. However, Article 13(1)(c)(ii) of the *Money Laundering Order* requires a *supervised person* to apply *identification measures* where the *supervised person* has doubts about the veracity or adequacy of documents, data or information previously obtained. In the context of this section, this would include where documents, data or information previously obtained for a *business relationship* do not satisfy additional new CDD requirements, such as those set out in the *Money Laundering (Amendment No.10) (Jersey) Order 2019* (the **No.10 Amendment Order**).

94. This means that where, during the course of its regular review of a *business relationship* (pursuant to Article 3(3)(b) of the *Money Laundering Order* and discussed at Section 3.4 of this Handbook) a *supervised person* becomes aware that documents, data or information previously obtained do not satisfy the additional *CDD* requirements set out in the No.10 Amendment Order (or any other subsequent amendments), the *supervised person* will need to apply CDD measures to that *customer* at that time, in line with the requirement in Article 13(1)(c)(ii) of the *Money Laundering Order*.

7.13 Exemptions from CDD Requirements – Overview

Overview

95. Part 3A of the *Money Laundering Order* provides for exemptions from *CDD* requirements that apply in some strictly limited circumstances, as set out in Articles 17B - D and 18.

96. Article 17A of the *Money Laundering Order* provides circumstances in which exemptions under Part 3A do not apply. See the table below:

Circumstances in which exemptions under Part 3A do not apply *(Article 17A)*	
Exemptions under Articles 17 B-D	**Exemptions under Article 18**

› the *supervised person* suspects *money laundering*	› the *supervised person* suspects *money laundering*
› the *supervised person* considers that there is a higher risk of *money laundering*, including the risk of *money laundering* if fail to apply appropriate identification measures or keep records.	› the *supervised person* considers that there is a higher risk of *money laundering*
› the *customer* is resident in a country that is not compliant with the *FATF recommendations*	› the *customer* is resident in a country that is not compliant with the *FATF recommendations*
› the *customer* is a person in respect of whom Article 15(1)(c) applies [specified persons having a *relevant connection* to country/territory in relation to which *FATF* has called for enhanced customer due diligence]	› the *customer* is a person in respect of whom Article 15(1)(c) applies [specified persons having a *relevant connection* to country/territory in relation to which *FATF* has called for enhanced customer due diligence]
› the *customer* is a person in respect of whom Article 15B(1) applies [certain deposit taking businesses with a banking or similar relationship with an institution whose address for that purpose is outside Jersey]	

97. Definitions for various terms used within Part 3A of the *Money Laundering Order* and this section are set out below (save that relevant person is replaced with supervised person) :

› **Relevant customer** means a *customer* of a *supervised person* that the *supervised person* knows or reasonably believes is:

- a *supervised person* in respect of whose *financial services business* the *JFSC* discharges supervisory functions, or a person carrying on *equivalent business;* or
- a person wholly owned by a *supervised person* described in the above point (the "parent"), but only if:
  - the person is incorporated or registered in the same jurisdiction as the parent
  - the person has no customers who are not customers of the parent
  - the person's activity is ancillary to the business in respect of which the *JFSC* discharges supervisory functions, or to *equivalent business* carried on by the parent; and
  - in relation to that activity, the person maintains the same policies and procedures as the parent.

› **third party identification requirements** means the requirements of Article 13 or 15, 15A, 15B to apply the *identification measures* specified in Article 3(2)(b)

› **non-public fund** means a scheme falling within the definition of "collective investment fund" in Article 3 of the CIF(J) Law, except that the offer of units in the scheme or arrangement is not an offer to the public within the meaning of that Article.

98. Exemptions from *identification measures* may only be applied in appropriate circumstances. Where specified, this will require an assessment of the risk of applying the exemption, in addition to a customer risk assessment.

Guidance notes

99. Articles 18 and 17B-D can be applied to the same *customer* relationship, as they apply to separate identification requirements, however there are some elements of customer due diligence that the *supervised* person will always be required to undertake – see the tables below:

CDD Element	Always required to be undertaken by the supervised person
Identification measures	Risk assessment
	Obtain information on purpose/nature
On-going monitoring	Scrutinising transactions/activity
	Keep documents/information up-to-date

CDD Element	Articles 17B-D provide an exemption from this obligation
Identification measures	ID third parties

CDD Element	Article 18 provides an exemption from this obligation (N.B. does not apply to third parties)	
Identification measures	ID *customer*	
	ID person acting for *customer*	Verify authority to act
	Where *customer* is not an individual:	Understand ownership/control structure
		ID *beneficial owners/controllers*

100. Article 18 only applies to the *customer* and does not extend to third parties. For example, Article 18 would apply to a general partner of a limited partnership or a trustee of a trust, but not to the limited partnership or trust itself. Articles 17B-D **can** be applied to third parties which would, for example, encompass the investors in a limited partnership or a unit trust.

7.14 Exemption from applying third party identification requirements in relation to relevant customers acting in certain regulated, investment or fund services business

Statutory requirements (paraphrased wording)

101. *Under Article 17B(1) of the Money Laundering Order, a relevant person is exempt from applying third party identification requirements in relation to a third party for which a relevant customer is acting where the relevant customer is acting in the course of a business:*

› *that falls within Paragraph (a), (b) or (d) in the definition of "regulated business" in Article 1, or equivalent business or*

› *that is an investment business or fund services business registered under the FS(J) Law, or equivalent business.*

102. *Under Article 17B(2) of the Money Laundering Order, a relevant person must record the reasons for applying the exemption, having regard to the risk of money laundering inherent in the relevant customer's business and the higher risk of money laundering associated with that type of business should the relevant customer fail to:*

a) apply the identification measures specified in Article 3(2)(b) or if the relevant customer is not in Jersey, similar identification measures required to be applied to satisfy the requirements in Recommendation 10 of the FATF recommendations or

b) keep records, or keep them for the period required to be kept.

AML/CFT/CPF Codes of Practice

103. A *supervised person* must be able to demonstrate that the exemption conditions required by the *Money Laundering Order* and summarised in the *statutory requirements* above are being met.

7.15 Exemption from applying third party identification requirements in relation to certain relevant customers involved in unregulated or non-public funds, trust company business or the legal profession

Statutory requirements (paraphrased wording)

104. *Under Article 17C(1) of the Money Laundering Order a relevant person is exempt from applying third party identification requirements in relation to a third party for which a relevant customer is acting if the relevant customer:*

a) is, or carries on business in respect of, an unregulated fund, within the meaning of the Collective Investment Funds (Unregulated Funds) (Jersey) Order 2008, or equivalent business

b) is, or carries on business in respect of, a fund that is a non-public fund, being a fund in respect of which a service is provided that is described in Paragraph 7(1)(h) of Part B of Schedule 2 to the Proceeds of Crime Law, or equivalent business

c) carries on trust company business and is registered to carry on such business under the FS(J) Law, or equivalent business, but only if the relevant person is:

i. carrying on deposit-taking business

ii. a lawyer carrying on business described in Paragraph 1 of Part B of Schedule 2 to the Proceeds of Crime Law or

iii. an accountant carrying on a business described in Paragraph 2 of Part B of Schedule 2 to the Proceeds of Crime Law or

d) is an independent legal professional carrying on a business described in Paragraph 1 of Part B of Schedule 2 to the Proceeds of Crime Law and is registered to carry on such business under the Supervisory Bodies Law, but only if the relevant person is carrying on deposit-taking business.

105. *Under Article 17C(2) of the Money Laundering Order, a relevant person who, by virtue of Article 17C(1), does not apply third party identification requirements must:*

a) be satisfied, by reason of the nature of the relationship with the relevant customer, that there is little risk of money laundering occurring and

b) obtain adequate assurance in writing from the relevant customer that the relevant customer:

i. has applied the identification measures specified in Article 3(2)(b) to the third party, or if the relevant customer is not in Jersey, has applied similar identification measures that would satisfy the requirements in recommendations 10 and 12 of the FATF recommendations

ii. will provide the relevant person, without delay and in writing, with the information obtained from applying the identification measures, if so requested by the relevant person

iii. will keep the evidence obtained during the course of applying the identification measures and

iv. will provide the relevant person with that evidence without delay, if requested to do so by the relevant person.

106. *Under Article 17C(3) of the Money Laundering Order the following requirements to adequate assurance apply:*

a) assurance is adequate if it is reasonably capable of being regarded as reliable and the person who relies on it is satisfied that it is reliable

b) assurance may be given in relation to one or more business relationships and for more than one transaction and

c) assurance need not be given before deciding not to comply with third party requirements if an assurance has previously been given by that customer to the relevant person in relation to a business relationship or transaction.

107. *Article 17C(4) of the Money Laundering Order provides that a relevant person (including a person who was formerly a relevant person) who has given an assurance to another person under Article 17C(2)(b) (or under an equivalent provision that applies outside Jersey) may, if requested by the other person, provide the person with the information or evidence obtained from applying the identification measures referred to in Article 17C(2)(b)(i) (See Paragraph 105 above).*

Guidance notes

108. In relation to the exemption set out at Article 17C(1)(a) or (b) of the Money Laundering Order, a *supervised person* may be satisfied that there is little risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* occurring where a particular fund is closed-ended, has no liquid market for its units, and permits subscriptions and redemptions to come from and be returned only to unitholders.

109. In relation to the exemption set out at Article 17C(1)(c)(i) of the Money Laundering Order, a *supervised person* may be satisfied that there is little risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* occurring where:

› deposited funds are held only temporarily for one or more third parties in a client account operated by a person carrying on *trust company business*, pending the transfer to a designated account for a third party, where the funds are not to be held on an undisclosed basis for longer than 40 days

- deposited funds are held only temporarily for one or more third parties in a client account operated by a person carrying on *trust company business*, pending the receipt of instructions when exiting a *customer* relationship, where the funds are not to be held on an undisclosed basis for longer than 40 days
- deposited funds are held only temporarily for one or more third parties in a client account operated by a person carrying on *trust company business*, to facilitate *ad hoc* (not routine) cheque payments where designated accounts do not otherwise have this facility
- deposited funds are held only temporarily for one or more third parties in a client account operated by a person carrying on *trust company business*, to facilitate the aggregation of statutory fees for onward payment
- deposited funds are held only temporarily for one or more third parties in a client account operated by a person carrying on *trust company business*, to receive fees payable to the *customer* which have been paid in advance
- deposited funds are held only temporarily for one or more third parties in a client account operated by a person carrying on *trust company business*, to receive *customer* money on an *ad hoc* basis paid to the *customer* in error
- deposited funds are held for one or more third parties in a client account operated by a person carrying on *trust company business*, where the number and value of third party transactions effected is low, e.g. to provide third parties with access to low-cost banking facilities where third parties' liquid assets are of insufficient value and volume for the establishment of a designated relationship (e.g. balances of £1,000 or less per relationship, with little activity) or
- deposited funds are aggregated by a person carrying on *trust company business* in order to attract a better return on investment for third parties, and where the aggregated deposit is received from and paid back (including income or profit generated) to an account held with another person carrying on deposit-taking business who is registered to do so by the *JFSC*, the Guernsey Financial Services Commission or the Isle of Man Financial Services Authority.

110. In relation to the exemption set out at Article 17C(1)(d) of the Money Laundering Order, a *supervised person* may be satisfied that there is little risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* occurring where the deposit is in respect of a third party's registered contract within the meaning of the *Control of Housing and Work (Jersey) Law 2012*.

111. In relation to the exemptions set out at Article 17C(1)(c)(ii) and (iii) of the Money Laundering Order, guidance on when a *supervised person* may be satisfied that there is little risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* occurring is provided in Section 15.4 and Section 16.5 of this Handbook.

7.15.1 Assessment of risk

Overview

112. The risk factors that are set out in this section will also be relevant to a *customer* risk assessment that is conducted under Section 3.3.4.1 in the cases highlighted at Section 4.4 and Section 4.5 of this Handbook.

Statutory requirements (paraphrased wording)

113. *Immediately before applying the exemptions set out in Part 3A, Article 17B(2) and 17D(2) of the Money Laundering Order require a relevant person to conduct an assessment as to whether it is appropriate to do so, having regard to the relevant customer's business and the higher risk of money laundering should the relevant customer fail to:*

- *apply the necessary identification measures to its customer(s) or*
- *keep records, or keep them for the period required to be kept.*

114. *Article 17B(2) and 17D(2) of the Money Laundering Order require a relevant person to prepare a written record of the reason why it is appropriate to apply CDD exemptions.*

115. *Article 17D(3) of the Money Laundering Order also sets out testing requirements for application of CDD exemptions under Article 17C . Under Article 17D(3) a relevant person must, in the manner, and as often as, the relevant person considers appropriate in all the circumstances, conduct tests in order to establish whether the relevant customer:*

a) has appropriate policies and procedures in place to apply the identification measures described in Articles 13(1)(a), 13(1)(c)(ii) and 15 (or if the relevant customer is not in Jersey, similar identification measures that satisfy the FATF recommendations in respect of identification measures)

b) obtains information in relation to the third party

c) keeps the information or evidence that has been obtained in relation to the third party and

d) provides the relevant person with that information or evidence without delay, if requested to do so by the relevant person.

In conducting such tests, the relevant person must consider whether the relevant customer may be prevented, by application of a law, from providing that information or evidence.

116. *If, as a result of conducting the tests referenced above, the relevant person is unable to establish that the relevant customer complies with the above requirements under Article 17D (3)(b), (c) or (d) of the Money Laundering Order, the relevant person must immediately apply the identification measures specified in Article 13(1)(a) and 13(1)(c)(ii).*

AML/CFT/CPF Codes of Practice

117. In a case where, for a particular *business relationship*, testing under Article 17D(3) of the Money Laundering Order highlights that a relevant customer has not found out information or obtained evidence of identity for a third party (or parties), does not keep that information or evidence of identity, or will not provide it on request and without delay when requested to do so, a *supervised person* must review the basis upon which it has applied *CDD* exemptions to other relationships with that particular relevant customer (if any) in order to determine whether it is still appropriate to apply those measures.

Guidance notes

118. Immediately before applying the exemptions set out in Part 3A of the Money Laundering Order, a *supervised person* may demonstrate that it has had regard to a relevant customer's business where it considers the following factors:

- the general risk appetite of the relevant customer
- the geographic location of the relevant customer's client base

- the general nature of the relevant customer's client base, e.g. whether institutional or private client
- the nature of the services that the relevant customer provides to its clients
- the extent to which the relevant customer carries on business with its clients on a non-face to face basis or clients are otherwise subject to *enhanced CDD measures* and
- the extent to which clients of the relevant customer may be *PEPs* or present a higher risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*, and the *sources of funds* of such *PEPs*.

119. Immediately before applying the exemptions set out in Part 3A of the Money Laundering Order, a *supervised person* may demonstrate that it has had regard for the higher risk of *money laundering,* the *financing of terrorism,* and the *financing of proliferation* should a relevant customer fail to apply *identification measures*, keep records, or keep records for the required period where it considers the following factors:

- the stature and regulatory track record of the relevant customer
- the adequacy of the framework to combat *money laundering,* the *financing of terrorism,* and the *financing of proliferation* (including financial sanctions) in place in the country or territory in which the relevant customer is based and the period of time that the framework has been in place
- the adequacy of the supervisory regime to combat *money laundering,* the *financing of terrorism,* and the *financing of proliferation* to which the relevant customer is subject
- the adequacy of identification measures applied by the relevant customer to combat money laundering, the financing of terrorism, and the financing of proliferation
- the extent to which the relevant customer itself relies on other obliged parties to identify its clients and to hold evidence of identity, and whether such parties are *supervised* persons or carry on an equivalent business.

120. A *supervised person* may demonstrate that it has considered the adequacy of *identification measures* applied by a relevant customer where it takes one or more of the following steps:

- reviews its previous experience (if any) with the relevant customer
- makes specific enquiries, e.g. through use of a questionnaire
- reviews relevant *policies and procedures* of the relevant customer
- where the relevant customer is a member of a financial group, makes enquiries concerning the extent to which group standards are applied to and assessed by the group's internal audit function
- conducts (or commissions from an external expert) sample testing of the adequacy of the relevant customer's *policies and procedures* to combat *money laundering,* the *financing of terrorism,* and the *financing of proliferation*, whether through onsite visits, or through requesting specific *CDD* information and/or copy documentation to be provided.

7.16 Further exemptions from applying identification requirements

Statutory requirements (paraphrased wording)

121. *Article 18 of the Money Laundering Order provides further specific circumstances where exemptions from applying identification measures may be used.*

Insurance Business

122. *Under Article 18(1) of the Money Laundering Order, a relevant person is exempt from applying the identification measures specified in Article 13 in respect of insurance business if:*

a) in the case of a policy of insurance in connection with a pension scheme taken out by virtue of a person's contract of employment or occupation, the policy contains no surrender clause and may not be used as collateral security for a loan

b) a premium is payable in one instalment of an amount not exceeding £1,750 or

c) a periodic premium is payable and the total amount payable in respect of any calendar year does not exceed £750.

Pension, superannuation, employee benefit, share option or similar scheme

123. *Under Article 18(2) of the Money Laundering Order, a relevant person is exempt from applying the identification measures specified in Article 13 if:*

a) the business relationship or one-off transaction relates to a pension, superannuation, employee benefit, share option or similar scheme

b) the contributions to the scheme are made by an employer or by way of deductions from wages

c) the rules of the scheme do not permit the assignment of an interest of a member of the scheme except after the death of the member and

d) the interest of a deceased member of the scheme is not being assigned.

Regulated person and those carrying on equivalent business

124. *Under Article 18(3) of the Money Laundering Order, a relevant person is exempt from applying the identification requirements in Article 13 in respect of the measures specified in Article 3(2)(a), (aa) and (c) in relation to a customer if the customer is:*

a) a regulated person

b) a person who carries on equivalent business to any category of regulated business or

c) a person wholly owned by a person (the "parent") mentioned in sub-Paragraph (a) or (b), but only if:

i. the person is incorporated or registered in the same jurisdiction as the parent

ii. the person has no customers who are not customers of the parent, the person's activity is ancillary to the regulated business or equivalent business carried on by the parent

iii. in relation to that activity, the person maintains the same policies and procedures as the parent.

Public authority or body corporate/limited liability company with listed securities

125. *Under Article 18(4) of the Money Laundering Order, a relevant person is exempt from applying the identification requirements in Article 13 in respect of the measures specified in Article 3(2)(a) and 3(2)(aa) (in so far as those measures require identifying any person purporting to act on behalf of the customer), 3(2)(c)(ii) and 3(2)(c)(iii) in relation to a customer if the customer is:*

a) a public authority acting in that capacity

b) a body corporate or limited liability company the securities of which are listed on an IOSCO-compliant market or on a regulated market or

c) a person wholly owned by a person mentioned in sub-Paragraph (b).

Person authorised to act on behalf of customer

126. *Under Article 18(5) of the Money Laundering Order, a relevant person is exempt from applying the identification requirements in Article 13 in respect of the measures specified in Article 3(2)(aa) (in so far as those measures require identifying any person purporting to act on behalf of a customer) in relation to a person if:*

a) the person is authorised to act on behalf of the customer

b) the customer is not a relevant person

c) the person acts on behalf of the customer in the course of employment by a person carrying on a financial services business; and

d) the financial services business is a regulated business or an equivalent business to a regulated business.

Schedule 2 Business (Lawyers and Estate Agents)

127. *Under Article 18(6) of the Money Laundering Order, a relevant person is exempt from applying the identification requirements in Article 13 to the extent that the measures require identification of a person within the meaning of Article 3(4)(b) if:*

a) the relevant person's business falls within Paragraph 1 [Lawyers] or 3 [Estate Agents] of Part B of Schedule 2 to the Proceeds of Crime Law and

b) that person enters into a business relationship or carries out a one-off transaction for the purpose of enabling a customer, directly or indirectly, to enter into a registered contract (within the meaning of the Control of Housing and Work (Jersey) Law 2012.

AML/CFT/CPF Codes of Practice

128. For each case described in Article 18 of the *Money Laundering Order*, a *supervised person* must obtain information on the purpose and intended nature of the *business relationship* or *one-off transaction*.

129. A *supervised person* must obtain and retain documentation establishing that the *customer* is entitled to benefit from an exemption in Article 18 of the *Money Laundering Order*.

7.16.1 Pension, superannuation, employee benefit, share option or similar schemes

Overview

130. Where a *supervised person* enters into a *business relationship* or carries out a *one-off transaction* relating to a pension, superannuation, employee benefit, share option or similar scheme, in some limited circumstances there is no requirement to apply *identification measures*.

131. However, the exemption cannot be applied if a *supervised person* considers that there is a higher risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*.

Guidance notes

132. A *supervised person* may demonstrate that it considers whether there is a higher risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* when, among other things, it considers the reputation of the sponsoring employer and adequacy of controls in place over membership.

7.16.2 Jersey Public Authority

Overview

133. Where a *customer* is a public authority in Jersey (meaning a person holding a public office in Jersey), then, in line with Article 18(4)(a) of the *Money Laundering Order*, there is no requirement to apply *identification measures* on that *customer*, on the *beneficial owners and controllers* of the *customer*, or those purporting to act on behalf of the *customer*.

134. However, in the above scenario the obligation to apply *identification measures* to any third party for which the *customer* may be acting and to verify the authority of persons acting on behalf of the *customer* remain in force.

135. The following may be considered to be public authorities in Jersey:

› a government department of the States of Jersey

› a majority States-owned company

› an agency established by a law of the States of Jersey

› a parish authority.

7.16.3 Body Corporate/limited liability company with Listed Securities

Overview

136. Where a *customer* is a body corporate or limited liability company, the securities of which are listed on a market that conforms to international standards set by *IOSCO* or on a *regulated market*, then in line with Article 18(4)(b) of the *Money Laundering Order*, there is no requirement to apply *identification measures* on that *customer* (or any wholly owned subsidiary), on the *beneficial owners and controllers* of the *customer* (or any wholly owned subsidiary), or those purporting to act on behalf of the *customer* (or any wholly owned subsidiary).

137. However, in the above scenario the obligation to apply *identification measures* to any third party for which the *customer* (or wholly owned subsidiary) may be acting and to verify the authority of persons acting on behalf of the *customer* (or wholly owned subsidiary) remain in force.

138. A market may be considered to be *IOSCO*-compliant if it is operated in a country or territory that has been assessed as having "fully implemented" or "broadly implemented" *IOSCO* Principles 16 and 17. In order to be assessed as having "fully implemented" or "broadly implemented" Principle 17, a country or territory must require:

- information about the identity and holdings of persons who hold a substantial *beneficial ownership* interest to be disclosed on a timely basis
- material changes in such ownership and other required information to be disclosed in a timely manner.

139. Whilst there is not a global list of countries and territories that "fully implement" or "broadly implement" *IOSCO* Principles 16 and 17, reference may be made to *IMF* Financial System Stability Assessment reports, prepared as part of the *IMF* Financial Sector Assessment Program.

140. Guidance published by the UK's Joint Money Laundering Steering Group addresses what may be considered to be a *regulated market*. The only list of exchanges currently available is for *EU*-regulated markets (follow the link provided in the glossary entry for *regulated market*).

7.16.4 Regulated persons and those carrying on equivalent business

Overview

141. Where a *customer* is:

- a *regulated person* (defined in Article 1(1) of the Money Laundering Order)
- a person who carries on *equivalent business* to any category of *regulated business* or
- wholly owned by a person listed above and which fulfils certain conditions (see Article 18(3)(c) of the Money Laundering Order)

Then in line with Article 18(3) of the Money Laundering Order, there is no requirement to apply identification measures in respect of the *customer*, the *beneficial owners and controllers* of the *customer*, or those purporting to act on behalf of the *customer*. Nor is there a requirement to verify the authority of any person purporting to act for the *customer*.

142. However, these provisions do not also provide an exemption in respect of any third party (or parties) for whom the *customer* is acting, or for the *beneficial owners and controllers* of such a third party (or parties).

7.16.5 Person authorised to act on behalf of a customer

Guidance notes

143. Where a person authorised to act on behalf of a *customer* holds their role by virtue of their employment by (or position in) a business that is a *regulated person* or an equivalent *regulated business*, a *supervised person* may demonstrate that this exemption applies where it obtains:

- the full name of the individual and
- an assurance from the employer that the individual is an officer or employee.

7.17 Simplified Identification Measures – Obtaining evidence of identity for very low risk products/services

Overview

144. Where funds involved in a *business relationship*:

› have been received from a bank that is a *regulated person* or carries on *equivalent business* to deposit-taking (see Section 1.8 regarding *equivalent business*) and

› have come from an account in the sole or joint name of the *customer* who is an individual (or are individuals)

Then the receipt of funds from such an account may be considered to be reasonably capable of verifying that the person to be identified is who they are said to be where the product or service requested by the *customer* is considered to present a very low risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*. This will be the case where funds may only be received from, and paid to, an account in the *customer's* name, i.e. a product or service where funds may not be paid in by, or paid out to, external parties.

145. In the event that any of the conditions set below are breached, evidence of identity for the customer must be obtained at that time in accordance with Section 4 and Section 7 of this Handbook.

AML/CFT/CPF Codes of Practice

146. The concession referred to above must not be applied in the following circumstances:

› where a supervised person suspects money laundering, the financing of terrorism, or the financing of proliferation;

› in any situation which by its nature can present a higher risk of *money laundering*, the *financing of terrorism*, or the *financing of proliferation*;

› where the customer has a relevant connection to an enhanced risk state; or

› where the customer is resident in a country or territory that is not compliant with the FATF Recommendations.

147. To benefit from the concession, the product or service must satisfy the following conditions:

› all initial and future payments must be received from an account at a bank that is a *regulated person* or carries on an *equivalent business* to deposit-taking (see Section 1.8), where the account can be confirmed as belonging to the *customer;*

› no initial or future payments may be received from external parties;

› cash withdrawals are not permitted, with the exception of face-to-face withdrawals by the *customer*, where they are required to produce evidence of identity before the withdrawal can be made;

› no payments may be made, other than to an account at a bank that is a *regulated person* or carries on an *equivalent business* to deposit-taking (see Section 1.8), where the account can be confirmed as belonging to the *customer*, or on the death of the *customer* to a personal representative named in the grant of probate or the letters of administration; and

› no future changes must be made to the product or service that enable funds to be received from or paid to external parties.

148. A *supervised* person must obtain and retain evidence confirming that payment has been received from an account at a bank that is a regulated person or carries on an equivalent business to deposit-taking (see Section 1.8), and, where a request for a withdrawal or transfer to another bank account is received, confirmation that this account is also in the customer's name and held at a bank that is a regulated person or carries on an equivalent business to deposit-taking.

149. If a *supervised person* has reason to suspect that the motive behind a particular transaction, or the way a business is being structured, is to avoid standard identification measures, it must not use this concession.

8 REPORTING MONEY LAUNDERING AND THE FINANCING OF TERRORISM, AND SANCTIONS REPORTING OBLIGATIONS

8.1 Overview of section

1. Under the *Proceeds of Crime Law* and *Terrorism Law*, where any *supervised* person conducting *supervised business* in or from within Jersey knows or suspects, or has reasonable grounds for suspecting that another person is engaged in *money laundering* or the *financing of terrorism*, then it must report its knowledge or suspicion to the *JFCU*.

2. Under the *Money Laundering Order*, a *supervised person* must have procedures in place for reporting knowledge or suspicion of *money laundering* or the *financing of terrorism* activity to the *JFCU*.

3. This section outlines the statutory provisions concerning reporting that apply to:

› an employee of a *supervised person* and

› a *supervised person*, in the course of carrying on any trade, profession or business.

It also sets *AML/CFT/CPF Codes of Practice* for and provides guidance to:

› employees making a report to their *MLRO* (or *deputy MLRO*) (referred to as an internal *SAR*) and

› *MLROs* (and *deputy MLROs*) making a report to the *JFCU* (referred to as an external *SAR*).

4. This section also considers the consent that must be sought from the *JFCU* before proceeding with a transaction or continuing a *business relationship*, and the application of tipping off provisions.

5. An important precondition for making a *SAR* is to know enough about a *business relationship* or *one-off transaction* to be able to recognise what is "unusual". Such knowledge is dependent upon the application of *identification measures* and on-going monitoring.

6. A *SAR* may also be based on information from other sources, including law enforcement agencies, other government bodies, the media, or the *customer*.

7. Whilst this section describes reports made to the *JFCU* under the Proceeds of Crime Law and Terrorism Law as *SARs*, depending on the circumstances such reports may involve **knowledge** of *money laundering* or the *financing of terrorism*, rather than **suspicion** (or reasonable grounds for knowledge or suspicion).

8. Section 8.8 of this Handbook explains the separate sanctions compliance reporting obligations under the *Sanctions and Asset-Freezing Law* .

8.2 Reporting knowledge or suspicion

Overview

9. Legislation deals with reporting by a *supervised person* and employees in the course of carrying on a *supervised business* in two ways:

› there is a **reporting requirement** under Article 34D of the *Proceeds of Crime Law* and Article 21 of the *Terrorism Law* - when a *SAR* must be made when there is knowledge, suspicion, or reasonable grounds for suspecting that:

- another person is engaged in *money laundering* or the *financing of terrorism*; or
- any property constitutes or represents proceeds of criminal conduct; or
- any property has been, is being or is intended to be used in criminal conduct; or
- any property is or may be terrorist property.

› there is **protection for reporting** under Article 32 of the *Proceeds of Crime Law* and under Article 18 of the *Terrorism Law* when there is suspicion or belief that any property constitutes or represents:

- the proceeds of criminal conduct; or
- property used in or intended to be used in criminal conduct; or
- terrorist property.

› Where the person making the report does any act or deals with the property in any way which would otherwise amount to the commission of a *money laundering* or the *financing of terrorism* offence, the person shall not be guilty of that offence (where certain conditions are fulfilled) where it makes a **protective report**.

10. In practice, a report made in accordance with the **reporting requirement** will also provide **protection**. For example, where a *supervised person* knows or suspects, or has reasonable grounds for suspecting that property constitutes or represents the proceeds of criminal conduct (or has been, is being or is intended to be used in criminal conduct), and has possession of that property, it must report its knowledge or suspicion under Article 34D of the *Proceeds of Crime Law*. Where it makes such a report, this will also address its suspicion or belief that property constitutes or represents the proceeds of criminal conduct (or has been used in or is intended to be used in criminal conduct) under Article 32 of the *Proceeds of Crime Law*. The effect of this is that the supervised person does not commit a *money laundering* offence under Article 30 (and potentially Article 31) of that law.
11. Within the *Proceeds of Crime Law* there is also a **reporting requirement** (Article 34A) and **protection for reporting** (Article 32) in a case where a matter or information comes to a *supervised person's* attention other than in the course of carrying on a *supervised business* (i.e. through any trade, profession, business or employment). A similar **reporting requirement** (and **protection**) may also be found in Articles 19 and 18 of the *Terrorism Law*.
12. Whilst the *Proceeds of Crime Law* and *Terrorism Law* anticipate that a report may be made by an employee directly to the *JFCU*, Article 21 of the *Money Laundering Order* requires that such reporting is made in line with a *supervised person's* **reporting procedures**. Such procedures must ensure that a report by an employee is made to the *MLRO* (or *deputy MLRO*).
13. Where the *MLRO* (or *deputy MLRO*) resolves to make an external *SAR* as a result of an internal *SAR* made under the *Proceeds of Crime Law* or *Terrorism Law*, Article 21 of the *Money Laundering Order* requires that *SAR* to be made using the approved form. In this section "approved form" means the form approved by the Minister, which may be changed from time to time.

14. A *SAR* made in respect of a *business relationship* or *one-off transaction* does not remove the need to make **further reports** in respect of knowledge or suspicion that subsequently arises in respect of that *business relationship* or *one-off transaction* (which may also be a series of linked transactions).

8.2.1 Requirement to report knowledge or suspicion

Overview

15. While carrying on a *supervised business*, employees of a *supervised person* are required to raise an internal *SAR* **as soon as practicable** where they have knowledge or suspicion, or where there are reasonable grounds for having knowledge or suspicion that:

› another person is engaged in money laundering or the *or financing of proliferation* or

› any property constitutes or represents the proceeds of criminal conduct or

› any property has been, is being, or is intended to be used in criminal conduct or

› any property is, or may be, terrorist property.

16. What may constitute reasonable grounds for knowledge or suspicion will be determined by the facts or circumstances present, from which an honest and reasonable employee working in a *supervised person* would have inferred knowledge or formed a suspicion (the so-called "objective test"). See Section 8.2.3.3

17. Something which appears unusual is not necessarily suspicious, but will likely be the cause for further investigation. This may, in turn, require judgement to be exercised as to whether something is indeed suspicious.

18. A *supervised person's MLRO* (or *deputy MLRO*) must consider all internal *SARs* **as soon as practicable**.

19. A *supervised person's MLRO* (or *deputy MLRO*) is required to make an external *SAR* **as soon as practicable** if they know, suspect or have reasonable grounds for suspecting that:

› another person is engaged in money laundering or the financing of terrorism; or

› any property constitutes or represents the proceeds of criminal conduct; or

› any property has been, is being, or is intended to be used in criminal conduct; or

› any property is, or may be, terrorist property.

20. Guidance on how a *supervised person* may demonstrate that internal and external *SARs* are being made as soon as reasonably practicable is set out at Sections 8.3.1 and 8.3.2 respectively.

21. Once an employee has made an internal *SAR*, and provided any additional information that may be requested by the *MLRO* (or *deputy MLRO*), they will have fully satisfied their statutory obligation in respect of the particular matter or information reported.

22. Under the Proceeds of Crime Law, the **requirement to report** applies in relation to the proceeds of such criminal conduct that constitutes an offence specified in Schedule 1 of the *Proceeds of Crime Law*, or, if it occurs or has occurred outside Jersey, would have constituted such an offence if it occurred in Jersey.

23. Under the Terrorism Law, the **requirement to report** applies in relation to property which is intended or likely to be used for the purposes of terrorism in Jersey or elsewhere, or for the support of a terrorist entity in Jersey or elsewhere.

24. Other than in the course of carrying on a *supervised business* (i.e. any other trade, profession or business carried on by the *supervised person*), employees of a *supervised person* are also required to raise an internal *SAR* where they have knowledge or suspicion that another person is engaged in *money laundering* or the *financing of terrorism* - where information or a matter on which knowledge or suspicion is based comes to them **in the course of their employment**. This will apply irrespective of the underlying nature of the business that is carried on, and irrespective of whether or not the business is being carried out on behalf of another person, e.g. under an outsourcing arrangement.

25. Where an *MLRO* who is part of a group receives information relating to suspicious activities within that group but with no specific Jersey connection, such information is not considered to have come to the *MLRO* in the course of carrying on a *supervised business*. This means that such matters, in the absence of a specific Jersey connection, are not required to be reported.

Statutory requirements (paraphrased wording)

26. *Under Article 34D(4) of the Proceeds of Crime Law, a relevant person and employees of that relevant person are required to make a report where two conditions are fulfilled.*

27. *The first is that they know, suspect or have reasonable grounds for suspecting that:*

- *another person is engaged in money laundering or the financing of terrorism;*
- *any property constitutes or represents the proceeds of criminal conduct; or*
- *any property has been, is being or is intended to be used in criminal conduct.*

28. *The second is that the information or matter on which the knowledge or suspicion is based, or which gives reasonable grounds for suspicion, comes to them **in the course of the carrying on of a financial services business**.*

29. *Such a report must be made to a designated police officer or designated customs officer (or, in the case of an employee, to the relevant person's MLRO (or deputy MLRO)), delivered in good faith, and made as soon as is practicable after the information or other matter on which the knowledge or suspicion is based, or which gives reasonable grounds for suspicion, comes to their attention.*

30. *However, under Article 34D(5) of the Proceeds of Crime Law, a person does not commit an offence if they have a reasonable excuse for not disclosing the information or other matter, or the person is a professional legal adviser and the information or other matter comes to them in the circumstances of legal privilege (except items held with the intention of furthering a criminal purpose).*

31. *Under Article 34D(6) of the Proceeds of Crime Law, an employee of a relevant person does not commit an offence of failing to disclose if they have not been given material training and, as a result, did not know or suspect that the other person was engaged in money laundering or the financing of terrorism.*

32. *Under Article 34D(9) of the Proceeds of Crime Law, a report made to a designated police officer or designated customs officer (or to the relevant person's MLRO or deputy MLRO) shall not be treated as a breach of any restriction imposed by statute, contract or otherwise.*

33. *When considering a report made under the Proceeds of Crime Law or Terrorism Law, Article 21(2) and (3) of the Money Laundering Order states that, if the MLRO (or deputy MLRO) knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering or the financing of terrorism, they must report to a designated police officer or designated customs officer as soon as is practicable using the approved form. Among other things, delivery of the approved form must comply with the requirements (including those in respect of delivery) indicated on the approved form.*

34. *Following the submission of a report, Article 21(4) of the Money Laundering Order requires a MLRO (or deputy MLRO) to provide a designated police officer or designated customs officer (within a set period of time) with such additional information relating to that report as may reasonably be requested.*

35. *A person who fails to make a report under Article 34D of the Proceeds of Crime Law is liable to imprisonment for a term not exceeding 5 years or to a fine or to both. An individual who fails to make a report using the approved form under Article 21(2) of the Money Laundering Order is liable to imprisonment for a term not exceeding 2 years or to a fine or to both. A body corporate who fails to make a report using the approved form under Article 21(2) of the Money Laundering Order is liable to a fine.*

36. *Article 34A of the Proceeds of Crime Law contains a similar requirement to report. In a case where a relevant person or employee knows or suspects that another person is engaged in money laundering or the financing of terrorism and the information or other matter on which that knowledge or suspicion is based comes to their attention in the course of* ***any trade, profession, business or employment*** *(other than carrying on of a financial services business), they must report that knowledge or suspicion and information or other matter to a police officer (or, in the case of an employee, to the relevant person's MLRO (or deputy MLRO)), in good faith and as soon as is practicable after the information or other matter comes to their attention.*

37. *Under Article 34A(3) of the Proceeds of Crime Law, a report made to a designated police officer or designated customs officer (or to the relevant person's MLRO or deputy MLRO) under Article 34A shall not be treated as a breach of any restriction imposed by statute, contract or otherwise.*

38. *Article 8 of the Money Laundering Order requires a relevant person to ensure that the MLRO (or deputy MLRO) has timely access to all records that are necessary or expedient for the purpose of performing his or her functions as a reporting officer, including, in particular, the records that a relevant person must keep under Article 19.*

39. *"Criminal conduct" is defined in Article 1(1) of the Proceeds of Crime Law as conduct that constitutes an offence specified in Schedule 1 of that law, or, if it occurs or has occurred outside Jersey, would have constituted such an offence if occurring in Jersey.*

40. *Articles 19 to 22 of the Terrorism Law contain similar reporting requirements in respect of the financing of terrorism.*

41. *In particular, Article 21 of the Terrorism Law requires a relevant person and employee of that relevant person to make a report where two conditions are fulfilled.*

42. *The first is that they know, suspect or have reasonable grounds for suspecting that:*

- *another person is engaged in the financing of terrorism or*
- *any property is, or may be, terrorist property.*

43. *The second is that the information or matter on which the knowledge or suspicion is based, or which gives reasonable grounds for suspicion, comes to them in the course of the carrying on of a financial services business.*

44. *Terrorist property is defined in Article 3 of the Terrorism Law to mean property which is intended to be used, or likely to be used, for the purposes of terrorism or support of a terrorist entity. A terrorist entity is defined in Article 4 as an entity which commits, prepares or instigates an act of terrorism or facilitates the commission, preparation or instigation of an act of terrorism.*

45. *The meaning of "terrorism" is defined in Article 2 of the Terrorism Law. The meaning of "terrorist entity" is defined in Article 4.*

8.2.2 Protective report

Overview

46. In the course of carrying on its business, employees of a *supervised person* will raise an internal *SAR* in order to be protected where they suspect or believe that:

› property constitutes or represents the proceeds of criminal conduct or property used in or intended to be used in criminal conduct; or

› property is terrorist property; or

› they are providing a service for the purposes of terrorism or for the support of a terrorist entity.

47. This will apply irrespective of the underlying nature of the business that is carried on, and irrespective of whether or not the business is being carried out on behalf of another person, e.g. under an outsourcing arrangement.

48. A *supervised person's MLRO* (or *deputy MLRO*) must consider all internal *SARs* **as soon as practicable**.

49. Under the *Proceeds of Crime Law* and *Terrorism Law*, a *supervised person's MLRO* (or *deputy MLRO*) is required to make an external *SAR* **before** the *supervised person* does a particular act, or **as soon as reasonably practicable** after the person has done the act or has become involved in the transaction or arrangement, in order to be protected.

50. In most cases, where the person making the report does any act or deals with the property in any way which would otherwise amount to the commission of a *money laundering* or the *financing of terrorism* offence, the person shall not be guilty of that offence where it makes such a protective report and certain conditions are fulfilled.

51. Under the *Proceeds of Crime Law*, protection for reporting applies in relation to the proceeds of such criminal conduct that constitutes an offence specified in Schedule 1 of the *Proceeds of Crime Law*, or if it occurs or has occurred outside Jersey, would have constituted such an offence if occurring in Jersey.

52. Under the *Terrorism Law*, protection for reporting applies in relation to property which is intended or likely to be used for the purposes of terrorism in Jersey or elsewhere or for the support of a terrorist entity in Jersey or elsewhere.

Statutory requirements (paraphrased wording)

53. *Where a relevant person or employee of a relevant person suspects or believes that any property constitutes or represents the proceeds of criminal conduct or property used in or intended to be used in criminal conduct and makes a report to a police officer (or to the relevant person's MLRO or deputy MLRO) under Article 32 of the Proceeds of Crime Law, they will not have committed a money laundering offence if the report is made in good faith and either:*

    - *if the report is made before the person does the act in question, the act is done with the consent of a police officer or*
    - *if the report is made after the person does the act in question, it is made on the person's own initiative and as soon as reasonably practicable after the person has done the act in question.*

54. *In proceedings against a person for an offence under Article 30 of the Proceeds of Crime Law, it shall be a defence under Article 32(7) to provide that the alleged offender intended to make a report and there is a reasonable excuse for the failure to have made a report.*

55. *Under Article 32(2) of the Proceeds of Crime Law, a report made to a police officer (or to the relevant person's MLRO or deputy MLRO) under Article 32 shall not be treated as a breach of any restriction imposed by statute, contract or otherwise, and shall not involve the person making it in liability of any kind.*

56. *When considering a report made under the Proceeds of Crime Law or Terrorism Law, Article 21(2) and (3) of the Money Laundering Order states that, if the MLRO (or deputy MLRO) knows or suspects that another person is engaged in money laundering or the financing of terrorism, they must report to a designated police officer or designated customs officer as soon as is practicable using the approved form. Among other things, delivery of the form must comply with the requirements (including those in respect of delivery) indicated on the form.*

57. *Subsequent to making a report, Article 21(4) of the Money Laundering Order requires a MLRO (or deputy MLRO) to provide a designated police officer or designated customs officer (within a set period of time) with such additional information relating to that report as may reasonably be requested.*

58. *An individual who fails to make a report using the approved form under Article 21(2) of the Money Laundering Order is liable to imprisonment for a term not exceeding 2 years or to a fine or to both. A body corporate who fails to make a report using the approved form under Article 21(2) of the Money Laundering Order is liable to a fine.*

59. *Article 8 of the Money Laundering Order requires a relevant person to ensure that the MLRO (or deputy MLRO) has timely access to all records that are necessary or expedient for the purpose of performing their functions as a reporting officer, including, in particular, the records that a relevant person must keep under Article 19.*

60. *"Criminal conduct" is defined in Article 1(1) of the Proceeds of Crime Law as conduct that constitutes an offence specified in Schedule 1, or, if it occurs or has occurred outside Jersey, would have constituted such an offence if occurring in Jersey.*

61. *Article 18 of the Terrorism Law contains similar provisions in circumstances where the financing of terrorism offences would otherwise be committed. In particular:*

    - *article 18(1) provides that no financing of terrorism offence is committed if a person is acting with the express consent of a police officer or customs officer*

- *article 18(2) provides that no financing of terrorism offence is committed if a person discloses a suspicion or belief that property is terrorist property after they have become involved in a transaction or arrangement to a police officer or customs officer in good faith and as soon as reasonably practicable*
- *article 18(3) provides that no financing of terrorism offence is committed if a person discloses a suspicion or belief to a police officer or customs officer that a service is being, or is to be, provided for the purposes of terrorism or for the support of a terrorist entity, after they have become involved in a transaction or arrangement, in good faith and as soon as reasonably practicable.*

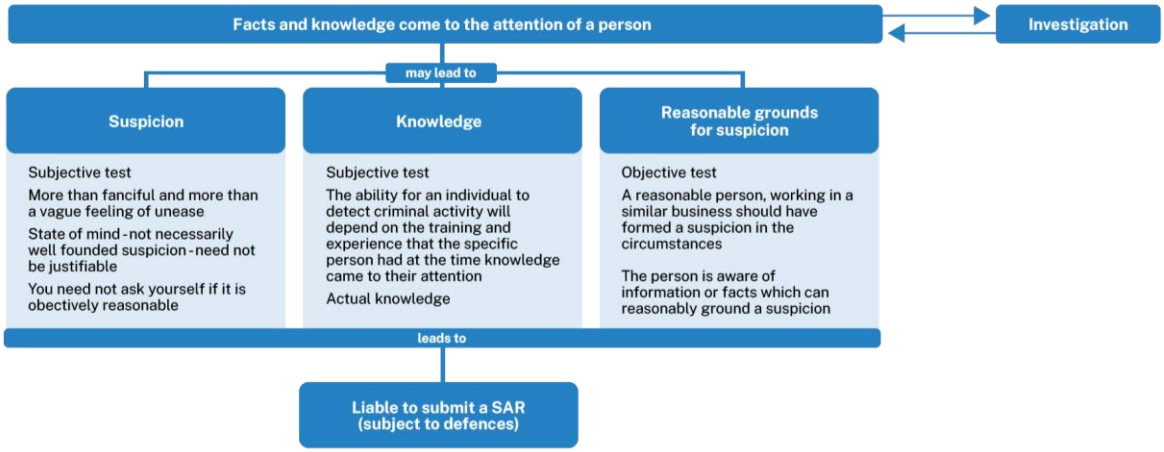
62. *However, unlike the Proceeds of Crime Law, an employee who makes a report to the relevant person's MLRO or deputy MLRO may still be charged with an offence. In such a case, it will be a defence under Article 18(8) for the employee to prove that a report was made in good faith and in accordance with the employer's procedures.*

8.2.3 What constitutes knowledge or suspicion?

Guidance notes

63. The terms 'knowledge', 'suspicion' and 'reasonable grounds for suspicion' are not defined within Jersey law. However, case law has provided some guidance on how they should be interpreted.

64. The diagram below summarises the differences between each of these three terms and where they sit within the wider reporting process:



8.2.3.1 Knowledge

65. Knowledge means actual knowledge. There is some suggestion that wilfully shutting one's eyes to the truth may amount to knowledge. However, the current general approach from the criminal courts is that nothing less than actual knowledge will suffice.

8.2.3.2 Suspicion

66. By contrast, suspicion is more than speculation, but it falls short of proof or knowledge. There is no requirement for the suspicion to be clear or firmly grounded on specific facts, but there must be a degree of satisfaction, not necessarily amounting to belief, but at least extending beyond speculation.

67. The test for whether a person holds a suspicion is subjective. The suspicion is one of believing that something is possible, which is more than fanciful. The suspicion must also be more than a vague feeling of unease. If someone thinks a transaction is suspicious, they are not expected to know the exact nature of the criminal offence or that particular funds were definitely those arising from the crime. They may have noticed something unusual or unexpected and, after making enquiries, the facts do not seem normal or make commercial sense. There does not have to be evidence that *money laundering or terrorist financing* is taking place for there to be a suspicion.

68. If someone has not yet formed a suspicion, but they have cause for concern, a *supervised person* may choose to ask the *customer* or other parties more questions. This decision will depend on what is already known, and how easy it is to make enquiries. If a *supervised person* does ask questions or make inquires to the *customer*, they should bear in mind the tipping-off provisions that they are subject to.

69. If there is a belief that a *customer* is innocent, but there are suspicions that another party to the business relationship or one-off transaction is engaged in *money laundering* or the *financing of terrorism*, a *supervised person* may need to consider referring the customer for specialist advice regarding the risk that they may be a party to a criminal offence.

70. Section 6.4 and the sector-specific sections of this Handbook provide a number of standard warning signs which may suggest an increased risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* and therefore give cause for concern. However, whether someone has a suspicion is a matter of their own judgement.

8.2.3.3 Reasonable grounds to suspect: the objective test of knowledge or suspicion

71. Articles 30 and 31, when read with Article 29 of the *Proceeds of Crime Law* and Articles 15 and 16 of the *Terrorism Law* provide for an offence to be committed when dealing with, using, concealing etc criminal or terrorist property where there are reasonable grounds to know or suspect that property represents the proceeds of criminal conduct or instrumentalities, or terrorist property.

72. This means that a person would commit an offence even if they did not know or suspect that a *money laundering* offence was being committed, and is determined by whether a reasonable person would suspect that criminality had occurred. In other words:

› were there factual circumstances from which a reasonable person, engaged in a similar business, should have inferred knowledge or formed the suspicion that another was engaged in *money laundering* or the *financing of terrorism;* or

› was there knowledge of circumstances which would put a reasonable person on enquiry?

8.3 Procedures for Reporting

73. Reporting procedures provide the interface between *CDD* measures carried out by a *supervised person* and the work of the *JFCU's* intelligence wing. Like all *policies and procedures*, they should be:

› drafted in a way that can be easily understood by employees

› tailored to the *supervised person's* business risk assessment and

› applied in every case where functions are outsourced (in line with Section 2.4.4 of this Handbook).

Statutory requirements (paraphrased wording)

74. *Article 21 of the Money Laundering Order requires that a relevant person must establish and maintain reporting procedures which:*

- *communicate to employees the identity of the MLRO (and any deputy MLROs) to whom an internal SAR is to be made*
- *provide for that report to be considered by the MLRO (or deputy MLRO) in the light of all other relevant information for the purpose of determining whether or not the information or other matter contained in the report gives rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering or the financing of terrorism*
- *allow the MLRO (or deputy MLRO) to have access to all other information which may be of assistance in considering the report*
- *provide for the information or other matter contained in an internal SAR to be disclosed as soon as is practicable by the MLRO (or deputy MLRO) to a designated police officer or designated customs officer using the approved form, where the MLRO (or deputy MLRO) knows, suspects or has reasonable grounds to know or suspect that another person is engaged in money laundering or the financing of terrorism and*
- *provide for additional information relating to a report to be given by the MLRO (or deputy MLRO) to a designated police officer or designated customs officer.*

75. *Article 22 of the Money Laundering Order states that if a deputy MLRO, on considering an internal SAR, concludes that it does not give rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering or the financing of terrorism, the deputy MLRO* ***need not forward it*** *to the MLRO. If a deputy MLRO, on considering an internal SAR, has concluded that it does give rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering or the financing of terrorism, although the SAR must still be forwarded to the MLRO, the MLRO* ***need not consider*** *that question. The effect of this is to require a report to be* ***considered*** *by the MLRO only in a case where the deputy MLRO* ***is not able to come to a conclusion****.*

8.3.1 Internal *SARs*

AML/CFT/CPF Codes of Practice

76. In addition to reporting procedures that must be maintained under Article 21 of the Money Laundering Order, a *supervised person* must maintain procedures that:

- highlight that reporting requirements extend to potential *business relationships* and *one-off transactions* that are declined (i.e. where no *business relationship* is established or *one-off transaction* carried out)
- highlight that internal *SARs* are to be made regardless of the amount involved in a transaction or relationship and regardless of whether it is thought to involve tax matters
- highlight the importance of making an internal *SAR* **as soon as practicable**
- require internal *SARs* to be made in a set format and to include as full a statement as possible of:

- the information or matter giving rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion
- the date that the information or matter came to the employee's attention and
- full details of the *customer*, transaction or activity that the *supervised person* holds on its records.
- require internal *SARs* to be acknowledged by the *MLRO* (or *deputy MLRO*) **as soon as practicable**
- require the *MLRO* (or *deputy MLRO*) to record all internal *SARs* in a register which includes the following:
- date of the internal *SAR*
- identity of the individual making the internal *SAR* and
- information to allow supporting documentation to be retrieved in a timely manner.

77. A *supervised person* must not allow internal *SARs* to be filtered by line management such that they do not reach the *MLRO* (or *deputy MLRO*). Where procedures allow employees to discuss relationships and transactions with line managers before an internal *SAR* is made, those procedures must emphasise that the decision on reporting remains with the employee and not the line manager.
78. A *supervised person* must establish and maintain arrangements for disciplining any employee who fails, without reasonable excuse, to make an internal *SAR* where they have knowledge, suspicion or reasonable grounds for knowledge or suspicion, or does not do so **as soon as practicable**.

Guidance notes

79. A *supervised person* may demonstrate that it has established and maintained arrangements for disciplining employees by ensuring that employment contracts and employment handbooks provide for the imposition of disciplinary sanctions for failing to report knowledge, suspicion or reasonable grounds for knowledge or suspicion without reasonable excuse, or failing to report as soon as practicable.
80. A *supervised person* may demonstrate that employees make internal *SARs* as soon as practicable where the *MLRO* (or *deputy MLRO*) periodically considers (by business area if appropriate):

- the amount of time taken between information or a matter coming to an employee's attention and the date of the internal *SAR* and concludes that it is reasonable
- the number and content of internal *SARs* and concludes that both are consistent with the *supervised person's* business risk assessment.

8.3.2 External *SARs*

Overview

81. The *MLRO* (or *deputy MLRO*) must consider each internal *SAR*. In order to do so, the Money Laundering Order requires that the *MLRO* (or *deputy MLRO*) has access to all necessary records. The *MLRO* (or *deputy MLRO*) may also require further information to be obtained from the *customer*. Any such approach will need to be made sensitively and probably by someone other than the *MLRO* (or *deputy MLRO*) to minimise the risk of alerting the *customer* that a report to the *JFCU* may be under consideration (though this may not yet be tipping off).

82. When considering an internal *SAR* the *MLRO* (or *deputy MLRO*), taking a risk-based approach, will need to strike an appropriate balance between the requirement to make a report to the *JFCU* as soon as practicable, especially if consent is required, and any delay that might arise from searching a number of potentially unlinked systems and records that might hold relevant information.

AML/CFT/CPF Codes of Practice

83. In addition to reporting procedures that must be maintained under Article 21 of the *Money Laundering Order*, a *supervised person* must maintain procedures that:

› require the *MLRO* (or *deputy MLRO*) to document all enquiries made in relation to each internal *SAR*

› require the *MLRO* (or *deputy MLRO*) to document the basis for reporting to the *JFCU* or deciding to not make such a report. This must be retained with the internal *SAR*

› require the *MLRO* (or *deputy MLRO*) to record all external *SARs* in a register which includes the following:

  - date of the report, and
  - information to allow supporting documentation to be retrieved in a timely manner.

› require the *MLRO* (or *deputy MLRO*) to inform the *JFCU* where relevant information is subsequently discovered.

Guidance notes

84. A *supervised person* may demonstrate that an internal *SAR* is considered in light of all other *supervised* information when the following are taken into account:

› the business and risk profile for the subject of the report

› the complexity and duration of the *business relationship*

› transaction patterns and volumes, and previous patterns of instructions

› any connected accounts or relationships. Connections can be commercial e.g. linked transactions or common referrals, or through individuals e.g. third parties, *beneficial owners and controllers* or account signatories and

› the risk that assets will dissipate.

85. A *supervised person* may demonstrate that the *MLRO* (or *deputy MLRO*) reports as soon as practicable where the Board considers:

› the typical amount of time taken by the *MLRO* (or *deputy MLRO*) to process an internal *SAR* (being the time taken from the date of the internal *SAR* and the date of the external SAR/decision to not report) and

› the number of internal *SARs* not processed within a period of time set by the Board/*senior management*, together with an explanation.

Refer to Section 2.1 for an explanation of the meaning of "the Board" in the context of this paragraph.

8.4 JFCU Consent

Overview

86. Protective reports **before** or **after** doing an act are not equal options which a *supervised person* can choose between.

› a report should be made **before doing an act** where a *customer* instruction is received prior to an activity or transaction taking place, or arrangements being put in place. However, when a transaction which gives rise to concern is already within an automated clearing or settlement system where a delay would lead to a breach of a contractual obligation or where it would breach market settlement or clearing rules, the *MLRO* (or *deputy MLRO*) may need to let the transaction proceed and report it later.

› a report should be made **after doing an act** where something appears suspicious only with the benefit of hindsight or following the receipt of additional information.

87. Under Article 32(4) of the *Proceeds of Crime Law,* if a *SAR* was made **before doing an act,** a *supervised person's MLRO* (or *deputy MLRO)* should request consent from the *JFCU* for a specific transaction (for example, a distribution). Such consent requests should be sent to the *JFCU* via the *SAR* portal (POLSAR), either as part of an initial *SAR* submission, or as part of a Continuation Report. Where no specific consent for an act is being sought under Article 32(4) of the *Proceeds of Crime Law*, the *JFCU* will usually only issue an acknowledgement in response to a *SAR*. Further guidance on the consent regime is provided on the *JFCU's* website and may be updated from time to time.

88. While waiting for the *JFCU* to provide consent to proceed with a transaction or activity, or in the event that the *JFCU* notifies a *supervised person* that consent will not be given, a *supervised person* should be aware of the risk of committing a tipping off offence where it fails to act on a *customer* instruction. In any written communication with that customer regarding the instruction, it should consider using generalised wording to explain the situation.

89. In a situation where consent is not given, a *supervised person* should contact the *JFCU* for guidance on what information can be provided to the *customer* (though the *JFCU* is not obligated to provide such guidance).

90. Where a *supervised person* does not wish to, or decides not to act upon a *customer's* instruction, this may lead to civil proceedings being instituted by the *customer* for breach of contract. In these circumstances it may be necessary for the *supervised person* to seek legal advice or direction from the law courts.

91. A *supervised person* may reduce the risk of civil proceedings by ensuring that *customers'* terms of business specifically:

› allow an instruction to be delayed or deferred pending investigation

› exclude breaches in circumstances where following a *customer* instruction may lead to the *supervised person* committing an offence.

8.5 Tipping off

Overview

92. In this section, reference to a "disclosure" is to the disclosure of matters **related** to a *SAR* or an investigation (and not the disclosure of suspicion or knowledge **through** a *SAR*).

93. Except as otherwise provided, where a person knows or suspects that an internal or external *SAR* has been or will be made, a person will commit a tipping off offence where they disclose to another person:

› the fact that they have made, or will make, an internal or external *SAR* or

› any information relating to such a *SAR*.

94. Except as otherwise provided, where a person knows or suspects that the Attorney General or any police officer is acting or proposing to act in connection with a criminal investigation into *money laundering* or the *financing of terrorism* that is being or is about to be conducted, a person will commit a tipping off offence where they:

› disclose to another person any information relating to the investigation or

› interfere with material which is likely to be relevant to such an investigation.

95. Among other things, the effect of this is that a *supervised person* or employee of a *supervised person*:

› cannot, **at the time**, tell a *customer* that a transaction or activity **is being delayed** because an internal *SAR* is about to be made or has been made to the *MLRO* (or *deputy MLRO*)

› cannot, **at the time**, tell a *customer* that a transaction or activity **is being delayed** because an external *SAR* is about to be made or awaiting consent from the *JFCU*

› cannot **later** tell a *customer* that a transaction or activity **was delayed** because an internal or external *SAR* had been made

› cannot tell the customer that law enforcement is conducting an investigation.

96. However, a tipping off offence is not committed when a *supervised person* discloses that an internal *SAR* has been made; that it will make or has made an external *SAR*; information relating to such *SARs*; or information relating to a criminal investigation, where the above information is disclosed to its:

› lawyer – in order to obtain legal advice or for the purpose of legal proceedings or

› accountant – for the purpose of enabling the accountant to provide certain services, e.g. in order to provide information that will be relevant to the statutory audit of a *supervised person's* financial statements

Except, where the disclosure is made with a view to furthering a criminal purpose.

97. Nor is a tipping off offence committed when a **lawyer** discusses that disclosure with its *customer*, where this is in connection with the provision of legal advice or for the purpose of actual or contemplated legal proceedings (except where the discussion is with a view to furthering a criminal purpose). **However, no similar provision is made for an accountant to discuss a disclosure with its *customer*.**

98. In addition, a tipping off offence will not be committed where a disclosure is permitted under the *Tipping Off Regulations* – known as a "**protected disclosure**". A disclosure will be a protected disclosure where it meets the conditions set in the *Tipping Off Regulations:*

› made as a result of a legal requirement

› made with the permission of the *JFCU*

› made by an employee of a person to another employee of the same person

› a disclosure within a financial group or network

› made to another supervised person (but not an equivalent business) or

› made to the *JFSC*.

99. Except where it is made pursuant to a legal requirement or with the permission of the *JFCU*, a disclosure will not be a protected disclosure under the *Tipping Off Regulations* unless it is made in good faith for the purpose of preventing or detecting *money laundering* or the *financing of terrorism*.

100. Whilst the *Tipping Off Regulations* permit disclosure **of the fact** that a *SAR* has been or will be made and/or any information relating to the *SAR*, they do not permit the *SAR* form or copy of the *SAR* form to be disclosed (except where done pursuant to a legal requirement or by one employee of a person to another employee of that person within Jersey).

101. In a case where a *supervised person*:

› is the *customer* of a financial institution or designated non-financial business or profession (A) that is not a *supervised person* and

› is acting for one or more third parties; and

› has undertaken to make a disclosure to A when it makes a *SAR* in respect of any of those third parties;

a tipping off offence is committed, except where such a disclosure is made with the permission of the *JFCU*.

102. Care should also be exercised where a person is also subject to legislation in force outside Jersey. Notwithstanding that a disclosure may be a protected disclosure under the *Tipping Off Regulations*, this protection will not extend to an offence that is committed where a disclosure is not permitted under that other legislation.

Statutory requirements (paraphrased wording)

103. *Article 35(4) of the Proceeds of Crime Law and Article 35(4) of the Terrorism Law make it an offence to disclose the fact that a SAR has been or will be made, or any information otherwise relating to such a SAR, if a person knows or suspects that a SAR has been or will be made, except if the disclosure is a **protected disclosure** under the Tipping Off Regulations.*

104. *Article 35(2) of the Proceeds of Crime Law and Article 35(2) of the Terrorism Law make it an offence to disclose any information relating to an investigation, or to interfere with material which is likely to be relevant to such an investigation, where a person knows or suspects that the Attorney General or any police officer is acting or proposing to act in connection with money laundering or financing of terrorism investigation - except if the disclosure is a* ***protected disclosure*** *under the Tipping Off Regulations.*

105. *Article 35(5) of the Proceeds of Crime Law and Article 35(5) of the Terrorism Law provide for the States of Jersey to make Regulations, specifying cases where a disclosure or interference shall not amount to an offence.*

106. *Articles 35(2) and (4) do not apply to the disclosure of an investigation or SAR which is made by a relevant person to:*

- *a professional legal adviser in connection with the provision of legal advice or for the purpose of actual or contemplated legal proceedings or*
- *an accountant for the purpose of enabling that person to provide external accounting services, tax advice, audit services or insolvency services*

so long as it is not made with a view to furthering a criminal purpose.

107. *A person who is guilty of an offence under Article 35 of either of the above laws is liable to imprisonment for a term not exceeding 5 years or a fine, or to both.*

108. *Regulation 2 of the Tipping Off Regulations lists disclosures that are protected disclosures. A disclosure will be protected where:*

- *it is made in good faith for the purpose of preventing or detecting money laundering or the financing of terrorism and it falls with any of the cases specified in Regulations 3 to 7*
- *it is made in good faith for the purpose of preventing or detecting money laundering or the financing of terrorism and it is made to a person's MLRO (or deputy MLRO)*
- *it is required to be made by statute in Jersey or law elsewhere*
- *it is made with the permission of the JFCU.*

109. *A disclosure that is required to be made by statute or law may include transmission of the form used to make a SAR (or copy thereof).*

110. *Regulation 3 of the Tipping Off Regulations permits an employee of a relevant person ("**D**") to make a disclosure to another employee of the same person ("**R**"). Such a disclosure may include transmission of* ***the form*** *used to make a SAR (or copy thereof) so long as the recipient of the disclosure is a person within Jersey. Such a disclosure may also include the name of the individual who has made the internal SAR.*

111. *Where a further disclosure is made by R in accordance with the Tipping Off Regulations (other than under Regulation 3), it may* ***not*** *disclose the identity of D.*

112. *Regulation 4 of the Tipping Off Regulations permits a relevant person and an employee of such a person ("**D**") to make a disclosure to a person in another part of its financial group or with whom D shares common ownership, management or compliance control ("**R**"). Such a disclosure may* ***not*** *include transmission of* ***the form*** *used to make a SAR (or copy thereof), nor may it disclose the identity of the individual who has made the internal SAR.*

113. *Where a further disclosure is made by R in accordance with the Tipping Off Regulations, it may* ***not*** *disclose the identity of D, where D is an individual.*

114. *Regulation 5 of the Tipping Off Regulations permits a relevant person and an employee of such a person ("**D**") to make a disclosure to another relevant person ("**R**") where the disclosure relates to a person who is a customer (or former customer) of both D and R, or relates to a transaction, or provision of a service, including both D and R. Such a disclosure may **not** include transmission of **the form** used to make a SAR (or copy thereof), nor may it disclose the identity of the individual who has made the internal SAR.*

115. *Where a further disclosure is made by R in accordance with the Tipping Off Regulations, it may **not** disclose the identity of D nor D's MLRO (or deputy MLRO).*

116. *Regulation 6 of the Tipping Off Regulations permits a relevant person and an employee of a relevant person to make a disclosure to any of the following:*

- *a customs officer, a police officer or any employee of the JFCU*
- *the JFSC*

117. *Where a further disclosure is made by any of the above in accordance with the Tipping Off Regulations (other than under Regulation 6), it may not disclose the identity of the relevant person, except where the recipient is a customs officer, a police officer, any employee of the JFCU, or the Commission.*

AML/CFT/CPF Code of Practice

118. In addition to reporting procedures that must be maintained under Article 21 of the *Money Laundering Order*, a *supervised person* must maintain procedures that remind employees making internal *SARs* of the risk of committing a tipping off offence.

8.5.1 CDD Measures

Overview

119. Article 13(1) of the *Money Laundering Order* requires identity to be found out and evidence of identity obtained **before** the establishment of a *business relationship* or **before** carrying out a *one-off transaction*, except in some limited circumstances. Article 13(1)(c) of the *Money Laundering Order* further requires that *identification measures* be applied where a *supervised person* suspects *money laundering* or the *financing of terrorism* (at any time) or has doubts about the veracity or adequacy of documents, data or information previously obtained under *CDD* measures during the course of a *business relationship*.

120. Where a *supervised person* suspects *money laundering* or the *financing of terrorism*, the application of *identification measures* could unintentionally lead to the *customer* being tipped off if the process is not managed with due care.

121. In circumstances where an external *SAR* has been made, and where there is a requirement to apply *identification measures*, the risk of tipping off a *customer* (and its advisers) may be reduced by:

- ensuring that employees applying *identification measures* are aware of tipping off provisions and are provided with adequate support, such as specific training or assistance
- obtaining advice from the *JFCU* where a *supervised person* is concerned that applying *identification measures* will lead to the *customer* being tipped off.

122. Where a *supervised person* reasonably believes that the application of *identification measures* could lead to the *customer* being tipped off, then under Article 14(6) of the *Money Laundering Order* it is not necessary to apply such measures, where an external *SAR* has been made and the *JFCU* has agreed that the measures need not be applied.

123. Making reasonable enquiries to a *customer* in a tactful manner regarding the background to a transaction or activity that is inconsistent with the *customer's* established profile is prudent practice and forms an integral part of *CDD* measures. Such enquiries, when conducted appropriately, are less likely to result in a tipping off offence being committed.

8.5.2 Terminating a business relationship

Overview

124. The giving of consent to proceed by the *JFCU* following an external *SAR* submission is not intended to override normal commercial judgement, and a *supervised person* is not obligated to continue a *business relationship* with a *customer* they have reported upon, if such action would pose a commercial risk.

125. A decision to terminate a *business relationship* is essentially a commercial decision (except where there is a requirement to do so under Article 14 of the *Money Laundering Order*), and a *supervised person* is free to make such judgements. However, in certain circumstances a *supervised person* should consider liaising with the *JFCU* to assess whether it is likely that termination would tip off the *customer* or affect an investigation in any way. If there is continuing suspicion and there are funds which need to be returned to the *customer*, a *supervised* person should seek advice from the *JFCU*.

8.6 Disclosure to group companies and networks

Overview

126. Whilst the focus of the *Money Laundering Order* is on the role that a particular *supervised person* has in preventing and detecting *money laundering* and the *financing of terrorism*, where a *supervised person* is part of a group or larger network it is also important that they play their part in the prevention and detection of *money laundering* and the *financing of terrorism* at group or network level.

127. Accordingly, it is important that there should be no legal impediment to providing certain information to a group company or network.

128. Where a *supervised person* also wishes to disclose information to another *supervised person* (something that is anticipated under the *Tipping Off Regulations*), it will first be necessary to ensure that there is a proper basis for doing so, e.g. it has the consent of its *customer* in certain circumstances.

Statutory requirements (paraphrased wording)

129. *Article 22A of the Money Laundering Order allows a relevant person to disclose the following to any person or institution with which the relevant person shares common ownership, management or compliance control, or (where different) any person within the same financial group, where such disclosure is appropriate for the purpose of preventing and detecting money laundering and the financing of terrorism:*

- *information contained in any report made to the MLRO (or deputy MLRO)*
- *information provided to the JFCU that is in addition to that contained in an external SAR*
- *any other information that is kept under the Money Laundering Order.*

130. *Article 1(5) of the Money Laundering Order states that a person is a member of the same financial group as another person if there is, in relation to the group, a parent company or the legal person that exercises control over every member of that group for the purposes of applying group supervision under:*

- *the Core Principles for Effective Banking Supervision published by the Basel Committee;*
- *the Objectives and Principles of Securities Regulation issued by IOSCO; or*
- *the Insurance Supervisory Principles issued by IAIS.*

8.7 Investigation and the use of court orders

Overview

131. Following the receipt of a *SAR* and initial enquiries by the *JFCU*, reports are allocated to financial investigation officers for further investigation. Intelligence from reports submitted to the *JFCU* is then disseminated to other intelligence agencies, as appropriate.

132. Where additional information is required from a reporting institution following a *SAR*, it will generally be obtained pursuant to a "production order" issued by the Royal Court under the Proceeds of Crime Law, Terrorism Law, Investigation of Fraud (Jersey) Law 1991 and the Criminal Justice (International Co-operation) (Jersey) Law 2001, or a "customer monitoring order" under the *Terrorism Law*. It is a criminal offence to fail to comply with the terms of any order received under the above legislation.

133. During the course of an investigation, a *supervised person* may be served with an order designed to restrain particular funds or property pending the outcome of an investigation. It should be noted that the restraint order may not apply to all funds or assets involved within a particular *business relationship* and a *supervised person* should consider what, if any, funds and assets may still be utilised subject to having obtained the appropriate consent from the *JFCU*.

134. Upon the conviction of a defendant, a court may order the confiscation of their criminal proceeds or the confiscation of assets to a value representing the benefit of their criminal conduct, which may require the realisation of assets which were **legitimately obtained**. A *supervised person* may be served with a confiscation order in relation to **any funds or property** belonging to that defendant. For example, if a person is found to have benefited from drug dealing to a value of £100,000, then the court may order the confiscation of **any assets** belonging to that person to a value of £100,000. Confiscation of the proceeds of criminal conduct is becoming common place within many jurisdictions, and legislation in place in Jersey provides a mechanism by which overseas criminal confiscation orders may be recognised. Overseas civil confiscation orders may also be recognised in Jersey.

135. Property may also be forfeited in Jersey utilising civil proceedings under the *Terrorism Law.*

136. The *JFCU* will, from time to time, issue liaison notices to all *supervised persons*, or to a particular category of business, with the goal of obtaining additional intelligence. The *JFCU* will ensure that the requests contained within such notices are proportionate and reasonable in the circumstances. *Relevant persons* are requested to respond with any relevant information **as soon as reasonably practicable**.

8.7.1 Updates/Feedback from the JFCU

Overview

137. Because a significant proportion of *SARs* received by the *JFCU* relate to the accounts or transactions of non-Jersey residents and so are disseminated to overseas intelligence agencies, it may not be possible for the *JFCU* to provide regular updates or feedback on individual disclosures. However, the *JFCU* will provide statistics, trends and advice on a regular basis to help enhance the quality of disclosures. Alternatively a periodic newsletter may be issued. In addition the States of Jersey Police Annual Report contains some information on disclosures, prosecutions and confiscations.

8.8 Sanctions compliance reporting obligations under the Sanctions and Asset-Freezing Law

138. Jersey's financial sanctions reporting obligations are outlined on the Government of Jersey website, and more extensive sanctions guidance can be found on the JFSC website.

139. It is a criminal offence to contravene or to intentionally participate in activities knowing that the object or effect of them is to circumvent, to enable, or to facilitate the contravention of any of the prohibitions in respect of Jersey's financial sanctions regimes.

140. Jersey's financial sanctions regimes are rules-based and designed to prevent sanctions breaches. They can relate to all sorts of financial crimes, such as *money laundering*, the *financing of terrorism*, the *financing of proliferation*, bribery, corruption, misappropriation of funds, market abuse etc. Sanctions breaches can lead to a potential prosecution for criminal offences and/or financial penalties, and cause reputational damage to the supervised person and to Jersey as an international financial centre.

141. Jersey implements both UNSC sanctions and autonomous UK sanctions by implementing the relevant UK Regulations through the Sanctions and Asset Freezing Law and the Sanctions and Asset-Freezing (Implementation of External Sanctions) (Jersey) Order 2021.

142. The list of active sanctions regimes is available on the JFSC website and provides further explanation of the sanctions legal framework, including

- targeted financial sanctions related to terrorism and terrorist financing
- targeted financial sanctions related to proliferation and proliferation financing
- other sanctions regimes in effect in Jersey

143. Sanctions compliance reporting obligations under the *Sanctions and Asset Freezing Law* are separate and distinct from any legal obligation to submit a *SAR*. For example, the *Sanctions and Asset Freezing Law* requires notification to the *Minister* concerning suspected financial sanctions breaches, sanctioned persons, and frozen assets. In some circumstances, it may be necessary to submit both reports,, i.e. an external *SAR* to the *JFCU* **and** a sanctions compliance report to the *FSIU*.

144. The *Minister* is the "Competent Authority" for sanctions in Jersey. All communication regarding sanctions breaches and licencing should be made using the approved forms. These forms provide details on what information is required.

145. Even though Jersey has an independent sanctions regime, some cross-border transactions may trigger certain extra-territorial effects and sanctions compliance reporting obligations in another jurisdiction. In Jersey, failure to comply with sanctions compliance reporting obligations is a criminal offence.

146. In this section, reference to a 'person' is a reference to a natural person, as well as a legal person, body or entity. 'Designated person' is defined in the Glossary above, and essentially means persons who are subject to financial sanctions. References to the 'listing' of a person means their inclusion on the lists of designated persons. Sanctions designations lists are available on the JFSC website.

Statutory requirements (paraphrased wording)

147. *Under Article 1 of the Sanctions and Asset Freezing Law, a "relevant financial institution" includes:*

- *all financial services businesses regulated by the JFSC under regulatory laws, as specified in Part A Schedule 2 of the Proceeds of Crime Law;*
- *certain other financial services businesses listed in Part B Schedule 2 of the Proceeds of Crime Law;*
- *a person (not being an individual) that is incorporated or constituted under the law of Jersey and carries on such financial services business in any part of the world.*

148. *Under Article 32 of the Sanctions and Asset Freezing Law , a relevant financial institution must inform the Minister as soon as practicable If -*

- *(a) it holds an account of a person, has entered into dealings or an agreement with a person or has been approached by or on behalf of a person;*
- *(b) it knows, or has reasonable cause to suspect, that the person*
  - *(i) is a designated person, or*
  - *(ii) has committed, is committing or intends to commit an offence under this Law; and*
- *(c) the information or other matter on which the knowledge or reasonable cause for suspicion based came to it in the course of carrying on its business.*

149. *The information given to the Minister must include:*

- *the information or other matter on which the relevant financial institution's knowledge or reasonable cause for suspicion is based;*
- *any information that the relevant financial institution holds about the person by which the person can be identified, and;*
- *if the person is a customer or client of the institution, the nature and amount or quantity of any funds or economic resources held by the institution for the person at the time when the institution first had the knowledge or reasonable cause for suspicion.*

150. *The Minister retains the power to require additional information and to disclose information under certain conditions.*

151. *By exception, under Article 15 of the Sanctions and Asset Freezing Law, the relevant financial institution may credit frozen accounts in certain circumstances. This activity must be reported to the Minister, as soon as practicable, but in any case, within 14 days.*

152. *Under Article 35(1) of the Sanctions and Asset-Freezing Law, a person commits an offence, and is liable to imprisonment for a term of 12 months and to a fine of level 3 on the standard scale, if the person, without reasonable excuse, refuses or fails within the time and in the manner specified (or, if no time has been specified, within a reasonable time) to comply with sanctions reporting requirements.*

153. *Under Article 35(2) of the Sanctions and Asset Freezing Law, a person commits an offence, and is liable to imprisonment for a term of 2 years and to a fine, if the person –*

- *(a) knowingly or recklessly gives any information, or produces any document, that is false in a material particular in response to a requirement of sanctions reporting obligations.*
- *(b) with intent to evade the reporting provisions , destroys, mutilates, defaces, conceals or removes a document; or*
- *otherwise intentionally obstructs the Minister in the exercise of the Minister's powers. .*

Guidance notes

154. The most common types of financial sanctions include:

- targeted asset freezes, which are usually applied to named individuals, entities, and bodies, restricting their access to and ability to use funds and economic resources;
- restrictions on access to a wide variety of financial markets and services, applicable to named individuals, entities, and bodies, to specified groups or to entire sectors, such as investment bans, restrictions on access to capital markets, directions to cease banking relationships and activities, requirements to notify or seek authorisation before certain payments are made or received, and restrictions on provision of financial, insurance, brokering, advisory services or other financial assistance; and
- directions to cease all business of a specified type with a specific person, group, sector, territory, or country.

155. Financial sanctions legislation will contain prohibitions on carrying out certain activities or behaving in a certain way where financial sanctions apply. What is prohibited depends on the exact terms of the relevant financial sanctions regime.

156. A *relevant financial institution* should refer to the most up-to-date version of the sanctions legislation imposing the specific financial sanctions that apply in their case, to understand exactly what is prohibited and if there is a breach. We strongly encourage independent advice to be sought if there is any doubt in respect of this point.

157. If the financial sanction takes the form of an asset freeze, it is generally prohibited to:

- deal with the funds or economic resources belonging to or owned, held, or controlled by a designated person;
- make funds or economic resources available, directly or indirectly, to, or for the benefit of, a designated person; or
- engage in actions that directly or indirectly circumvent the financial sanctions.

158. The *relevant financial institution*, which knows or has a "reasonable cause to suspect" that it is in possession or control of, or is otherwise dealing with, the funds or economic resources of a designated person, may demonstrate their sanctions reporting compliance by undertaking and documenting the following:

- Immediately freeze funds or economic resources without notice and without delay;
- refrain from dealing with the funds or assets or making them available (directly or indirectly) to such persons unless licensed by the Minister;

- **as soon as practicable**, report any findings to the FSIU, together with any additional information that would facilitate compliance with the *Sanctions and Asset Freezing Law*;
- provide any further information concerning the frozen assets of designated persons, if required. Examples of information to be reported to the Minister may be found in Annex A to the JFSC's Financial sanctions practical guidance.

159. "Reasonable cause to suspect" refers to an objective test that the Court uses to ascertain whether there were factual circumstances from which an honest and reasonable person should have inferred knowledge, or formed the suspicion, of a sanctions breach.

160. The requirement to disclose a breach to the Minister "as soon as practicable" after discovery of the breach is dependent on the circumstances in each case. Although it is reasonable for a person to take some time to assess the nature and extent of the breach, and/or seek advice, this should not delay an effective response to the breach. A *relevant financial institution* should demonstrate their decision-making process and document any reason for a reporting delay.

161. Where full disclosure is not possible, it is recommended that a relevant financial institution makes an early disclosure with partial information on the basis that it is still working out the facts and will make a further disclosure as soon as possible.

162. Sanctions reporting is not generally related to a tipping-off offence since sanctions designations are public. However, there may be circumstances when tipping off provisions may apply, such as when a SAR has been submitted for related suspected money laundering or the financing of terrorism.

163. The sanctions landscape is constantly changing and evolving. It requires dedicated and qualified staff to ensure that all sanctions designation changes are reviewed and implemented without delay through effective sanctions screening and asset-freezing processes. A relevant financial institution may demonstrate an effective sanctions compliance culture by:

- having appropriate procedures and controls in place to ensure that there are dedicated staff assigned to sanction compliance monitoring and reporting;
- evidencing that relevant training is provided to the assigned employees and to management, including sanctions evasion techniques and identification of sanctions evasion;
- ensuring that the requisite report is filed in accordance with the legislation relevant to the particular sanctions regime and its guidance;
- appropriate sanctions reporting record-keeping.

164. The JFSC and the Government of Jersey provide regular updates on sanctions matters, and deliver sanctions webinars, workshops, and presentations. Further information, including a, description of sanctions regimes in effect in Jersey and their relevant guidance, is available on the JFSC website. Further sources of information in respect of proliferation financing are also available on the JFSC's "Additional information sources – ML/TF/PF" page.

9 SCREENING, AWARENESS AND TRAINING OF EMPLOYEES

9.1 Overview of section

1. One of the most important controls over the prevention and detection of *money laundering,* the *financing of terrorism* and the *financing of proliferation* is to have appropriately screened employees who are:

› alert to money laundering, terrorist financing, and proliferation financing risks and

› well trained in the recognition of notable transactions or activity which may indicate money laundering, the financing of terrorism, or the financing of proliferation activity (see Section 6 of this Handbook).

2. The effective application of even the best designed *systems and controls* (including *policies and procedures*) is compromised if employees lack competence, integrity, are unaware of, or fail to apply, *systems and controls* (including *policies and procedures*), or if employees are not adequately trained.

3. It is essential that a *supervised person* takes action to make sure that *customer*-facing and other employees are:

› competent and have integrity

› aware of policies and procedures and their obligations under the *Anti-Money Laundering and Counter-Terrorism Legislation* and the AML/CFT/CPF Codes of Practice issued under the *Supervisory Bodies Law*

› trained in the recognition of notable transactions or activities (which may indicate money laundering, the financing of terrorism, or the financing of proliferation) or transactions and activity with *enhanced risk states* and/or sanctioned parties (see Section 6 of this Handbook).

4. In particular, *customer*-facing employees and those who handle, or are responsible for the handling of, *customers* and transactions will provide a *supervised person* with its strongest defence, or its weakest link.

5. As noted in the Glossary, for the purposes of this Handbook the term "employee" should be understood to include officers of a *supervised person* and is not limited to individuals working under a contract of employment. It will include temporary and contract employees, and the employee of any external party fulfilling a function in relation to a *supervised person* under an outsourcing agreement.

6. A *supervised person* should also encourage its employees to maintain an active awareness of the risks of *money laundering,* the *financing of terrorism,* and the *financing of proliferation* as they carry out their duties.

9.2 Screening of *employees*

Statutory requirements (paraphrased wording)

7. *Article 11(1)(d) of the Money Laundering Order requires a relevant person to maintain appropriate and consistent policies and procedures relating to screening of employees.*

AML/CFT/CPF Code of Practice

8. A *supervised person* must screen the competence and probity of the following *employees* at the time of recruitment and where there is a subsequent change in an *employee's* role:

› *customer*-facing *employees* and other *employees* handling, or being responsible for the handling of, *business relationships* or *one-off transactions*

› *employees* directly supporting *customer*-facing *employees* or other *employees* handling or responsible for the handling of *business relationships* or *one-off transactions*, e.g. individuals processing and book-keeping *customer* transactions

› the *MLRO* (and any *Deputy MLRO*) and *MLCO* and

› the Board and senior management.

Guidance notes

9. A *supervised person* may demonstrate that *employees* are screened where it does one or more of the following, as appropriate for the nature of the employee's role and responsibilities:

› obtains and confirms references provided

› obtains and confirms employment history and qualifications disclosed

› obtains details of any regulatory action taken against the individual (or absence of such action)

› obtains and confirms details of any criminal convictions (or absence of such convictions).

10. Enquiries into an individual's criminal past must be subject to the Rehabilitation of Offenders (Jersey) Law 2001, which prevents a *supervised person* requesting information from its directors, senior managers and other employees (and prospective directors, senior managers and other employees) about convictions that are "spent", except where provided for by the Rehabilitation of Offenders (Exceptions) (Jersey) Regulations 2002.

9.3 Obligations to promote awareness and to train

Overview

11. The *Money Laundering Order* requirements concerning both the promotion of awareness and the provision of training apply to *employees* whose duties relate to the provision of a *supervised business* (defined in the Glossary as "relevant employees"). They do not apply to all *employees* of a *supervised person*. However, *money laundering,* the *financing of terrorism,* and the *financing of proliferation* offences established in the *Proceeds of Crime Law, Terrorism Law* and other legislation are wider in scope, therefore all *employees* will need to have a basic understanding of *money laundering,* the *financing of terrorism,* and the *financing proliferation* and how they may manifest themselves. All *employees* must also know and apply internal reporting procedures and know the identity of the *MLRO* (and, if applicable, the *Deputy MLRO*) and know how to contact them.

12. *Relevant employees* will include, among others, relationship managers, accounting and book-keeping staff, and stock-brokers.

Statutory requirements (paraphrased wording)

13. *Articles 11(9), (10), (10A), (11) and (12) of the Money Laundering Order require that a relevant person must, in relation to employees whose duties relate to the provision of a financial services business:*

- *take appropriate measures from time to time for the purposes of making them aware of:*
  - *the CDD, record-keeping, reporting and other policies and procedures for the purposes of preventing and detecting money laundering and the financing of terrorism*
  - *the enactments in Jersey relating to money laundering and the financing of terrorism and any relevant Code of Practice.*
- *provide those employees from time-to-time with training in the recognition and handling of:*
  - *transactions carried out by or on behalf of any person who is or appears to be engaged in money laundering or the financing of terrorism*
  - *other conduct that indicates that a person is or appears to be engaged in money laundering or the financing of terrorism.*

Such training to include the provision of information on current money laundering techniques, methods and trends and on the financing of terrorism

- *establish and maintain procedures that monitor and test the effectiveness of the relevant person's policies and procedures, employees' awareness and the training provided to employees, such testing having regard to the risk of money laundering that exist in respect of the relevant person's business, and matters that may have an impact on that risk (e.g. size, nature and structure).*

AML/CFT/CPF Code of Practice

14. A *supervised person* must:

- provide *employees* who are not *relevant employees* with a written explanation of the *supervised person's* and *employees'* obligations and potential criminal liability under the *Anti-Money Laundering and Counter-Terrorism Legislation*, including the implications of failing to make an internal *SAR*
- require such *employees* to acknowledge that they understand the *supervised person's* written explanation and its procedures for making internal *SARs*.

15. In the case of a *supervised person* who is a *sole trader*, that person must be aware of the enactments in Jersey relating to *money laundering,* the *financing of terrorism,* and the *financing of proliferation* and the *AML/CFT/CPF Codes of Practice*.

16. In the case of a *supervised person* who is a *sole trader*, that person must be able to recognise and handle:

- transactions carried out by, or on behalf of, a person who is, or appears to be, engaged in *money laundering*, the *financing of terrorism*, or the *financing of proliferation*
- other conduct that indicates a person is, or appears to be, engaged in *money laundering*, the *financing of terrorism*, or the *financing of proliferation*.

Guidance notes

17. A *supervised person* may demonstrate that it has satisfied awareness raising and training obligations that apply to *relevant employees* where it includes:

› *customer*-facing *employees* and other *employees* handling, or being responsible for the handling of, *business relationships* or *one-off transactions*

› *employees* directly supporting *customer*-facing *employees* or other *employees* handling, or being responsible for the handling of, *business relationships* or *one-off transactions*, e.g. individuals processing, book-keeping and accounting for *customer* transactions

› the *MLRO* (and any *Deputy MLRO*) and *MLCO*

› the Board and senior management.

18. A *supervised person* who is a *sole trader* may demonstrate that they are aware of relevant enactments (under Paragraph 15), and are able to recognise and handle transactions and other conduct (under Paragraph 16) where they have received formal training or through self-study.

9.4 Awareness of relevant employees

Overview

19. With the passage of time between training initiatives, the level of *employee* awareness of the risk of *money laundering,* the *financing of terrorism,* and the *financing of proliferation* decreases. The utilisation of techniques to maintain a high level of awareness can greatly enhance the effectiveness of a *supervised person's* defences against *money laundering, financing of terrorism,* and *financing of proliferation* risk.

Guidance notes

20. A *supervised person* may demonstrate that it has appropriate awareness measures in place to make *relevant employees* aware of *policies and procedures* where it:

› provides them with a written explanation of its business risk assessment, in order to provide context for those policies and procedures

› provides them with case studies illustrating how products or services provided by the supervised person may be abused, in order to provide context for the application of policies and procedures

› provides ready access to its policies and procedures.

21. A *supervised person* may demonstrate that it takes appropriate measures to make *relevant employees* aware of enactments in Jersey relating to *money laundering,* the *financing of terrorism,* and the *financing of proliferation* where it:

› provides relevant employees with a written explanation of the supervised person's and employee's obligations and potential criminal liability under the Proceeds of Crime Law, Terrorism Law, Directions Law, and the Targeted Financial Sanctions Measures, including the implications of failing to make an internal SAR

› provides *relevant employees* with a written explanation of the disciplinary measures that may be applied for failing to report knowledge, suspicion, or reasonable grounds for knowledge or suspicion, without reasonable excuse, or as soon as practicable

› requires such employees to acknowledge that they understand the *supervised person's* written explanations and procedures for making internal *SARs*

› reminds employees of their obligations from time-to-time and the need to remain vigilant

› circulates relevant material, e.g. material that is published by the *JFSC* or *JFCU*, *FATF*, or *EU*, in order to provide context for enactments in Jersey

› circulates relevant media reports, in order to provide context for enactments in Jersey.

22. A *supervised person* may demonstrate that it takes appropriate measures to make *relevant employees* who are officers (e.g. directors and equivalent) aware of enactments in Jersey relating to *money laundering,* the *financing of terrorism,* and the *financing of proliferation*, where the *supervised person* also explains how officers may be held personally liable for an offence committed by the *supervised person*.

9.4.1 Monitoring and testing effectiveness

Guidance notes

23. A *supervised person* may demonstrate that it maintains procedures for monitoring and testing the effectiveness of awareness-raising where it periodically tests *employees'* awareness of:

› risks and policies and procedures and

› statutory obligations

and takes appropriate action where awareness is insufficient.

9.4.2 Technological developments

AML/CFT/CPF Code of Practice

24. Where a *supervised person* has identified a risk that may arise in relation to new products, services, business practices or technology, including where developed at group level or by outside developers (in Jersey and elsewhere), a *supervised person* must take steps to ensure that those involved in their development have a basic awareness of *money laundering,* the *financing of terrorism,* and the *financing of proliferation,* and of current *money laundering* techniques, methods and trends.

Guidance notes

25. A *supervised person* may demonstrate that developers have a basic awareness *of money laundering,* the *financing of terrorism,* and the *financing of proliferation,* and of current techniques, methods and trends where it:

› provides them with a written explanation of its business risk assessment, in order to provide context for development work

› provides case studies illustrating how new products, services, business practices and technology may be abused

› circulates any relevant material, e.g. material that is published by the *JFSC* or *JFCU*, the *FATF*, or the *EU* and

› circulates relevant media reports.

26. A *supervised person* may also demonstrate that developers have a basic awareness of *money laundering,* the *financing of terrorism,* and the *financing of proliferation* and of current techniques, methods and trends, where it obtains assurances that similar measures to those set out in Paragraph 25 are taken by group or outside developers.

9.5 Training of *employees*

Overview

27. The guiding principle for all *AML/CFT/CPF* training should be to encourage *employees*, irrespective of their level of seniority, to understand and accept their responsibility to contribute to the protection of the *supervised person* against the threat of *money laundering,* the *financing of terrorism,* and the *financing of proliferation*.

28. There can be a risk that more junior *employees*, non-customer facing *employees* and support *employees* consider that their role is less crucial than, or secondary to, that of more senior or *customer*-facing colleagues. This can lead to failures to report important information because of assumptions that the information will have already been identified and dealt with by other colleagues. A *supervised person* should be aware of this risk and take steps to address it through the training provided.

AML/CFT/CPF Codes of Practice

29. A *supervised person* must provide *employees* with adequate training at appropriate frequencies. Such training must:

› be tailored to the *supervised person* and be relevant to the *employees* to whom it is delivered

› highlight to *employees* the importance of the contribution that they can individually make to the prevention and detection of *money laundering,* the countering of *terrorist financing,* and the countering of *proliferation financing*

› cover key aspects of legislation to prevent and detect *money laundering,* counter terrorist *financing,* and counter *proliferation financing.*

9.5.1 All relevant employees

Guidance notes

30. A *supervised person* may demonstrate the provision of adequate training to *relevant employees* where it addresses:

› the supervised person and employees' obligations under the Proceeds of Crime Law, Terrorism Law, Directions Law, the Targeted Financial Sanctions Measures, Money Laundering Order and AML/CFT/CPF Codes of Practice issued under the Supervisory Bodies Law

› vulnerabilities of products and services offered by the supervised person (based on the supervised person's business risk assessment), and subsequent *money laundering*, *terrorist financing*, and *proliferation financing* risk

› policies and procedures, and employees' responsibilities under the same

› application of risk-based CDD policies and procedures

- Recognition and examination of notable transactions and activity, such as activity outside of expected patterns, unusual settlements, abnormal payment or delivery instructions and changes in the patterns of business relationships.
- money laundering, financing of terrorism, and financing of proliferation developments, including techniques, methods, trends and typologies (having regard for reports published by relevant Jersey authorities, FATF and FATF-style regional bodies (also known as FSRBs).
- management of business relationships or one-off transactions subject to an internal *SAR*, e.g. risk of committing the offence of tipping off, and dealing with questions from such customers, and/or their advisers.

9.5.2 The Board or equivalents

Guidance notes

31. A *supervised person* may demonstrate the provision of adequate training to Board members where (in addition to training for *relevant employees*) it addresses:

- conducting and recording a business risk assessment
- establishing a formal strategy to counter money laundering, the financing of terrorism, and the financing of proliferation and
- assessing the effectiveness of, and compliance with, *systems and controls* (including *policies and procedures*).

9.5.3 The *MLCO*

Guidance notes

32. A *supervised person* may demonstrate the provision of adequate training to the *MLCO* where, in addition to training for *relevant employees*, it addresses the monitoring and testing of compliance with *systems and controls* (including *policies and procedures*) in place to counter *money laundering,* the *financing of terrorism,* and the *financing of proliferation.*

9.5.4 The MLRO and Deputy MLRO(s)

Guidance notes

33. A *supervised person* may demonstrate the provision of adequate training to the *MLRO* (and, if applicable, *Deputy MLROs*) where, in addition to training for *relevant employees*, it addresses:

- the handling and validation of internal *SARs*
- liaising with the *JFSC*, *JFCU* and law enforcement
- management of the risk of tipping off and
- the handling of production and restraint orders.

9.5.5 Non-relevant *employees*

Guidance notes

34. A *supervised person* may demonstrate the provision of adequate training to *employees* who are not *relevant employees* where it addresses:

    › the threat of *money laundering*, the *financing of terrorism,* and the *financing of proliferation*; and

    › procedures for making internal *SARs*.

9.5.6 Timing and frequency of training

Guidance notes

35. A *supervised person* may demonstrate the provision of training at appropriate frequencies by:

    › providing all *employees* with induction training **within 10 working days** of the commencement of employment and, when necessary, where there is a subsequent change in an *employee's* role and

    › delivering training to all *employees* **at least once every two years**, and otherwise determining the frequency of training for *relevant employees* on the basis of risk, with more frequent training delivered where appropriate.

9.5.7 Monitoring the effectiveness of screening, awareness and training

Overview

36. Monitoring and testing the effectiveness of *policies and procedures*, awareness-raising measures and of training provided is a function of the *MLCO*, further detail of which is set out at Section 2.5 of the *AML/CFT/CPF* Handbook.

37. Such monitoring and testing should also be considered in the context of the Board's periodic check that *systems and controls* (including *policies and procedures*) are operating effectively, as set out at Section 2.4.1 of the *AML/CFT/CPF* Handbook.

10 RECORD-KEEPING

10.1 Overview of section

1. This section outlines the statutory provisions concerning record-keeping for the purposes of countering *money laundering* and the *financing of terrorism*. It also sets *AML/CFT/CPF Codes of Practice* and provides guidance on the keeping of records. More general obligations on *supervised persons* to maintain records in relation to their business are not addressed in this section – these may extend the period for which records must be kept.
2. Record-keeping is essential to facilitate effective investigation, prosecution and confiscation of criminal property. If law enforcement agencies, either in Jersey or elsewhere, are unable to trace criminal property due to inadequate record-keeping, then prosecution for *money laundering,* the *financing of terrorism,* or the *financing of proliferation* and confiscation of criminal property may not be possible. Likewise, if the funds used to finance terrorist activity or proliferation activity cannot be traced back through the financial system, then the sources and the destination of *terrorist financing* or *proliferation financing* will not be identified.
3. Record-keeping is also essential to facilitate effective supervision, allowing the *JFSC* to supervise compliance by *supervised persons* with statutory requirements and *AML/CFT/CPF Codes of Practice*. Records provide evidence of the work that a *supervised person* has undertaken to comply with these requirements. Records also provide a necessary context for the opinion that may be prepared on the truth and fairness of a *supervised person's* financial statements by its external auditor.
4. Records may be kept:
   - by way of original documents
   - by way of copies of original documents (certified where appropriate)
   - in scanned form or
   - in computerised or electronic form.

10.2 Recording evidence of identity and other *CDD* measures

Overview

5. In relation to evidence of a *customer's* identity, a *supervised person* must keep a copy of, or references to, the evidence of the *customer's* identity obtained during the application of *CDD* measures. In circumstances where it would not be possible to take a copy of the evidence of identity (such as where evidence is obtained at a *customer's* home and photocopying facilities are not available), a record will be made of the type of document and its number, date and place of issue, so that the document may be obtained from its issuing authority if necessary.
6. In addition, a *supervised person* must keep supporting documents, data and information in respect of a *business relationship* or *one-off transaction* including:
   - documents, data and information obtained under *identification measures*
   - accounts files
   - business correspondence and
   - the results of any analysis undertaken.

Statutory requirements (paraphrased wording)

7. *For the purpose of the record retention requirements set out below, Article A19 of the Money Laundering Order defines a 'relevant person' as including a person who **was formerly** a relevant person.*

8. *Article 19(2)(a) of the Money Laundering Order requires a relevant person to keep the following records:*

   - *copies of evidence of identity or information that enables a copy of such evidence to be obtained*
   - *all the supporting documents, data and information in respect of a business relationship or one-off transaction which is the subject of CDD measures, including the results of analysis undertaken in relation to the business relationship or any transaction.*

9. *Article 19(4) of the Money Laundering Order requires a relevant person to keep records in such a manner that they can be made available swiftly to the Commission, police officer or customs officer for the purpose of complying with a requirement under any enactment, e.g. a production order under Article 40 of the Proceeds of Crime Law*.

10. *Articles 20(1) and 20(2) of the Money Laundering Order require a relevant person to keep records for at least five years from:*

    i) the end of the business relationship with the customer or

    ii) the completion of the one-off transaction.

11. *Article 20(5) of the Money Laundering Order allows the Commission to require a relevant person to keep records for a period longer than five years.*

Guidance notes

12. A *supervised person* may demonstrate that it keeps all supporting documents, data and information in respect of a *business relationship* or *one-off transaction* where it keeps accounts files and business correspondence.

10.3 Recording transactions

Overview

13. Details of all transactions carried out by *a supervised person* with or for a *customer* in the course of carrying on a *supervised business* must be recorded. Additional records in support of such transactions, in whatever form they are used, e.g. credit/debit slips, cheques, will also be kept.

Statutory requirements (paraphrased wording)

14. *Article 19(2)(b) of the Money Laundering Order requires a relevant person to keep a record containing details of every transaction carried out with or for the customer in the course of a financial services business. In every case, sufficient information must be recorded to enable the reconstruction of individual transactions.*

15. *Article 19(4) of the Money Laundering Order requires a relevant person to keep records in such a manner that they can be made available swiftly to the Commission, police officer or customs officer for the purpose of complying with a requirement under any enactment, e.g. a production order under Article 40 of the Proceeds of Crime Law.*

16. *Article 20(3) of the Money Laundering Order requires a relevant person to keep records relating to transactions for at least five years from the date when all activities relating to the transaction are completed.*

17. *Article 20(5) of the Money Laundering Order allows the Commission to require a relevant person to keep records of transactions for a period that is longer than five years.*

AML/CFT/CPF Codes of Practice

18. A record must be kept of the following for every transaction carried out in the course of a *business relationship* or *one-off transaction*:
    - the name and address of the *customer*
    - if a monetary transaction, the kind of currency and the amount
    - if the transaction involves a *customer's* account, the number, name or other identifier for the account
    - the date of the transaction
    - details of the counterparty, including account details
    - the nature of the transaction and
    - details of the transaction.

19. *Customer* transaction records must provide a clear and complete transaction history of incoming and outgoing funds or assets.

Guidance notes

20. A *supervised person* may demonstrate that it has kept details of a transaction where it records:
    - valuation(s) and price(s)
    - the form in which funds are transferred (e.g. cash, cheque, electronic transfer)
    - memoranda of instruction(s) and authority(ies)
    - memoranda of purchase and sale
    - custody of title documentation.

21. A *supervised person* may demonstrate that it has a clear and complete transaction history where it records **all transactions undertaken on behalf of a *customer*** within that *customer's* records. For example, a *customer's* records should include all requests for wire transfer transactions where settlement is provided other than from funds drawn from a *customer's* account with the *supervised person*.

22. When original vouchers or documents are used for account entry, e.g. credit/debit slips and cheques, and not returned to the *customer*, a *supervised person* may demonstrate that it has kept details of a transaction where such vouchers or documents are kept for at least one year to assist forensic analysis.

10.4 Other recording-keeping requirements

10.4.1 Corporate governance

AML/CFT/CPF Codes of Practice

23. A *supervised person* must keep each business risk assessment that it conducts and records under Section 2.3 of the *AML/CFT/CPF Handbook* for a period of five years after the end of the calendar year in which it is superseded.

24. A *supervised person* must keep adequate and orderly records of its *systems and controls* (including *policies and procedures*) that it must document under Section 2.3 of the *AML/CFT/CPF Handbook* for a period of at least five years after the end of the calendar year in which they are superseded.

25. A *supervised person* must keep adequate and orderly records showing how the Board/senior management has assessed both the effectiveness of, and compliance with, *systems and controls* (including *policies and procedures*) in line with Section 2.3 of the *AML/CFT/CPF Handbook*, including reports presented by the *MLCO* on compliance matters and the *MLRO* on reporting, for a period of five years after the end of the calendar year in which a matter is considered.

26. A *supervised person* must keep a record of what barriers (including cultural barriers) exist to prevent the operation of effective *systems and controls* (including *policies and procedures*) in line with Section 2.3 of the *AML/CFT/CPF Handbook* for a period of five years after the end of the calendar year in which a matter is considered.

27. A *supervised person* must keep adequate and orderly records to demonstrate the *MLRO* (and *Deputy MLRO*) and *MLCO's* experience and skills, independence, access to resources and technical awareness, in line with Sections 2.5 and 2.6 of the *AML/CFT/CPF Handbook* for a period of five years after the end of the calendar year in which an individual ceases to act in said positions.

28. A *supervised person* must keep adequate and orderly records to demonstrate that in line with Section 2.3 of the *AML/CFT/CPF Handbook*:

    - measures that are at least equivalent to *AML/CFT/CPF Codes of Practice* are applied to *supervised business* carried on by a *supervised person* through *overseas branches* and
    - subsidiaries are required to apply measures that are at least equivalent to *AML/CFT/CPF Codes of Practice*

    for a period of five years after the end of the calendar year in which a measure is applied.

10.4.2 Identification measures

AML/CFT/CPF Code of Practice

29. Where a *supervised person* is required to apply an *identification measure* through an *AML/CFT/CPF Code of Practice* set in Sections 4, 5 and 7 of the *AML/CFT/CPF Handbook*, an adequate and orderly record of that measure must be kept in line with the record-keeping requirements set out in Part 4 of the Money Laundering Order.

30. A *supervised person* must keep its risk assessment for each *customer* that has still to be remediated in line with Section 4.7.2 of the *AML/CFT/CPF Handbook* for a period of five years after the end of the calendar year in which it is superseded.

10.4.3 On-going monitoring

Guidance notes

31. A *supervised person* may demonstrate that it has kept details of the results of analysis undertaken regarding a *business relationship* or any transaction where it keeps adequate and orderly records containing the findings of its examination of notable transactions and activity, i.e. those that:

    - are inconsistent with the *supervised person's* knowledge of the *customer*
    - are complex or unusually large
    - form part of an unusual pattern or
    - present a higher risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*,

    for a period of five years from the end of the calendar year in which the examination is undertaken.

32. A *supervised person* may demonstrate that it has kept details of the results of analysis undertaken regarding a *business relationship* or any transaction where it keeps adequate and orderly records containing the findings of its examination of transactions and activity with a person which has a *relevant connection* to an *enhanced risk state*, for a period of five years from the end of the calendar year in which the examination is undertaken.

10.4.4 SARs

AML/CFT/CPF Code of Practice

33. A *supervised person* must keep registers of internal and external *SARs*, maintained in line with procedures required under Sections 8.3.1 and 8.3.2 of the *AML/CFT/CPF Handbook*.

34. In line with procedures required under Sections 8.3.1 and 8.3.2 of the *AML/CFT/CPF Handbook*, a *supervised person* must keep adequate and orderly records containing:

    - a copy of the form and supporting documentation used to make any internal *SAR* for that *customer*
    - enquiries made in relation to that internal *SAR* and the decision of the *MLRO* (or *Deputy MLRO*) to make or not make an external *SAR*
    - where an external *SAR* has been made, a copy of the form used to make the external *SAR* and supporting documentation provided to the *JFCU* and
    - relevant information passed to the *JFCU* after making the external *SAR*

    for a period of five years from the date that a *business relationship* ends, or if in relation to a *one-off transaction*, for five years from the date that a transaction was completed.

10.4.5 Screening, awareness and training of *employees*

AML/CFT/CPF Code of Practice

35. A *supervised person* must keep adequate and orderly records of training provided on the prevention and detection of *money laundering,* the *financing of terrorism,* and the *financing of proliferation* for five years after the end of the calendar year in which the training was provided, including:
    - the dates on which training was provided
    - the nature of the training provided
    - names of *employees* who received the training and
    - records of testing subsequently carried out to measure *employees'* understanding of the training provided, including pass rates and details of any action taken in cases of failure.

10.5 Access and retrieval of records

Overview

36. The Money Laundering Order does not specify **where** records should be kept, but the overriding objective is for *supervised persons* to be able to access and retrieve relevant information **without unreasonable delay**.

AML/CFT/CPF Code of Practice

37. A *supervised person* must keep documents, data or information obtained under *identification measures* in a way that facilitates on-going monitoring of each *business relationship*.
38. For all other purposes, the records kept by a *supervised person* must be readily accessible and retrievable by the person. Unless otherwise specified, records relating to evidence of identity, other *CDD* measures, and transactions must be accessible and retrievable **within 5 working days** (whether kept in or outside of Jersey), or such longer period as agreed with the *JFSC*. Other records must be accessible and retrievable **within 10 working days** (whether kept in or outside of Jersey), or such longer period as agreed with the *JFSC*.
39. A *supervised person* must periodically review the condition of paper and electronic records and consider the adequacy of its record-keeping arrangements.
40. A *supervised person* must periodically test procedures regarding access to and retrieval of its records.
41. Records must be maintained in a **readable format**. Where records are kept other than in readable form, they must be maintained such that they can be produced in readable form at a computer terminal in Jersey.
42. When original documents (such as transaction-related vouchers used to input data onto computer systems) that would ordinarily have been destroyed are requested for investigation purposes, a *supervised person* must ascertain whether the documents have in fact been destroyed.

10.5.1 External record-keeping

Overview

43. Where records are kept by another person (group or otherwise), or kept outside Jersey, such as under an outsourcing or storage arrangement, this will present additional factors for a *supervised person* to consider. Regardless of the particular circumstances, the *supervised person* remains responsible for compliance with all record-keeping requirements.

44. Where an *obliged person* ceases to trade or have a relationship with a *customer* for whom it has provided an assurance to a *supervised person*, particular care needs to be taken to check whether the assurance continues to have effect, or to ensure that evidence of identity is obtained from the *obliged person*. Section 5 of this Handbook deals with reliance arrangements made with *obliged persons*.

AML/CFT/CPF Code of Practice

45. A *supervised person* must not:

    › allow another person (group or otherwise) to keep records or

    › keep records outside Jersey

    where access and retrieval of records (by that person, the *JFSC* and/or law enforcement) is likely to be impeded by confidentiality or data protection restrictions.

10.5.2 Reorganisation or termination

Overview

46. Record-keeping requirements persist and are unaffected where a *supervised person*:

    › merges with another person

    › continues as another person

    › is taken over by another person

    › is subject to internal reorganisation

    › terminates its activities or

    › transfers a block of *customers* (i.e. a "book of business") to another person.

AML/CFT/CPF Code of Practice

47. A *supervised person* that undergoes mergers, continuance, takeovers or internal reorganisations, must ensure that records remain readily accessible and retrievable for the required periods stated above. This extends to the rationalising of computer systems and storage arrangements.

48. Record-keeping arrangements must be agreed with the *JFSC* where a *supervised person* terminates its activities or transfers a block of *customers* to another person.

10.6 Disclosure of records

Overview

49. The *FATF Recommendations* identify a number of cases where a financial institution (or *DNFBP*) may provide an assurance to another that it will provide documents, data or information:

    › *FATF Recommendation* 13 provides that a respondent institution (in the context of a **correspondent banking relationship**) should be able to provide relevant *customer* identification data upon request to the correspondent financial institution

- *FATF Recommendation* 17 provides that a financial institution relying upon another party should be required to take adequate steps to be satisfied that relevant documentation relating to *CDD* requirements will be made available by that party upon request and without delay.

50. Accordingly, it is important that where the respondent institution or party relied upon is a *supervised person* in Jersey, there should be no legal impediment to providing the data and information requested.

Statutory requirements (paraphrased wording)

51. *Article 16(7) of the Money Laundering Order states that, where a relevant person (including a person who was formerly a relevant person) (**A**) has given an assurance under Article 16 (or under a provision that applies outside Jersey that is equivalent to Article 16) to another relevant person (**B**), Person A **must** make available to Person B, at Person B's request, evidence of identity that Person A has obtained under Article 3 of the Money Laundering Order. Person A commits an offence under the Proceeds of Crime Law where it fails do so.*

52. *Article 17C(4) of the Money Laundering Order states that, where a relevant person (**A**) has given an assurance under Article 17C(2)(b) (or under a provision that applies outside Jersey that is equivalent to Article 17C) to another person (**B**), Person A **may** make available to Person B, at Person B's request, information and evidence of identity that Person A has obtained under Article 3 of the Money Laundering Order. However, A is not required by law to do so.*

53. *Article 19(7) of the Money Laundering Order applies to a relevant person carrying on deposit-taking business (a **respondent**) who is in receipt of banking services provided by an institution whose address is outside Jersey (a **correspondent**). It allows the respondent to provide the correspondent with evidence, documents, data and information obtained under Article 3 of the Money Laundering Order on request. However, the respondent is not required by law to provide information to the correspondent.*

11 WIRE TRANSFERS

11.1 Overview of Section

1. The EU Legislation (Information Accompanying Transfers Of Funds) (Jersey) Regulations 2017 (the *Wire Transfers Regulations*) were brought into force on 13 June 2017, following the EU's enactment of Regulation (EU) 2015/847 on Information Accompanying Transfers of Funds (the *EU Regulation*) on 20 May 2015. It implements *FATF* Recommendation 16 and promotes an enhanced framework around the traceability of transfers of funds for the purpose of preventing, detecting and investigating *money laundering,* the *financing of terrorism,* and the *financing of proliferation* and other financial crimes.
2. The *EU Regulation* expanded the regulatory requirements with the following objectives:
    - to prevent the abuse of fund transfers for *money laundering*, *terrorist financing* and other financial crime purposes
    - to detect such abuse should it occur
    - to support the implementation of restrictive measures; and
    - to allow *supervised* authorities to access the information promptly.
3. In Jersey, Regulation 2 of the *Wire Transfers Regulations* gives the *EU Regulation* full force and effect, subject to certain adaptations, exceptions and modifications as set out in its Schedule 1. In this section, any reference to a numbered Article, without further detail, is a reference to the Article so numbered of the *EU Regulation*.
4. Under the *Wire Transfers Regulations*, the following definitions apply:
    - "payment service provider" ("**PSP**") means a person, being a person registered under the *BB(J) Law*, when:
        - the person is carrying out payment services in or from within Jersey or
        - being a legal person established under Jersey law, the person is carrying out payment services in any part of the world other than in or from within Jersey
    - "intermediary payment service provider" ("**IPSP**") means a PSP that is neither that of the payer nor that of the payee and that participates in the execution of transfers of funds
    - "payer" means a person that is the holder of an account held with a PSP that allows a transfer of funds from the account or, where there is no account, a person that places an order for a transfer of funds
    - "payee" means a person that is the intended final recipient of transferred funds.
5. The core requirement is that every wire transfer must be accompanied by specific information ("**complete information**") about the payer and the payee, which should be collected and retained by payment institutions, unless special exemptions and derogations apply, including funds transfers between the British Islands (referred in this section as being the UK, Jersey, Guernsey and the Isle of Man).
6. A PSP should establish for each transfer of funds whether it acts as the PSP of the payer, the payee or as an IPSP. This will determine what information has to accompany a transfer of funds and the steps required to comply with the *Wire Transfers Regulations*.

7. The *Wire Transfers Regulations* also require PSPs to put in place effective procedures to detect transfers of funds that lack the required information about the payer and the payee, and to determine whether to execute, reject or suspend such transfers of funds.
8. In line with the Data Protection (Jersey) Law 2018, personal data obtained by PSPs should be used only for the purpose of preventing *money laundering*, *terrorist financing,* and *proliferation financing*. PSPs should ensure the confidentiality of such data.
9. Any record of information on the payer/payee should not be kept longer than is necessary for the purposes of preventing, detecting and investigating *money laundering,* the *financing of terrorism,* and the *financing of proliferation*.

11.2 Scope of the Wire Transfers Regulations

Overview

Statutory requirements (paraphrased wording)

10. *Under Article 1, the Wire Transfers Regulations shall apply to transfers of funds, in any currency, which are sent or received by PSP or IPSP established in Jersey. These apply to credit transfers, direct debits, money remittances and transfers carried out using a payment card, an electronic money instrument, or a mobile phone, or any other digital or IT prepaid or post-paid device with similar characteristics, irrespective of whether the payer and the payee are the same person and irrespective of whether the PSP of the payer and that of the payee are one and the same. For British Islands-based PSPs, it includes, but is not necessarily limited to, international payment transfers made via SWIFT, including various Euro payment systems, and domestic transfers via CHAPS and BACS.*
11. *Article 2(2) provides the reference to exclusions from the scope of the Wire Transfers Regulations.*
12. *The Wire Transfers Regulations shall not apply to transfers of funds that represent a low risk of money laundering or the financing of terrorism under Article2(4), such as:*

    - *transfers of funds, that involve the payer withdrawing cash from the payer's own payment account*
    - *transfers of funds to a public authority as payment for taxes, fines or other levies within the British Islands*
    - *transfers of funds where both the payer and the payee are PSPs acting on their own behalf*
    - *transfers of funds carried out through cheque images exchanges, including truncated cheques.*

13. *By way of exception, under Article 2(3), the Wire Transfers Regulations shall not apply to transfers of funds carried out using payment cards, electronic money instruments, mobile phones or other digital or information technology (IT) prepaid or postpaid devices with similar characteristics, where the following conditions are met:*

    (a) that card, instrument or device is used exclusively to pay for goods or services; and

    (b) the number of the card, instrument or device accompanies all transfers flowing from the transaction.

14. *By way of derogation, under Article 2(5), the Wire Transfers Regulations shall not apply to transfers of funds within the British Islands to a payee's payment account permitting payment exclusively for the provision of goods and services where all of the following conditions are met:*

(a) the PSP of the payee is subject to the requirements of the Money Laundering (Jersey) Order 2008 or the Terrorism (Jersey) Law 2002 or is subject to equivalent requirements under enactments of the United Kingdom, Guernsey or the Isle of Man;

(b) the PSP of the payee is able to trace back, through the payee, by means of a unique transaction identifier, the transfer of funds from the person who has an agreement with the payee for the provision of goods or services;

(c) the amount of the transfer of funds does not exceed EUR 1,000.

Guidance notes

Wire Transfers

15. A *supervised person* should have in place *systems and controls* (including *policies and procedures*) to ensure the conditions for the exemptions and derogations are met

16. PSPs and IPSPs may demonstrate compliance with the *Wire Transfers Regulations* if they have in place relevant *systems and controls* (including *policies and procedures*) which set out clearly:

    - which criteria they use to determine whether or not their services and payment instruments fall under the scope of the *Wire Transfers Regulations*
    - which of their services and payment instruments fall within the scope of the *Wire Transfers Regulations* and which do not, and
    - which information relating to transfers of funds has to be recorded, how this information should be recorded, and where.

17. PSPs and IPSPs may demonstrate their compliance with the application of the exemption under Article 2(3) of the *EU Regulation* when they have procedures for identifying and documenting:

    - that transfers by card, instrument or device are for goods or services, where the exemption applies, as opposed to person-to-person transfers and
    - that their systems and controls ensure that the number of the card, instrument or digital device, for example, the Primary Account Number(PAN), is provided in a way that allows the transfer to be traced back to the payer.

11.3 Outgoing transfers – obligations upon the PSP of the payer

Wire Transfers

11.3.1 Transfers for non-account holders

Statutory requirements (paraphrased wording)

18. *Under Article 4(3), the PSP of the payer shall ensure that transfers of funds are accompanied by the following complete information on the payer and the payee:*

(a) the name of the payer;

(b) a unique transaction identifier (which can trace a transaction back to the payer); and (c) one of either the payer's address, official personal document number, customer identification number or date and place of birth; ©(c) one of either the'payer's address, official personal document number, customer identification number or date and place of birth;

(d) the name of the payee; and

(e) a unique transaction identifier (which can trace a transaction back to the payee).

19. *These requirements apply to all types of transfers outside the British Islands and exceeding EUR 1, 000, whether those transfers are carried out in a single transaction or in several transactions which appear to be linked.*

20. *The 'unique transaction identifier' is defined as a combination of letters, numbers or symbols determined by the PSP, in accordance with the protocols of the payment and settlement systems or messaging systems used for the transfer of funds, which permits the traceability of the transaction back to the payer and the payee.*

21. *Under Article 5 and 6 of the Wire Transfer Regulations the following derogation applies, which allow for a reduced information to be provided:*

› Under Article 5, where all of the PSPs involved in the payment chain are established in the British Islands, the transfer shall include at least the unique transaction identifier (which can trace a transaction back to the payer and payee) for the payer and the payee. If further information is requested by the PSP of the payee or the Intermediary PSP, such information shall be provided within three working days of the receipt of a request for such information.

› Under Article 6, where PSP of the payee is established outside the British Islands, transfers of funds not exceeding EUR 1,000 shall be accompanied by at least: the names of the payer and the payee and the unique transaction identifier.

Note: For transfers of funds not exceeding EUR 1,000 the PSP of the payer need not verify the information on the payer unless the funds to be transferred have been received in cash or in anonymous electronic money, or the PSP has reasonable grounds for suspecting ML and/or FT.

11.3.2 Transfers for Account holders

Wire Transfers

Statutory requirements (paraphrased wording)

22. *Under Article 4(1) and 4(2), where a transfer of funds is made from or to an account, the PSP of the payer shall ensure that transfers of funds are accompanied by the following complete information:*

(a) the name of the payer;

(b) the payer's payment account number; and

(c) one of either the payer's address, official personal document number, customer identification number or date and place of birth;

(d) the name of the payee; and

(e) the payee's payment account number

23. *These requirements apply to all types of transfers outside the British Islands and exceeding EUR 1,000, whether those transfers are carried out in a single transaction or in several transactions which appear to be linked.*

24. *Under Article 5 and 6 of the Wire Transfer Regulations the following derogation from the requirements of Article 4 apply:*

- *where all of the PSPs involved in a transfer are established in the British Islands, Article 5 of the Regulation requires that the transfer includes a payment account number of the payer and the payee. The account number could be but is not required to be, expressed as the IBAN. If further information (for example, the name and address of the payer) is requested by the PSP of the payee or the IPSP, such information shall be provided by the PSP within three working days.*
- *under Article 6, where PSP of the payee is established outside the British Islands, transfers of funds not exceeding EUR 1,000 that do not appear to be linked to other transfers of funds which, together with the transfer in question, exceed EUR 1 000, shall be accompanied by at least: the names of the payer and the payee and the payment account numbers of the payer and of the payee.*

Note: For transfers of funds not exceeding EUR 1,000 the PSP of the payer need not verify the information on the payer unless the funds to be transferred have been received in cash or in anonymous electronic money, or the PSP has reasonable grounds for suspecting ML and/or FT.

AML/CFT/CPF Codes of Practice

Wire Transfers

25. In the case of a payer that is a company, a wire transfer must be accompanied by an address at which the company's business is conducted, or at which it may be contacted. In the case of a payer that is a trustee, a wire transfer must be accompanied by the address of the trustee.

Guidance notes

26. Linked transactions are defined as at least those transactions that are sent from the same payment account (or the same payer) to the same payee within a short time-frame, for example, within six months. PSPs and IPSPs may demonstrate that they are able to detect transfers of funds that appear to be linked where they provide, in their policies and procedures, examples of scenarios where transfers are found to be linked which are relevant to their type of business.
27. The exemptions for transfers within the British Islands arises from expediency, not principle, in order to accommodate transfers by domestic systems like BACS which are currently unable to include complete information. Accordingly, where the system used for a transfer within the British Islands has the functionality to carry complete information, it is considered a good practice to include it, and thereby reduce the likely incidence of inbound requests from payee PSPs for complete information.
28. The verification requirement set out in the Regulations will be met for an account holding customer of a PSP where the payer's identity has already been verified by CDD measures and is stored, in accordance with the *Money Laundering Order.*
29. In order to meet the technical limitations and to manage cases with multiple account holders and different addresses, the PSP of the payer may demonstrate compliance with the Wire Transfer Regulations by documenting the priority given to the payer's information in line with law enforcement purposes to trace the payer and for sanctions screening. For example, by de-prioritising titles and full middle names, whilst prioritising the initial of the given name and the full family name and at least the country and the city of address; or for joint accounts holders to provide both names, giving priority to family name over given names.

11.3.3 Batch Files – payments either inside or outside of British Islands

Wire Transfers

Statutory requirements (paraphrased wording)

30. *Under Article 6(1), transfers of funds from a single payer to several payees that are to be sent in batch files containing individual transfers shall carry only the payment account number or the unique transaction identifier of the payer, as well as complete information on the payee, provided that the batch file contains complete information on the payer that is verified for accuracy and complete information on the payee that is fully traceable.*

31. *Where the transfer is at or below the EUR 1,000 threshold it need only include:*

(a) the names of the payer and or payee; and

(b) the payment account numbers of the payer and the payee or a unique transaction identifier if there is no payment account for one or both parties.

11.4 Incoming Transfers - Obligation on the PSP of the payee and IPSP

Wire Transfers

Overview

32. Under the *Wire Transfers Regulations*, the PSPs of the payee and IPSPs are required to implement a targeted and proportionate risk-based approach to the monitoring of incoming fund transfers. The PSP of the payer holds responsibility for communicating all mandatory wire transfer information, which must be transmitted in the designated data fields of the payment message scheme.

33. If the required information on the payer or the payee has been provided only in part ("**incomplete information**") or has not been provided ("**missing information**"), there is an increased threat of *money laundering* or *terrorist financing* presented by anonymous transfers.

34. In order to address the potential risk presented by such transfers, PSPs of the payee should put in place the following measures, ensuring they are commensurate with and proportionate to the *money laundering* and *terrorist financing* risks to which the PSP or IPSP are exposed:

- effective *systems and controls* to detect transfers of funds that lack required information; and
- risk-based *policies and procedures* to determine whether to execute, reject or suspend a transfer of funds that lacks the required information.

35. Effective *policies and procedures* should be set up in a way that reflects the adoption of a risk-based approach and should clearly document the following aspects:

- which information relating to transfers of funds has to be recorded, how this information should be recorded, and where it is stored;
- which transfers of funds have to be monitored in real time and which transfers of funds can be monitored on an *ex-post* basis, and why;
- the obligations of members of staff where they detect missing or incomplete information and the processes they should follow.

36. PSPs of the payee should document which high-risk factors or combination of high-risk factors are to be considered when determining the risk-based approach, for example:
    - residual risks (risk posed by the types of *customers*, products, services, and delivery channels)
    - country risks (association with high-risk jurisdictions or relevant sanctions regimes)
    - unusual value and volume of transactions (compare to their particular business model);
    - a negative *AML/CFT/CPF* compliance record on the part of the PSP of the payer or the prior PSP in the payment chain.
37. PSPs of the payee and IPSPs should implement three methods of wire transfer monitoring: Real-Time Monitoring, Post-Event Monitoring and random Post-Event **Sampling**. It should be determined and documented which high-risk factors (or combinations of high-risk factors) will **always** trigger real-time monitoring, and which will trigger a **targeted *ex-post* review**. In cases where *ex-post* monitoring identifies concerns, subsequent transfers of funds should always be monitored in real time.
38. In addition to real-time and targeted *ex-post* monitoring, PSPs of the payee and IPSPs should regularly perform *ex-post* reviews on a **random sample** taken from all processed transfers of funds.

11.4.1 Admissible characters or input and missing information checks

Wire Transfers

Statutory requirements (paraphrased wording)

39. *Under Article 7(1) and Article 11(1), the PSP of the payee and the IPSP respectively shall implement effective procedures to detect whether the fields relating to the information on the payer and the payee in the messaging or payment and settlement system used to effect the transfer of funds have been filled in using characters or inputs admissible in accordance with the conventions of that system.*
40. *Under Article 7(2) and Article 11(2), the PSP of the payee and the IPSP shall implement effective procedures, including, where appropriate, ex-post monitoring or real-time monitoring, in order to detect whether the payer or payee information listed in those articles is missing.*

AML/CFT/CPF Codes of Practice

Wire Transfers

41. A PSP of the payee must subject incoming payment traffic to an appropriate level of post-event risk-based sampling to detect non-compliant payments.

Guidance notes

42. PSPs of the payee and IPSPs may demonstrate compliance with the *Wire Transfers Regulations* by conducting and documenting a risk assessment that covers their payment activities, taking into account the overall volume and jurisdictions of funds transfers and the roles of all bodies involved.
43. PSPs of the payee and IPSPs may demonstrate compliance with the obligation to detect inadmissible characters and inputs if their system's validation rules adopt certain controlling functions, for example, the automatic prevention of sending/receiving of payments with inadmissible characters or inputs.

44. Other specific measures may be considered for a "meaningful character check". For example, in some cases the payer and payee information fields may include incorrect or meaningless information which does not make sense, even if this information has been provided using characters or inputs in accordance with the conventions of the messaging or payment and settlement system, for example, "our client", 'my customer'', etc. A *supervised person* may identify these issues by undertaking sample testing, maintaining a list of commonly found meaningless terms and keeping it up-to-date.

45. In addition to real-time and targeted *ex-post* monitoring, PSPs of the payee and IPSPs may demonstrate an appropriate level of *systems and controls* where they perform *ex-post* reviews on a random sample taken from all processed transfers of funds.

46. PSPs of the payee and IPSPs may also wish to consider other specific measures, e.g. checking, at the point of payment delivery, that payer information is compliant and meaningful on all transfers that are collected **in cash** by payees on a "pay on application and identification" basis.

47. PSPs of the payee and IPSPs may draw on existing *policies and procedures* if they are considered sufficient to meet their obligations under the *Wire Transfers Regulations*, as long as those *policies and procedures* are subject to periodic reviews and updates, and training is provided to all relevant members of staff, including persons responsible for processing transfers of funds.

11.4.2 Managing transfers of funds with missing information or inadmissible characters or inputs

Wire Transfers

Statutory requirements (paraphrased wording)

48. *Under Article 8(1) and Article 12(1), the PSP of the payee and the IPSP shall implement effective risk-based procedures – including the measure referred to in Article 3(5) of the* Money Laundering Order *– for determining whether to execute, reject or suspend a transfer of funds lacking the required complete payer and payee information and for taking the appropriate follow-up action.*

49. *Under Article 8(2) and Article 12(2), the PSP of the payee and the IPSP should consider the most appropriate course of action on a risk-sensitive basis, which may initially include the issuing of warnings and setting of deadlines. Where the requested information is not provided by the set deadline, the PSP or IPSP should, in line with its risk-based policies and procedures:*

(a) decide whether to execute or reject the transfer

(b) consider whether or not the prior PSP in the payment chain's failure to supply the required information gives rise to suspicion; and

(c) consider the future treatment of the prior PSP in the payment chain for AML/CFT compliance purposes e.g. rejecting any future transfers of funds from that PSP, or restricting or terminating its business relationship with that PSP.

50. *Under Article 9, separate from the decision whether to execute, suspend or reject a transaction, missing or incomplete information must be considered as a factor when assessing whether a transfer of funds, or any related transaction, is suspicious and whether a disclosure is to be made under Article 34D(4) of the Proceeds of Crime Law, Articles 21(2) of the Money Laundering Order or Article 21(4) of the Terrorism Law.*

Guidance notes

Wire Transfers

51. In order to determine whether to reject, suspend or execute a transfer of funds in compliance with Articles 8 and 12, PSPs of the payee and IPSPs may consider the *money laundering*, *terrorist financing,* and *proliferation financing* risks associated with that transfer of funds and document it, for example:

    › what *money laundering*, *terrorist financing,* and *proliferation financing* concerns the type of missing information gives rise to and

    › what high-risk indicators have been identified that may suggest that the transaction presents a high *money laundering*, *terrorist financing,* and *proliferation financing* risk or gives rise to suspicion of *money laundering*, *terrorist financing,* or *proliferation financing*.

52. PSPs of the payee and IPSPs may demonstrate implementation of effective risk-based *policies and procedures* by documenting and recording all of their actions and reasons for their actions or inaction, including:

    › making a decision on rejecting the transfer and informing the prior PSP in the payment chain of the reason for the rejection

    › making a decision on execution of the transfer and sending of a request for information, before or after crediting the payee's payment account or making the funds available to the payee

    › all appropriate follow-up steps taken to obtain the response, including the issuing of warnings and setting of deadlines, before either rejecting any future transfers of funds from that prior PSP or restricting or terminating its business relationship with that prior PSP.

11.4.3 Failure to provide information

Wire Transfers

Statutory requirements (paraphrased wording)

53. *Under Article 8(2) and Article 12(2) should the PSP of the payer **repeatedly fail** to provide the required information on the payer or the payee, even after warnings and deadlines, the PSP of the payee or IPSP shall take further steps by:*

    › *either rejecting any future transfers of funds from that PSP; or*

    › *restricting or terminating its business relationship with that PSP.*

54. *The PSP of the payee or IPSP shall report that failure, and the steps taken, to the JFSC.*

Guidance note

55. A range of criteria may be used in order to assess whether a PSP of the payer or IPSP is 'repeatedly failing' to provide information, for example:

    › the percentage of transfers with missing information sent by a specific PSP or IPSP within a certain timeframe

    › the percentage of follow-up requests that were left unanswered or were not adequately answered by a certain deadline

- the level of cooperation of the requested PSP or IPSP relating to previous requests for missing information
- the type of information which is missing.

56. The report to the *JFSC* should be completed without undue delay and contain the following information as set out in the JFSC form at Appendix E1 of this Handbook:
    - the name of the PSP of the payer or IPSP identified as repeatedly failing to provide the required information
    - the country in which the PSP of the payer or IPSP is authorised
    - the nature of the breach, including:
        - the frequency of transfers of funds with missing information,
        - the period of time during which the breaches were identified and
        - any reasons the PSP of the payer or IPSP may have given to justify their repeated failure to provide the required information.
    - details of the steps the reporting PSP of the payer or IPSP has taken, including the issuing of warnings or deadlines up until the decision to restrict or terminate the relationship was made.
57. The obligation to report applies only to circumstances where information requests are not fulfilled and the PSP of the payee or IPSP invokes measures which restrict or terminate the business relationship with the PSP of the payer. The reporting requirement does not apply where a request for information is fulfilled by the PSP of the payer.

11.4.4 Additional obligations on IPSPs

Wire Transfers

Statutory requirements (paraphrased wording)

58. *Under Article 10, the IPSP shall ensure that all the information received on the payer and the payee that accompanies a transfer of funds is retained with the transfer.*

Guidance notes

59. IPSPs should satisfy themselves that their *systems and controls* enable them to comply with the requirement that all information on the payer and the payee that accompanies a transfer of funds is retained with that transfer. As part of this, IPSPs should satisfy themselves of their system's ability to convert information into a different format without error or omission.

11.5 Reporting of breaches

Wire Transfers

Statutory requirements (paraphrased wording)

60. *Under Article 21(1), PSPs shall notify the JFSC of any breaches of the Wire Transfers Regulations.*
61. *Article 21(2) requires PSPs to establish appropriate internal procedures for their employees, or persons in a comparable position, to report breaches internally through a secure, independent, specific and anonymous channel, proportionate to the nature and size of the PSP.*

62. *Under Regulation 3 of the Wire Transfers Regulations, a relevant person who contravenes any requirement of Article 21(2), shall be guilty of an offence and liable to imprisonment for a term of 2 years and to a fine. This applies to all PSPs and IPSPs, irrespective of the capacity within which the PSP or IPSP is acting.*

Guidance notes

63. A *supervised person* should ensure that any breach of the *Wire Transfers Regulations* is promptly reported to the *JFSC*.

64. The report to the *JFSC* should be completed without undue delay and contain the following information as set out in the form at Appendix E2 of this Handbook:

- the specific provision in the *Wire Transfers Regulations* which has been breached
- the nature of the breach, including its cause
- the date the breach was identified by the PSP and
- where possible, a summary of the measures taken by the PSP in relation to the breach and any subsequent changes to its *systems and controls* (including *policies and procedures*) to mitigate against a recurrence.

65. A *supervised person* should establish *policies and procedures* for the internal reporting of breaches of the *Wire Transfers Regulations* and maintain a record of those breaches and action taken, ensuring sufficient confidentiality and protection for employees who report breaches committed within the *supervised person*.

11.6 Information, data protection and record retention

Wire Transfers

Statutory requirements (paraphrased wording)

66. *Under Regulation 3 of the Wire Transfers Regulations, a relevant person who contravenes any requirement of Articles 14, 15(2) or (3), or 16 of the EU Regulation shall be guilty of an offence and liable to imprisonment for a term of 2 years and to a fine. This applies to all PSPs and IPSPs, irrespective of the capacity within which the PSP or IPSP is acting.*

67. *Under Article 14 of the EU Regulation, a relevant person shall respond fully and provide without delay all requested information concerning wire transfers to Jersey authorities responsible for preventing and combating money laundering or terrorist financing.*

68. *Under Article 15(2) of the EU Regulation, personal data shall be processed by PSPs only for the purposes of the prevention of money laundering and terrorist financing and shall not be further processed in a way that is incompatible with those purposes. The processing of personal data for commercial purposes shall be prohibited.*

69. *Under Article 15(3) of the EU Regulation, PSPs shall provide new customers with the information required pursuant to the Data Protection (Jersey) Law 2018 before establishing a business relationship or carrying out an occasional transaction (i.e. a one-off transaction). That information shall, in particular, include a general notice concerning the legal obligations of PSPs under the EU Regulation when processing personal data for the purposes of the prevention of money laundering and the financing of terrorism.*

70. *Article 16 of the EU Regulation requires that information on the payer and the payee shall not be retained for longer than is strictly necessary. PSPs of the payer and of the payee shall retain records of the information referred to in Articles 4 to 7 for a period of six years.*

Guidance notes

Wire Transfers

71. The "authorities responsible for preventing and combating *money laundering* or *terrorist financing*" described in Article 14 of the *EU Regulations* should be understood in Jersey to be the *JFSC* and the States of Jersey Police, including the *JFCU*.

11.7 Offences and criminal liability

Wire Transfers

Statutory requirements (paraphrased wording)

72. *Under Regulation 3 of the Wire Transfers Regulations, a relevant person, whether acting in the capacity of PSP of the payer, PSP of the payee or an IPSP, who contravenes any requirement of the specific provisions of the EU Regulations, which have effect in Jersey by virtue of Regulation 2, shall be guilty of an offence and liable to imprisonment for a term of 2 years, and to a fine as follows:*

- *PSP of the payer - Articles 4, 5, 6 (see section 11.3 Outgoing Transfers - Obligations upon the PSP of the Payer)*
- *PSP of the payee - Articles 7, 8, 9 (see section 11.4 Incoming Transfers - Obligations upon the PSP of the payee and IPSP)*
- *IPSP - Articles 10, 11, 12 (see section 11.4 Incoming Transfers - Obligation upon the PSP of the payee and IPSP)*

73. *In deciding whether a person has committed an offence under the Wire Transfers Regulations, the court shall take into account whether the person followed any relevant guidance that applies to the person and which was at the time issued, adopted or approved by the JFSC under any other enactment.*

74. *A person shall not be guilty of an offence under the Wire Transfers Regulations if they took all reasonable steps, and exercised all due diligence, to avoid committing the offence.*

75. *Under Regulation 4(1) of the Wire Transfers Regulations, if an offence under these Regulations committed by a limited liability partnership, a separate limited partnership, any other partnership having separate legal personality or a body corporate is proved to have been committed with the consent or connivance of:*

(a) a person who is a partner of the partnership, or a director, manager, secretary or other similar officers of the body corporate; or

(b) any person purporting to act in any such capacity;

the person is also guilty of the offence and liable in the same manner as the partnership or body corporate to the penalty provided for that offence.

76. *Under Regulation 4(2) of the Wire Transfers Regulations, if the affairs of a body corporate are managed by its members, paragraph (1) applies in relation to acts and defaults of a member in connection with the member's functions of management as if they were a director of the body corporate.*

12 TRUST COMPANY BUSINESS

12.1 Definition of Trust Company Business

1. *Trust Company Business* is defined in the Glossary above.
2. Paragraph 4 of Part A of Schedule 2 to the *Proceeds of Crime Law* includes *Trust Company Business* activity that is considered *supervised business.*
3. This section also covers activities which are not *Trust Company Business*, but are similar services provided way of business to legal persons or arrangements (Paragraph 8 of Part B of Schedule 2 to the *Proceeds of Crime Law*).

12.2 Identification measures

Overview

4. The purpose of this section is to assist with the application of *identification measures* to a *customer* where a *supervised person* establishes a *business relationship* or carries out a *one-off transaction* in the course of carrying on *trust company business*.
5. This section applies where a *supervised person* carries on a business under Article 2(3) of the *FS(J) Law* and, in the course of providing those services, the person provides any of the services specified in Article 2(4) of the *FS(J) Law* (except any activity that is explicitly excluded from the scope of Part A of Schedule 2 of the *Proceeds of Crime Law*).
6. This section also applies where a *supervised person* carries on a business that is described in paragraph 8 of Part B of Schedule 2 of the *Proceeds of Crime Law*. The effect of paragraph 8 is that this section is extended to include legal persons and legal arrangements that are not otherwise covered by the *FS(J) Law*.
7. This section **does not** deal with the provision of any service to a "COBO-only" fund. A COBO-only fund is a scheme that would be a collective investment fund (as defined in the *CIF(J) Law*) except for the fact that the capital, the collective investment of which is the object or one of the objects of the scheme or arrangement, is not acquired by means of an offer to the public of *units* for subscription, sale or exchange.
8. Activity that is excluded from the scope of Part A of Schedule 2 to the *Proceeds of Crime Law* includes individuals who:
   - act as directors in the course of employment by a trading company (that is not administered by a person carrying on *trust company business*)
   - act as directors of a company that is prudentially supervised by the *JFSC* under the *Regulatory Laws* or
   - act as, or fulfil the function of, a director to six or less companies.

12.2.1 Obligation to apply Identification Measures

TCB

Overview

9. Among other things, Article 13 of the *Money Laundering Order* requires a *supervised person* to apply *identification measures*:
   - before the establishment of a *business relationship* or before carrying out a *one-off transaction* and

› in the course of a *business relationship*, where the *supervised person* has doubts about the adequacy of information previously obtained under *identification measures*.

10. A *supervised person* ("**Person A**") that provides, acts as or fulfils one or more of the functions listed in Article 2(4) of the *FS(J) Law*, or arranges for another person ("**Person B**") to do so (where Person B is an officer or employee of Person A) will be considered to have established a business relationship under the *Money Laundering Order*.

11. Where Person B is not an officer or employee of Person A, then Person A will not be considered to have established a *business relationship* each time that it arranges for another person to act as or fulfil such function. However, a *supervised person* will need to consider whether such an arrangement (a transaction) is a *one-off transaction* as defined in Article 4 of the *Money Laundering Order*.

12. A *supervised person* that acts only as a formation agent will not be considered to have established a *business relationship* with its *customer*. However, a *supervised person* will need to consider whether forming a legal arrangement or legal person (a transaction) is a *one-off transaction* as defined in Article 4 of the *Money Laundering Order*.

13. For the avoidance of doubt, the requirement to apply *identification measures* also applies where the relationship that a *supervised person* has with its *customer* is conducted through another service provider, e.g. the *supervised person* provides a director to a client company that is administered by another person carrying on *trust company business*.

12.2.2 Information for assessing risk – Stage 1.4

TCB

Overview

14. This section must be read in conjunction with and is supplemental to, Section 3.3.2 of this Handbook, which explains how a *supervised person* may demonstrate that it has obtained appropriate information for assessing the risk that a *business relationship* or *one-off transaction* will involve *money laundering,* the *financing of terrorism,* or the *financing of proliferation*.

12.2.2.1 ***Supervised person*** **providing limited services**

Overview

15. Where a *supervised person* provides **only:**

› registered office services and/or

› secretarial services (defined in this section as "**limited services**")

That *supervised person* is unlikely to have any oversight of, or control over, the activities of the legal arrangement or legal person in the way that it would if it also provided one or more directors (or equivalent) or provided full administration services. The absence of oversight or control increases the risk that a legal arrangement or legal person may be used for *money laundering,* the *financing of terrorism,* or the *financing of proliferation*.

16. The presence of this additional risk therefore requires a *supervised person* to request additional information on its *customer*, and on the activities of the legal arrangement or legal person to which it is to provide only limited services, for the purpose of countering *money laundering,* the *financing of terrorism,* and the *financing of proliferation*.

17. The risk that a legal arrangement or legal person may be used for *money laundering,* the *financing of terrorism,* or the *financing of proliferation* is likely to be mitigated where a customer to whom only limited services are provided is a body corporate, the securities of which are listed

on an *IOSCO* compliant market or on a *regulated market*, or where a *customer* is a *regulated person* (or person who carries on *equivalent business* to any category of *regulated business*).

Guidance notes

TCB

18. In the case of a *supervised person* that provides **only** limited services to a legal arrangement or legal person, a *supervised person* may demonstrate that it has obtained appropriate information for assessing the risk that a *business relationship* or *one-off transaction* will involve *money laundering,* the *financing of terrorism,* or the *financing of proliferation* where it collects (at the time that a limited service is first provided and then on an ongoing basis thereafter) information on activities by reference to:

    - copies of minutes of directors' and members' meetings that must be kept by a company (including, in the case of a *PCC*, copies of minutes of directors' and members' meetings of the cell company and each of its cells) under Part 15 of the *Companies Law* (or equivalent for other legal persons or legal arrangements) and
    - copies of accounts that must be prepared by the directors of a company (including, in the case of a *PCC*, copies of accounts that must be prepared by the directors of the cell company and each of its cells) under Part 16 of the *Companies Law* (or equivalent for other legal persons or legal arrangements) or
    - where accounts are not required to be prepared, underlying financial records that are maintained by the directors of that company (or equivalent for other legal persons or legal arrangements).

12.2.2.2 Co-trustees and additional general partners

Overview

TCB

19. In some cases, an express trust or limited partnership may have more than one trustee or general partner respectively. In such cases, it will be necessary for a *supervised person* that is to act as trustee or general partner to obtain information on each co-trustee or additional general partner (or limited partner that participates in the management of the limited partnership) in order to fully consider *money laundering, financing of terrorism,* and *financing of proliferation* risk.

Guidance notes

TCB

20. A *supervised person* that is to act as a trustee of an express trust may demonstrate that it has obtained appropriate information for assessing the risk that a *business relationship* or *one-off transaction* will involve *money laundering,* the *financing of terrorism,* or the *financing of proliferation* where it collects information on any co-trustees of the trust.

21. A *supervised person* that is to act as a general partner of a limited partnership may demonstrate that it has obtained appropriate information for assessing the risk that a *business relationship* or *one-off transaction* will involve *money laundering,* the *financing of terrorism,* or the *financing of proliferation* where it collects information on any additional general partners or limited partners that participate in the management of the limited partnership.

22. The information requested may include why it is necessary to have more than one trustee or general partner, and the stature and regulatory track-record of the co-trustee or additional general partner.

12.2.3 Assessment of risk – Stage 2.1

TCB

Overview

23. This section must be read in conjunction with and is supplemental to Section 3.3.4 of this Handbook, which sets out a number of factors that are to be taken into account by a *supervised person* carrying on *trust company business* when assessing the risk that a *business relationship* or *one-off transaction* will involve *money laundering,* the *financing of terrorism,* or the *financing of proliferation*.

Guidance notes

24. A *supervised person* that carries on *trust company business* may demonstrate that it has assessed the risk that a *business relationship* or one-off transaction will involve *money laundering,* the *financing of terrorism,* or the *financing of proliferation* where it takes into account the following additional risk factors:

    - any failure on the part of a *customer* to be open about the *source of funds*. In the case of a trust, this could indicate that, for example, a settlor is in fact a "dummy" settlor who is using another's funds and not their own
    - any failure to be open about the purpose and intended nature of the *business relationship* or *one-off transaction*. In the case of a trust, this could indicate that, for example, a settlor is withholding information on the persons who are actually intended to benefit from the trust, e.g. a settlor only nominates charities as beneficiaries of a trust, but they do not intend that the charity will in fact benefit (known as a "blind" trust)
    - any request to include unusual or non-standard clauses in a trust instrument or other constitutional document that might indicate that the disclosed purpose of the structure is not genuine
    - any request for unusually close supervision or control of assets by a person other than the *supervised person*.

12.2.4 Identification measures: Finding out identity and obtaining evidence

TCB

Overview

25. The meaning of *identification measures* within this Handbook is set out in the Glossary above. *Identification measures* include determining who the *customer* is.

26. Where a *supervised person* carries on *trust company business* and is to act as the trustee of an express trust, *customers* will include the settlor, protector (if any), beneficiaries with a vested right and any other beneficiaries and persons who are the object of a power and that have been identified as presenting a higher risk (see Section 12.2.4.1 below).

27. Where a *supervised person* carries on *trust company business* and is to act as the general partner of a limited partnership, *customers* will include the limited partners of the partnership (see Section 12.2.4.4).

28. Where a *supervised person* carries on *trust company business* and is to provide a non-management service, such as registered office, in respect of a limited partnership, the *customer* will be the general partner acting for the limited partnership – a third party (see Section 4.4.3 of the *AML/CFT/CPF Handbook*).
29. Where a *supervised person* carries on *trust company business* and is to provide a service to a company, the *customer* will be the company (see Section 4.5.1 of the *AML/CFT/CPF Handbook*).
30. Where a *supervised person* carries on *trust company business* and is to provide a service to a foundation, the *customer* will be the foundation (see Section 4.5.3 of the *AML/CFT/CPF Handbook*).
31. Where a *supervised person* carries on *trust company business* and is to provide a service to a separate limited partnership, incorporated limited partnership or limited liability partnership, the *customer* will be the partnership (see Section 4.5.5 of the *AML/CFT/CPF Handbook*).
32. Where a *supervised person* carries on *trust company business* and is to form a company, partnership or foundation, the *customer* will be the persons who are the *beneficial owners and controllers* of the legal person (see Sections 4.3.1 and 4.5 of the *AML/CFT/CPF Handbook*).

12.2.4.1 Finding out identity – Legal arrangement that is a trust

Guidance notes

TCB

33. A *supervised person* that is to act as the trustee of an express trust may demonstrate that it has applied *identification measures* under Article 3(2)(a) of the *Money Laundering Order* to its *customer*, where it applies those measures to:
    - the settlor, including any person subsequently settling funds into the trust (except if deceased) and any person who directly or indirectly provides trust property or makes a testamentary disposition on trust or to the trust
    - any co-trustee
    - any protector
    - any beneficiary with a vested right
    - any other beneficiary or person who is the object of a power and that has been identified as presenting a higher risk and
    - any other person exercising **ultimate effective control** over the trust.
34. In any case where a settlor, protector, beneficiary, object of a power or other person referred to in paragraph 33 (the "**person**") is not an individual, a *supervised person* may demonstrate that it has identified each individual who is the person's *beneficial owner or controller* under Article 3(2)(c)(iii) of the *Money Laundering Order* where it has identified:
    - each individual with a **material controlling ownership interest** in the capital of the person (through direct or indirect holdings of interests or voting rights) or who exerts **control through other ownership means**
    - to the extent that there is doubt as to whether the individuals exercising control through ownership are *beneficial owners*, or where no individual exerts control through ownership, any other individual exercising **control** of the person **through other means**

- where no individual is otherwise identified under this section, individuals who **exercise control** of the person **through positions held** (e.g. those who have and exercise strategic decision-taking powers or have and exercise executive control through *senior management positions*).

35. For lower risk relationships, a general threshold of 25% is considered to indicate a **material controlling ownership interest** in the capital of the person. Where the distribution of interests is uneven, the percentage where effective control may be exercised (a material interest) may be less than 25% when the distribution of other interests is taken into account i.e. interests of less than 25% may be material interests.

12.2.4.2 Finding out identity – Legal arrangement that is a charitable trust (capital markets)

Guidance notes

TCB

36. A *supervised person* that is to act as the trustee of a charitable trust which is established to hold an investment in a security-issuing vehicle, or to hold security (as bare trustee for security-holders) over assets held within such a vehicle, may demonstrate that it has applied *identification measures* under Article 3(2)(a) of the *Money Laundering Order* to its customer, where it applies those measures to:
    - the originator or instigator of the capital market transaction
    - each security-holder that is able to exercise **effective control** over the underlying security-issuing vehicle.

12.2.4.3 Obtaining evidence of identity – Legal arrangement that is a trust

Overview

37. The measures that must be applied to obtain evidence of identity of beneficiaries and persons who are the object of a power and that have been identified as presenting higher risk will reflect the verification methods that are available at a particular time to the trustee. For example, it may not be appropriate to request evidence directly from the beneficiary or object of a power.

38. Where a *supervised person* is not familiar with a document obtained as evidence of identity, appropriate measures may be necessary to satisfy itself that the evidence is genuine.

AML/CFT/CPF Codes of Practice

TCB

39. All key documents (or parts thereof) obtained as evidence of identity must be in a language understood by the employees of the business and must be translated into English at the request of the *JFCU* or of the *JFSC*.

12.2.4.4 Finding out identity – Legal arrangement that is a limited partnership

Guidance notes

TCB

40. A *supervised person* that is to act as the general partner of a limited partnership may demonstrate that it has applied *identification measures* under Article 3(2)(a) of the *Money Laundering Order* to its *customer* where it applies those measures to limited partners holding a

material controlling ownership interest in the capital of the partnership (through holdings of interests or voting rights) or any other person exercising **control through other ownership means**, e.g. partnership agreements, power to appoint *senior management*, or any outstanding debt that is convertible into voting rights.

41. To the extent that there is doubt as to whether the persons exercising control through ownership are *beneficial owners*, or where no person exerts control through ownership, a *supervised person* that is to act as the general partner of a limited partnership may demonstrate that it has applied *identification measures* under Article 3(2)(a) of the *Money Laundering Order* to its customer where it applies those measures to any other person exercising **control** over the partnership **through other means**, e.g. those who exert control through personal connections, by participating in financing, because of close family relationships, historical or contractual associations or as a result of default on certain payments.

42. Where no person is identified under this section, a *supervised person* that is to act as the general partner of a limited partnership may demonstrate that it has applied *identification measures* under Article 3(2)(a) of the *Money Laundering Order* to its customer where it applies those measures to persons who exercise **control through positions held** (e.g. those who have or exercise strategic decision-taking powers or have or exercise executive control through *senior management positions*, e.g. general partner or limited partner that participates in management).

43. In any case where a partner or other person is not an individual, a *supervised person* may demonstrate that it has identified each individual who is that person's *beneficial owner or controller* under Article 3(2)(c)(iii) of the *Money Laundering Order* where it has identified:

    - each individual with a **material controlling ownership interest** in the capital of the partnership (through direct or indirect holdings of interests or voting rights) or who exerts **control through other ownership means**.
    - to the extent that there is doubt as to whether the individuals exercising control through ownership are *beneficial owners*, or where no individual exerts control through ownership, any other individual exercising **control over the partnership through other means**.
    - where no individual is otherwise identified under this section, individuals who exercise **control** of the partnership **through positions held** (e.g. those who have and exercise strategic decision-taking powers or have or exercise executive control through *senior management positions*).

44. For lower risk relationships, a general threshold of 25% is considered to indicate a **material controlling ownership interest** in the capital of a limited partnership. Where the distribution of interests is uneven, the percentage where effective control may be exercised (a material interest) may be less than 25% when the distribution of other interests is taken into account i.e. interests of less than 25% may be material interests.

12.2.4.5 Obtaining evidence of identity – Legal arrangement that is a Limited partnership

Overview

TCB

45. Where a *supervised person* is not familiar with a document obtained as evidence of identity, appropriate measures may be necessary to satisfy itself that the evidence is genuine.

AML/CFT/CPF Codes of Practice

TCB

46. All key documents (or parts thereof) obtained as evidence of identity must be in a language understood by the employees of the business and must be translated into English at the request of the *JFCU* or of the *JFSC*.

12.2.4.6 Finding out identity – Legal person that is a PCC

Overview

TCB

47. This section must be read in conjunction with and is supplemental to Sections 4.5.1 and 4.5.2 of this Handbook.

48. Under Article 127YDA(1) of the *Companies Law*, in the case of both *PCCs* and *ICCs*, a cell shall have the same registered office and secretary as the cell company. The registered office must also be in Jersey.

49. As a result, where a *supervised person* carrying on *trust company business* provides a registered office or secretary to a *PCC,* **it will do so for each cell of that *PCC* as well**. Because the cell of a *PCC* does not have the ability to enter into arrangements or contract in its own name, for the purposes of Article 3 of the *Money Laundering Order*, the *PCC* will be taken to be a *customer* acting for a third party and each cell will be taken to be a third party that is a person other than an individual. *Identification measures* must therefore be applied under Article 13 of the *Money Laundering Order* to the ***PCC*** (the customer) and **each cell** of the *PCC* (a third party).

12.2.4.7 Finding out identity – Legal person that is a *Private Trust Company*

Overview

TCB

50. Schedule 2 of the *Proceeds of Crime Law* provides that a *PTC* is not subject to the *Money Laundering Order*.

51. The basis for this concession is that *CDD* measures in respect of the specific trust or trusts that are serviced by the *PTC* will be applied by the *supervised person* registered to carry on *trust company business*, since the *PTC* is administered by the *supervised person* (see Article 13 of the *Money Laundering Order*).

52. A *supervised person* will consider the *PTC* to be its *customer* and each of the trusts serviced by the *PTC* to be third parties (which are not legal persons).

AML/CFT/CPF Codes of Practice

TCB

53. A *supervised person* that administers a *PTC* must apply *CDD* measures, record-keeping and reporting requirements to that *PTC* in line with the *Money Laundering Order*.

12.2.5 Timing of identification measures

TCB

Overview

54. This section must be read in conjunction with and is supplemental to Section 4.7 of this Handbook.

55. In line with Article 13(8) of the *Money Laundering Order*, a *supervised person* that is to act as a trustee may delay obtaining evidence of the identity of a *customer* after the time that a *business relationship* is established so long as:

    › it obtains evidence of identity at the time of, or before, distribution of trust property or income and

    › it is satisfied that there is little risk of *money laundering* or the *financing of terrorism* occurring as a result of obtaining evidence after entitlement is conferred.

56. Similar provisions should apply in a case where the *customer* of the *supervised person* changes during the course of a *business relationship*.

Guidance notes

57. During a *business relationship*, a *supervised person* that is the trustee of an express trust may demonstrate that it has obtained evidence that is reasonably capable of verifying the identity of each beneficiary with a vested right where:

    › it obtains evidence of identity at the time of, or before, distribution of trust property or income; and

    › it is satisfied that there is little risk of *money laundering* or the *financing of terrorism* occurring as a result of obtaining evidence after entitlement is conferred.

58. During the course of a *business relationship*, a *supervised person* that is the trustee of an express trust may demonstrate that it has obtained evidence that is reasonably capable of verifying the identity of a beneficiary or person who is the object of a trust power, where it does so at the time that the person is **identified as presenting a higher risk**.

12.2.6 Failure to complete identification measures

TCB

Overview

59. This section must be read in conjunction with and is supplemental to Section 4.8 of this Handbook.

60. Under Article 14 of the *Money Laundering Order*, if a *supervised person* is unable to apply *identification measures* when required to do so, then it must terminate that *business relationship* or not carry out that *one-off transaction* and consider whether to make a *SAR* to the *JFCU*.

61. This requirement may cause conflicts where a *supervised person* is acting as a trustee, its *customer* is the beneficiary or object of a power of a trust and:

    › the relationship between a *supervised person* and its *customer* is governed by other legislation - e.g. the Trusts (Jersey) Law 1984 and

    › the termination of a relationship with a *customer* (a beneficiary or object of a power) may have a prejudicial effect on the interests of other *customers*.

62. This requirement may also cause conflicts where a *supervised person* is acting as a council member, its *customer* is a foundation and the foundation is governed by the *Foundations Law*. In particular, under Article 12(3) of the *Foundations Law* the retirement or removal of the qualified member of a foundation does not take effect until **immediately before** the appointment of a new qualified person to be the qualified member of the council has taken effect.

63. In order to address such potential issues, termination of a *business relationship* may be **delayed** until such time as compliance with Article 14 of the *Money Laundering Order* does not conflict with another legal requirement, and/or does not have any prejudicial effect on the interests of other *customers*, so long as the risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* is effectively managed.

12.2.7 Provision of information by trustees

TCB

Statutory requirements (paraphrased wording)

64. *Article 2 of the Proceeds of Crime (Provision of Information by Trustees) (Jersey) Order 2021 (the Information Order) requires a person who is acting as a trustee of a trust to state that that person is acting in their capacity as trustee of that trust (and not in that person's personal capacity) when:*

- *forming a business relationship with a relevant business or*
- *conducting a one-off transaction with a relevant business.*

65. *Article 3(1) of the Information Order states that despite any provision of any trust document, or any other enactment, the trustee of a trust:*

- *must provide to a competent authority any information requested by that competent authority and*
- *may provide to a relevant business with which the trust has a business relationship, on request by that business, information regarding:*
  - *the beneficial ownership of the trust*
  - *the settlor, protector or enforcer of the trust, if any or*
  - *the assets of the trust that are to be held or managed by the relevant business under the terms of the business relationship.*

66. *Article 3(2) of the Information Order states that a request for information by an external competent authority must be made via a competent authority under an appropriate international co-operation request.*

67. *Article 3(3) of the Information Order states that on receipt of a request for information from an external competent authority under paragraph (2), a competent authority may request all or any of that information from the trust.*

13 FUNDS AND FUND OPERATORS

13.1 Overview of section

1. This section is supplemental to and should be read in conjunction with the sections of this Handbook referenced in the text below.

2. The purpose of this section is to assist with the application of *CDD*, the conduct of Risk Assessments and additional *AML/CFT/CPF* requirements by funds and fund operators. The definition of *financial services business* in the *Proceeds of Crime Law* means that both **regulated** and **prudentially supervised** funds and fund operators are subject to the same statutory requirements in the *Money Laundering Order* as **unregulated** funds and fund operators. The types of funds and fund operators to which this section applies are set out below. For the purposes of the tables below and this section:

   - references to a Fund include all sub funds and constituent parts of the Fund, e.g., those constituent parts of a fund referred to in a Certificate issued to the Jersey Certified Fund.
   - an example of a non-domiciled public fund that will be issued with a Certified Fund certificate and that is also a *supervised person* is a non-Jersey company with an established place of business in Jersey.

3.

Type of Fund	***Proceeds of Crime Law*** **Schedule 2**
Recognized funds under the *CIF(J) Law*	Part A Paragraph 3(1)(b)
Unclassified funds (not just Jersey Certified Funds but also non domiciled funds that are *relevant persons*) under the *CIF(J) Law*	Part A Paragraph 3(1)(c)
Unregulated funds under the Collective Investment Funds (Unregulated Funds) (Jersey) Order 2008 (the *Unregulated Funds Order*)	Part B Paragraph 6
CoBO funds (meaning CoBO-Only funds, Private Placement Funds (**PPFs**), Jersey Private Funds and very private funds) all under the Control of Borrowing (Jersey) Order 1958 (CoBO) (not just Jersey CoBO funds but also non domiciled funds that are *relevant persons*)	Part B Paragraphs 7(1)(h) and (n)

4.

Type of Fund Operator	***Proceeds of Crime Law*** **Schedule 2**
Functionary of recognized fund under the *CIF(J) Law*	Part A paragraph 3(1)(a)
Fund Services Business under the *FS(J) Law*	Part A paragraph 4
Those providing services related to CoBO funds (meaning CoBO-Only funds, PPFs), Jersey Private Funds and very private funds)	Part A paragraph 4 – such as carrying on: › trust company business i.e. acting as partner/trustee or providing a director › investment business Part B paragraphs 7(1)(h), (k), (l), (m) or (n)
The ***guidance notes*** will also be relevant for entities providing other services to a fund that fall within the activities listed in Schedule 2 of the *Proceeds of Crime Law*. See paragraph 6 below.	

5. Every *supervised person* has obligations pursuant to the *Money Laundering Order*. Where there are a number of different Fund Operators involved in a Fund structure their respective *CDD* obligations and subsequent *CDD* measures applied may differ. The differences may be attributable to different roles, risk appetites and risk assessments, which will determine how they fulfil their *AML/CFT/CPF* obligations.

6. Fund Operators can include all those entities and activities listed in Schedule 2 Part A and Part B of the *Proceeds of Crime Law*. The list below provides some examples of roles that *supervised persons* may hold with a Fund as their *customer*. As noted in paragraph 5 above, different *supervised persons* may have varying *CDD* obligations based on the type of service they provide to a Fund:

   - Auditor
   - Administrator/Registrar
   - Manager
   - Investment Adviser
   - Lender
   - Class G Director
   - Asset Manager
   - Distributor
   - Custodian
   - Legal Adviser

7. Natural Persons such as Class G Directors regulated under the FS(J) Law are *supervised persons* and will also have *AML/CFT/CPF* obligations. The *JFSC* has produced the guidance note "Natural Persons carrying on a Single Class of Trust Company Business" for these individuals.

8. An entity that is a "Managed Entity" (meaning an entity that is managed by a Manager of a Managed Entity registered to carry on class ZK of Fund Services Business) has the same *AML/CFT/CPF* obligations as any other Fund Operator. The JFSC has produced a guidance note for Managers of managed entities and certain managed entities.

9. Funds and Fund Operators may have different *AML/CFT/CPF* obligations. For example, any one of the Fund Operators in the list above may be neither a Jersey body corporate nor carrying on business in or from within Jersey and so will not be a *supervised person* and will not be subject to Jersey *AML/CFT/CPF* obligations. A Fund and/or Fund Operator that is not a *supervised person* may have *AML/CFT/CPF* obligations in another jurisdiction. A Non-Jersey Fund Operator that is not subject to Jersey *AML/CFT/CPF* obligations may act for a Jersey Fund, such as a Jersey Fund Company, that **does** have Jersey *AML/CFT/CPF* obligations.

13.2 AML/CFT/CPF risk assessments

Funds

13.2.1 Overview – Obligation to conduct risk assessments

10. In order to meet its *AML/CFT/CPF* obligations, a *supervised person* is required to prepare a Business Risk Assessment (**BRA**), along with a Customer Risk Assessment (**CRA**) for each of its *customers*. These obligations are covered in Sections 2.3 and 3.3.2 respectively. The BRA and CRA may be completed differently based on what the *supervised person* is/does, for example:

Supervised person	**BRA**	**CRA**
Administrator	Administrator's Business	Funds for which the administrator acts
Fund	Fund itself	Investors

11. All the *financial services businesses* defined by the *Proceeds of Crime Law* that are *supervised persons* under the *Money Laundering Order* must conduct a *BRA* and individual *CRAs*. Where the conducting of a *BRA*/*CRA* is outsourced to an external party, the *supervised person* must take adequate steps to ensure the *BRA* and *CRA* are properly conducted and documented.

Guidance notes

12. For Fund Operators who are subject to one or more of the Codes of Practice published by the *JFSC* (such as the Trust Company Business Code of Practice) there is also an obligation for a wider, operational business risk assessment to be conducted. When preparing a *BRA* or *CRA*, factors in this operational business risk assessment may be relevant. Therefore, a combined *BRA* and operational business risk assessment may be appropriate.

13. Risks that are not normally considered to be *AML/CFT/CPF*-specific may also be relevant to a *BRA*, for example, credit risk, tax risk, investor eligibility risk, cyber security etc.

14. It is common practice for a Fund to outsource the conduct of its *BRA* to an administrator. In such circumstances, the administrator will also need to conduct a *CRA* on the Fund (its customer) as it has two separate roles - acting both for itself (conducting a *BRA* on itself and *CRA* on the Fund) and as delegate for the Fund (conducting a *BRA* and *CRA* on behalf of the Fund). Although there may be similar factors considered in the *BRA* and the *CRA*, separate assessments will need to be conducted and documented.

13.2.2 Business risk assessment

Funds

15. This section is supplemental to and should be read in conjunction with Section 2.3 of this Handbook, regarding *BRAs*.

Guidance notes

16. When conducting a *BRA* there may be a number of parties involved in the creation of a Fund and the conduct of the fund business – in such circumstances, the *AML/CFT/CPF* risks arising from the involvement of all parties will need to be considered.

17. *Supervised persons* should satisfy themselves that sufficient information been obtained in relation to a fund structure to fully understand the structure and manage the risk of being involved with the proceeds of criminal conduct (or property used in or intended to be used in criminal conduct). This may include the fund itself being set up for a fraudulent purpose or the fund being used to facilitate *money laundering*. Not all of these potential factors will be applicable in every case (e.g. there may be no external finance).

18. Potential factors to consider when conducting a Fund *BRA* may include but are not limited to those set out in the table below. This list is not exhaustive and the supervised person will need to consider the risks relevant to them:

Fund	
Type of Fund	› Open/closed › Public/private › Regulated/unregulated › Listed/ unlisted › Asset Class - Private equity / venture capital / property / hedge fund / fund of funds
Rationale for Fund	› Does fund proposal make sense in light of the objective? › Capital accumulation / income producing / both
Jurisdiction/Domicile of Fund	› Local / Non-domiciled
Fund Structure	› Legal Structure: Limited partnership / company / unit trust / incorporated cell company / protected cell company / incorporated limited partnership / separate limited partnership? › Separate governing body i.e. general partner/trustee › Complex / Simple › Special Purpose Vehicles (*SPVs*) to hold assets › Part of Fund Manager's Platform › Umbrella
Conflicts of Interest	› Promoter v Fund investors › Fund Operators v Fund investors › Related parties v Fund Investors › Between Investors (Evidenced in some cases by Side Letters) › Between Fund Operators
Unusual Features	› Lock ins › Asset holding arrangements › In specie contributions

Fund	
Influential Persons	› The entities named in the list at paragraph 6 › Promoter › Investment Committee – powers, composition, independence › Consultants –value for money, related? › Valuers – independent? › Suppliers › SPV level suppliers › Letting agents › Asset managers › Developers › Legal advisers › Tax advisers › Auditors › Co-investors › Key investors/Seed investors
Risk Indicators	› PEPs › High Risk Jurisdictions › Sanctions- check the lists
Cash Flow	› In specie payments/redemptions permitted › Third party payments permitted › Early redemptions permitted › Budgetary and payment controls of monies flowing out of fund

19.

Investors / Target Market	
Type	› Retail › Professional / Sophisticated › Institutional › Co-investors at fund level or at investment level (see paragraph 25 below)
Method of Distribution/ Solicitation	› Word of mouth / club arrangement / reverse solicitation / private distribution / public distribution › Control of raising money and distribution of securities › Distributor employed › Promoter distributes › In house fund (i.e. Bank for high net worth clients) › Investment Adviser distributes › Subject to local marketing requirements e.g. AIFMD?
Investor's Holding Method	› Via intermediaries › Via nominee › Directly/indirectly › Complexity of holding structure

Investors / Target Market	
	› Rationale for holding structure
Investor information	› Source of funds › Source of wealth › Rationale

20.

Investments	
Type / Asset Class	› Property / private equity / hedge fund / fund of funds / Infrastructure etc › Liquid/illiquid assets
Listed / Unlisted	› Recognised market?
Risks associated with that Asset Class	› Diamonds / gold / luxury goods – higher *AML/CFT/CPF* risk › Have Fund and Fund Operators sufficient knowledge and competence to deal with the asset class?
Valuation	› Listed assets easier to value › Specialist assets may be difficult to value › Independent Valuer - Experts linked already to the fund?
In Specie receipt/payment	› Valuation › Title transfer effective? › Liquid/ illiquid › Related party transferring the asset?
Sanctions	› Check the *JFSC* Sanctions lists

21.

Factors Common to Fund Operators, Governing Body, Finance Provider, Investors / Target Market, Instigator / Promoter / Creator	
Stature	› Public / Private › Newly established / long established › Listed / unlisted › Global / local / number of jurisdictions / number of offices
Legal Form	› Legal person / legal arrangement
Ownership and Control	› Wide spread of ownership / control or sole ownership › Dominant directors / shareholders
Regulatory Status	› Regulated / unregulated

Factors Common to Fund Operators, Governing Body, Finance Provider, Investors / Target Market, Instigator / Promoter / Creator	
Reputation	› Subject to regulatory or other disciplinary actions › Subject to legal action › International / national reputation › Held in high regard in business community
Track Record	› Relevant experience particularly in the case of specialist funds or those perceived to be high risk, for example, futures and options funds.
Jurisdiction	› Local / non-domiciled › Multiple jurisdictional operations › Multiple branches / regional office
Solvency	› Insolvency proceedings › Judgements › Issues with accounts (Audit) › Lack of liquidity
Risk Indicators	› PEPs - Are there are any? › Sanctions - Have they been checked? › High Risk Jurisdictions – are there links?

22.

Instigator / Promoter / Creator	
Control of Fund	› Participation in structure – owns management shares, owns governing body, is investment manager /adviser/ directors on board of governing body

23.

Fund Operators	
General	› Risks in relation to fund operator role or that particular fund operator › Sub outsourcing

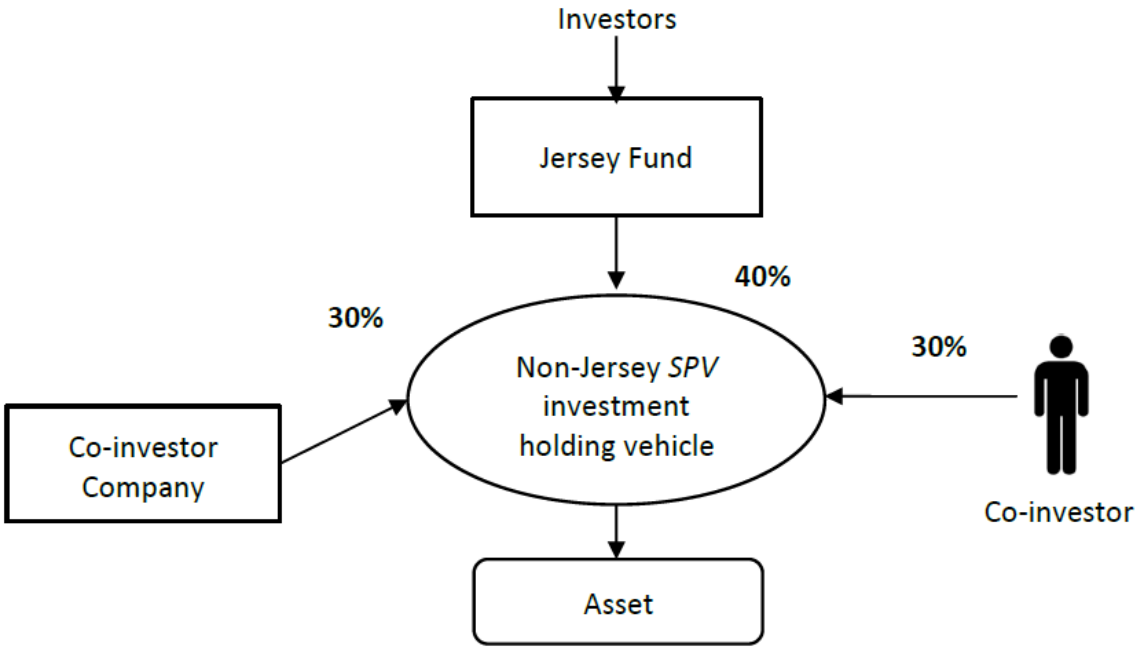
24.

Governing Body	
Control	› Independent / equal / proportionate / dominant individuals › Bank Account Mandates
Corporate Governance	› Compliance Culture, compliance monitoring policy › Frequency that Policy and Procedures are updated

25.

Finance	
Source of borrowing	› Regulated Bank / credit institution › Private finance – where are funds from? › Layers of borrowing- how many lenders? › Related party?
Structure	› Loan › Bond › Ring fencing › Priority
Security	› Secured/unsecured › Collateral › Limited recourse › Guarantor › Take title › Can lender deal with the asset it is holding as security?
Level of borrowing	› Fund › SPV
Rationale	› Make sense? › Normal commercial terms? › Unusual features?
Onward Lending	› Why? › Who to? › Benefit to the Fund?

26. An example of a factor to consider in a Fund BRA is the existence of co-investors – see the diagram below:



27. The non-Jersey *SPV* investment holding vehicle is not a *supervised person* so has no Jersey *AML/CFT/CPF* obligations.

28. The Fund's *BRA* should consider the *AML/CFT/CPF* risks arising from the existence of the Co-investors in the structure. These risks may include (but are not limited to) connections to a jurisdiction listed in Appendix D2 of the *AML/CFT/CPF Handbook* or whether the Co-investor or the *ultimate beneficial owner* of the Co-investor company is a *PEP*. Sufficient information should be obtained to assess the *AML/CFT/CPF* risks in this aspect of the business.

13.2.3 Customer risk assessment – Risk indicators

Funds

29. This section is supplemental to and should be read in conjunction with Section 3.3.4 of this Handbook.

30. The lists below provide examples of potential risk indicators and are not exhaustive. The results of any National Risk Assessment or similar must also be taken into account. The presence of one or more low or high risk indicators does not necessarily mean a *customer* is low or high risk and their rating needs to be assessed on a **case by case basis**. Risk will be assessed at initial take-on of a *customer* but will also need to be reviewed on a regular basis and at trigger events, to ensure the risk rating remains appropriate.

31. Consideration should also be given to whether it is appropriate to on-board a *customer* at all, and whether a *SAR* should be submitted.

32. Potential Higher Risk Indicators at take-on of a *customer* (Fund or investor).

    Where the customer:

    - has provided information/documentation that cannot be verified
    - has links to a *PEP*
    - has links to a *higher risk country or territory*

- is evasive / inconsistent when additional information is requested such as regarding identity of *beneficial owners* / *source of funds* / purpose and expected transactions
- has a complex structure, for example, operates via layers of representatives making identification difficult
- is revealed to have money problems (i.e. debt judgements)
- is the subject of regulatory or criminal actions or has associates with these characteristics
- acts as a nominee and there is an unwillingness to identify the underlying third party
- is a Non-Profit Organisation / Charity that might be susceptible to abuse regarding terrorist activities such as medical and emergency relief charities with an unlimited global scope. Or where a Non-Profit Organisation / Charity operates in a specific geographical area but then transfers monies to a country / territory / jurisdiction not within the specific geographical area
- is a Fund and:
    - is aiming to invest in products that may be susceptible to *money laundering*, for example diamonds and gold.
    - has a one off minimum investment amount so that it operates below AML reporting threshold amounts.
    - is a highly liquid open-ended Fund (the customer) with the possibility of frequent subscriptions and redemptions.
    - uses unregulated fund operators
    - outsources functions without any valid reasons provided
    - has a complex structure so it is difficult to ascertain who the underlying beneficiary is, for example using many *SPV*s and intermediaries.

33. Potential Higher Risk Indicators that may be flagged during ongoing monitoring of the *customer* (Fund or investor).

    Where the Fund:

- has entered or intends to enter into finance arrangements that are either at a higher rate or lower rate than usual with no rationale provided
- has or intends to purchase assets without independent valuations (particularly from connected persons)
- receives or sends monies to related or unrelated third parties that do not fit the pattern of transactions expected for the Fund and no acceptable rationale is provided
- transfers monies to *SPV*s which the Fund customer appears to have no control over
- purchases assets without proof of title from the seller and title to the assets is not clearly transferred to the Fund customer
- engages consultants who add little benefit and receive high fees (particularly in countries associated with a higher risk of corruption)
- enters into a promise to purchase agreements for which monies are paid where transactions are regularly aborted, resulting in forfeiture of the monies
- is investing with no obvious commercial rationale and is inconsistent with the Fund customer profile

- regularly pays fees, commissions and costs to source and investigate transactions, but no transactions are executed
- exhibits transaction activity that does not follow the expected pattern or changes substantively with no rational explanation
- displays endemic conflicts of interest
- regularly changes bank accounts and uses different Fund Operators in different jurisdictions.

Where the investor:

- requires a high level of liquidity and indicates funds may need to be withdrawn / moved at short notice
- is proposing an investment of an unexpected large amount.

13.2.4 Risk assessments for SPV governing bodies

Funds

34. An "SPV Governing Body" is a vehicle established for the specific purpose of acting as the governing body of a Fund. Common examples are a company established to act as the general partner of a limited partnership Fund or a trustee of a unit trust Fund.

35. A unit trust or a limited partnership has no separate legal personality, so the SPV Governing Body is considered to be the *customer* of the Fund Operator (see Article 3(2)(a) and (c) of the *Money Laundering Order*). However, trustees and general partners are also Fund Operators. Effectively they have two capacities - they are both Fund Operator and Fund governing body. For the purposes of this section if a trustee or general partner provides services to **more than one** Fund it will not be regarded as an *SPV* but will be regarded as a Fund Operator.

36. In these circumstances, its *BRA* and *CRA* conducted as Fund Operator and the *BRA* it conducts in its capacity as SPV Governing Body of the Fund are likely to significantly overlap. In order to avoid duplication of effort, it may be appropriate to consolidate these 3 Risk Assessments, provided that all relevant risks (i.e. of all 3 risk assessments) are appropriately considered.

37. This has no effect on the separate obligation of the Fund to conduct a *CRA* on each of its *customers*, i.e. the investors.

Entity	BRA	CRA	Entity	BRA	CRA
Non SPV Trustee of Unit Trust Funds	Self	Fund	*SPV* Trustee of one Unit Trust Fund	Consolidated Risk Assessment Combined BRA/CRA for Trustee and Fund BRA as SPV Trustee is intrinsically part of the Fund.	
Unit Trust	Self	Investors	Unit Trust	See above	Investors

13.2.5 Documenting risk assessments

Funds

Overview

38. This section is supplemental to and should be read in conjunction with Section 3 and Section 2 of this Handbook.

39. *Supervised persons* are required to ensure their *BRAs* and *CRAs* are properly documented.

Guidance notes

40. Comprehensive subscription agreements / investor questionnaires may assist in obtaining information on a Fund's investors and provide sufficient detail to enable the Fund to carry out a *CRA*. However, a subscription agreement / investor questionnaire **is not** a replacement for a *CRA*.

41. For certain types of products or services, standard *customer* profiles may assist the *CRA* process. In such cases, the *supervised person* will need documented procedures which consider:

    - whether the intention is to only accept investors who fit the standard *customer* profile
    - if not, how will exceptions to the standard *customer* profile be managed; either at the outset or subsequently?
    - whether (for instance) individual *CRAs* will be conducted with respect to any *customers* that do not fit the standard *customer* profile.

42. The *supervised person* always remains ultimately responsible for its Risk Assessments regardless of whether they outsource the conduct of them to another party.

13.3 Customer Identification Measures

Funds

Overview

43. Section 3 of the *AML/CFT/CPF Handbook* describes the stages of the identification process and provides guidance in relation to each stage. *CDD* is not limited to finding out the identity of the *customer* and obtaining verification (e.g. taking their personal details and copies of their passport and driving licence). The table below (explained in further detail at Section 3.3) summarises *CDD* requirements:

CDD Element	**Activity**	
Identification measures	Risk assessment	
	ID *customer*	
	ID third parties	
	ID person acting for *customer*	Verify authority to act
	Where *customer* not individual:	Understand ownership/control structure
		ID *beneficial owners/controllers*
	Obtain information on purpose/nature	
On-going monitoring	Scrutinising transactions/activity	
	Keep documents/information up-to-date	

44. The following sections provide guidance on the identification of *customers*, *ultimate beneficial owners* and third parties. These sections must be read in conjunction with the referenced sections of the *AML/CFT/CPF Handbook*.

13.3.1 Obligation to apply identification measures

Funds

Overview

45. Section 3.1 of this Handbook states that a *customer* may be an individual (or a group of individuals) or a legal person. Further guidance on finding out identity and obtaining evidence of identity is provided at the following sections:

AML/CFT/CPF Handbook Section	**Type of customer**	**Fund Structure**
4.3	Individual/group of individuals	
4.5	Legal person	› Company › Limited Liability Partnership, › Separate Limited Partnership › Incorporated Cell
4.4	Individual or legal person acting for a legal arrangement	› Trustee on behalf of a Unit Trust › General Partner on behalf of a Limited Partnership

46. For the purposes of this section, companies, limited partnerships and unit trusts will be used as practical examples as these are the most common Fund structures.

47. Each of the Fund's investors are its *customers*. The investors may take a variety of legal forms and Article 3 of the *Money Laundering Order* specifies how *identification measures* are applied to each.

Fund Structure	*Supervised person* re each Fund structure	Customer/Investor
Company	Company	› Article 3(2)(a) individual › Article 3(2)(aa) any person acting on behalf of the customer › Article 3(2)(b) acting for a third party (legal arrangement) › Article 3(2)(c) not an individual but legal person. Legal persons/arrangements apply the Three Tier Test
Limited partnership	General Partner on behalf of the Limited Partnership	
Unit Trust	Trustee on behalf of the Unit Trust	

48. The Three Tier Test refers to the process by which a *supervised person* may determine each individual who is a *beneficial owner or controller* and is covered in detail at Section 4 above. However it can be summarised as determining the individuals who exercise control through 1) ownership means and 2) other means; or 3) through positions held. When applying the Three Tier Test, if no one is present at Tiers 1 and/or 2 then consider Tier 3. There may be more than one individual at Tiers 1 and/or 2.

49. Section 3.3 lists the various steps of the identification process, of which identifying the *customer* is only a part. A *supervised person* must also understand the ownership and control of the *customer* and identify:

    › any *beneficial owners and controllers* of the *customer*

    › those third parties for whom the *customer* acts indirectly/directly (e.g. legal arrangements) and

    › others listed in Article 3(2) of the *Money Laundering Order* (which links to Article 3(7) e.g. settlor/protector).

50. The starting point is that the *supervised person* has to determine who everyone detailed in paragraph 49 above is, as part of its identification measures.

Guidance notes

Funds

51. Responsibility for applying *CDD* measures (which includes *identification measures* and on-going monitoring) rests with the **governing body** of the Fund, as detailed in the table below:

Type of Fund Entity	Responsibility
Company	Directors
Limited Partnership/Unit Trust	Directors of the general partner/trustee of the limited partnership/unit trust where the general partner/trustee is a company
Protected Cell	Directors of the protected cell company (PCC), not each of the protected cells, although the directors of the protected cells may assist with compliance

Type of Fund Entity	Responsibility
Incorporated Cell	Directors of each of the incorporated cells

13.3.2 Identification Measures - Fund operators

Funds

Guidance notes

52. A number of Fund Operators are likely to provide services to the Fund. Each will be a *supervised person*, with the Fund as their *customer*. Each will have their own *CDD* obligations pursuant to the *Money Laundering Order*.

53. Even where a Fund Operator is not providing investor-facing services and only provides services to the Fund, they should ensure when conducting their *CRA* (of their *customer* - the Fund) that they obtain sufficient information on the investors (e.g. *source of funds*) and *beneficial owners and controllers* of the Fund. Rather than gathering this information themselves, in a low risk scenario the Fund may be able to provide a list of its investors with holdings of 25% or more and *source of funds* information provided to the Fund by investors via subscription agreements/investor questionnaires (see also paragraph 135 below).

54. The first step for a *supervised person* is to determine the nature of their *customer* and determine the *customer's* potential beneficial owners and controllers, any third parties on whose behalf the *customer* acts (and any third party's *beneficial owners and controllers*) and others listed in Article 3(2) of the *Money Laundering Order*. It may not always be necessary to verify all of them.

55. The application of Article 3 differs depending on the legal form of the Fund. For the examples in the two tables below it is assumed that both the general partner and trustee are companies.

Application of Article 3 where the Fund Operator's customer is a:

Legal person i.e. a Company			
Customer	Third Party	Owners/Investors of the Fund	Governing Body
Company *Article 3(2)(a), (aa) and (c)*	N/A	Shareholder(s) (owns customer) *Article 3(2)(c)(iii)*	Directors of Company Re customer *Article 3(2)(aa), c(ii) and c(iii)*
Legal arrangement i.e. a Limited Partnership/Unit Trust			
General Partner/Trustee (Company) *Article 3(2)(a),(aa) and (c)*	Limited Partnership/Unit Trust *Article 3(2)(b)(iii)*	Limited Partner(s)/ Unit Holder(s) (owns Third Party) *Article 3(2)(b)(iii)(A), (B) and (C)* *(Note the requirements of Article 3(7))*	Directors/ Shareholders of General Partner/ Trustee Re *customer* *Article 3(2)(aa), c(ii) and c(iii)* Re third party *Article 3(2)(aa), (b)(iii)(A), (B) and (C)*

56. Once a *supervised person* fully understands the ownership and control structure of a *customer* the *supervised person* can determine the *beneficial owners and controllers* pursuant to the Three Tier Test and then apply the necessary *identification measures*.

57. The Three Tier Test is applied on a case by case basis and the table below indicates potential *beneficial owners or controllers* in different scenarios where the ***supervised person*** **is a Fund Operator and the Fund is a**:

Legal person i.e. a Company		
Customer	Third party	*Beneficial Owners/Controllers*
Company *Article 3(2)(a), (aa) and (c)*	N/A	Apply the Three Tier Test (see above) › Shareholder(s) Article 3(2)(c)(iii) - Potentially Tier 1 › Promoters/Instigators Article 3(c)(ii) - Potentially Tier 2 › Directors of Company - Potentially Tier 3 *Article 3(2)(aa), (c)(ii) and (c)(iii)*
Legal arrangement i.e. Unit Trust/Limited Partnership		
General Partner for Limited Partnership / Trustee for Unit Trust (Company) *Article 3(2)(a), (aa) and (c)*	Limited Partnership/ Unit Trust *Article 3(2)(b)(iii)*	Apply the Three Tier Test to the customer and the third party: › *customer* – General Partner/Trustee *Article 3(2)(aa) and (c)* › Third Party- Limited Partnership/Trust *Articles 3(2)(b) and 3(7)*

58. More detailed guidance on how to determine and identify *beneficial owners and controllers* is contained in the following sections of the *AML/CFT/CPF Handbook*:

Entity	**Finding out identity**	**Obtaining evidence**
Limited Partnership	4.4.3	4.4.4
Trust (not Unit Trust)	4.4.1	4.4.2
Company	4.5.1	4.5.2

13.3.3 Identification Measures - Unit trusts

Funds

Guidance notes

59. Unit trusts differ from traditional private trusts. For example, with a private family trust there is

normally a settlor who not only establishes the trust but also provides the initial funds and ongoing funding to the trust. Beneficiaries may be expressly referred to or may form part of a class and may not have a vested right to the trust assets.

60. In a unit trust the promoter or instigator may fund the establishment of the unit trust and may fund the initial investment, thus being considered a settlor. While the individual investors are not considered to be settlors for the purposes of Article 3(7)(a) of the *Money Laundering Order*, each of the unit holders will be *customers* of the Fund (unit trust) investing their money into the unit trust. This may include the promoter as an investor.

61. Statutory requirements relating to *identification measures* that apply to unit trusts are set out at Article 3(7).

13.3.4 Fund operators – Passive investors

Funds

Guidance notes

62. Identification of investors in a Fund will be approached differently by the Fund and the Fund Operator.

63. The Fund has an obligation to identify each of its investors, as they are the Fund's *customers*. This obligation exists regardless of whether they are passive investors who do not exercise control over the Fund.

64. The Fund Operator, however, has an obligation to identify the *beneficial owners and controllers* of their *customer* (the Fund) and should apply the Three Tier Test to ascertain who the *beneficial owners and controllers* are. Where ownership of a Fund is distributed widely, it may be that none of the investors control the Fund through their ownership. In such a case, these "passive" investors are not *beneficial owners* at Tier 1 and, assuming they are not controllers via Tier 2 or 3, a Fund Operator need not apply *identification measures* to them.

65. It should be noted, however, that in order to demonstrate that sufficient information has been collected on *source of funds* for a *customer* relationship, it may still be necessary to consider the provenance of investors who have a **material interest** in a *customer*, but who do not also **exercise control**. The effect of this may still be to require information to be obtained on such passive investors (though it may not be necessary to also obtain evidence of identity).

66. For example, an investment advisor giving advice directly to a regulated Fund with passive investors will still need to obtain *source of funds* information in relation to those investors in order to understand the *AML/CFT/CPF* risk posed by its *customer*.

67. The extent of *source of funds* information collected will be proportionate to the risks identified and determined on a case by case basis. In a lower risk relationship, *source of funds* information should be obtained for all passive investors with a holding of **25% or more**. Where there are no 25%+ holders, generic investor information on *source of funds* such as a generic profile could be obtained. In a higher risk relationship, more stringent measures should be applied. These measures should be determined on a case-by-case basis with reference to the *supervised person's customer* risk assessment of the relationship.

68. Similarly, in order to demonstrate that sufficient information has been collected to assess the *AML/CFT/CPF* risks posed by a *customer*, it may be necessary to consider the identity, nature, structure and location of investors who have a **material interest** in a *customer*, but who do not also **exercise control**. See Sections 3.3.2 and 3.3.4 for further detail.

13.3.5 Fund operators - Promoters

Funds

Guidance notes

69. A *supervised person* may need to consider whether the promoter of a Fund is a *beneficial owner or controller*. For example, the promoter / instigator of the Fund may have direct control by owning the governing body (i.e. the general partner or the trustee) or by owning management shares of a Fund company.

70. In addition, a promoter may also be considered to be a *beneficial owner or controller* where the Board of a Fund does not exercise sufficient effective control. For example, a promoter may be the investment adviser / investment manager or may have a significant presence on the investment committee, which may indicate "**control by other means**" (see Tier 2 of the Three Tier Test).

13.3.6 Multiple layers

Funds

Overview

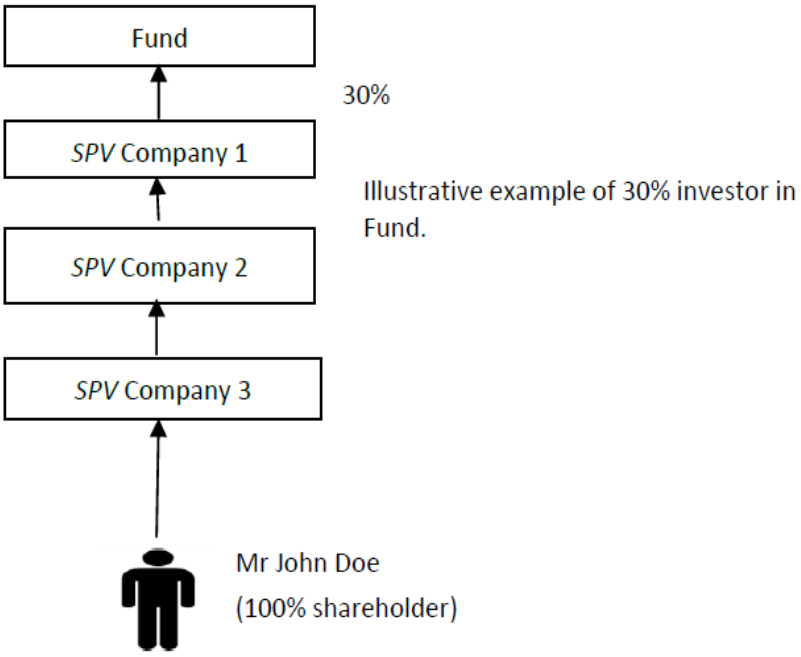
71. Fund structures are often complicated by ultimate *beneficial owners* not entering into transactions directly and there may be multiple entities, such as holding companies, trusts, nominees and intermediaries between the investment in the Fund and the individual who is the ultimate *beneficial owner*. The more complex the structure, the more difficult it may be to determine the *beneficial owner and controller*.

72. A *supervised person's* approach to a complex ownership and control structure will be informed by the risk rating allocated to that *customer*. However, as set out in Section 4 of this Handbook the following are always required to be identified:

    - the *customer*
    - the *ultimate beneficial owner(s)/controller(s)* of the *customer* (the Three Tier Test can assist *supervised persons* in working out which persons fall within this category) and
    - any third parties on whose behalf the *customer* acts.

Guidance notes

73. In the example below the Fund is the *supervised person*. The general rule is that you are trying to ascertain the ultimate individual(s) who control(s) the structure.



Customer

74. *SPV* Company 1 is the *customer* of the Fund.

75. The Fund is obliged to find out the identity of its *customer* and obtain evidence of identity. The *AML/CFT/CPF Handbook* provides guidance on *identification measures* to be applied to a legal person that is a company:

    - section 4.5.1 - Finding out the identity of a legal person that is a company and
    - section 4.5.2 - Obtaining evidence of identity of a legal person that is company.

Beneficial Owner/Controller

76. *SPV* Company 1 is a legal person and the *supervised person* must understand the ownership and control structure of the *customer*. The Fund is obliged to find out the identity and obtain evidence of identity of its *beneficial owners/controllers*. The Three Tier Test is applied in order to ascertain who controls the *customer*:

    - control via ownership and
    - control via other means or
    - control through positions held (if no-one at Tiers 1 and/or 2)

77. Understanding a *customer's* ownership and control structure will allow a *supervised person* to determine the *ultimate beneficial owner/controller*. Article 2(2) of the *Money Laundering Order* states "*…. it is immaterial whether an individual's ultimate ownership or control is direct or indirect*".

78. In this example the structure is in place for the purpose of facilitating the investment of John Doe and he is exercising effective control. Therefore, regardless of the holding companies, John Doe is the *ultimate beneficial owner/controller* of the *customer*.

79. The *AML/CFT/CPF Handbook* provides guidance for individuals (in this example John Doe):

    - section 4.3.1 - Finding out the identity of an individual

- section 4.3.2 - Obtaining evidence of identity of an individual

80. If none of the individuals with ownership interests **exercise control** then they may not need to be identified (Section 13.3.4 regarding passive investors).

Multi-layered structure

81. In the above scenario understanding the ownership and control structure of the *customer* is likely to require some effort, but it may not be necessary to obtain detailed identity information and evidence in relation to each entity in the structure.

82. Verification of identity may not be necessary in relation to *SPV* Company 2 and *SPV* Company 3 – they are not *customers* or *beneficial owners/controllers* or third parties on whose behalf the *customer* is acting (see paragraph 72 above). The reason they are not controllers is because they are acting on the instructions of the **ultimate controller** Mr John Doe and are therefore merely links in the control chain.

83. Whilst obtaining evidence of identity may not be necessary, sufficient information will still need to be obtained in relation to these two entities in order to understand the wider ownership and control structure. The information required will depend on the complexity of the structure and the overall risk of the *customer* relationship. However as a minimum for a low risk *customer* the following should be obtained:

- name of the entity
- evidence the entity exists
- names of the directors
- names of the shareholders or those with other interests
- details of ownership and control of the entity (proportion of holdings, voting rights, decision-making authority, etc.)

13.3.7 Nominees/Investment managers

Funds

Guidance notes

84. This section is supplemental to and should be read in conjunction with Section 7.15 of this Handbook regarding designated relationships and pooled relationships.

85. There may be scenarios where the Fund's *customer* is representing other parties, for example as a nominee/investment manager. In this scenario the normal obligations apply and the *supervised person* still has to identify:

- the *customer*
- the *ultimate beneficial owner/controller* of the *customer* (as per the Three Tier Test)
- any third parties for whom the *customer* acts.

86. If the customer is a company, then the *supervised person* would apply the guidance in paragraph 75 above.

87. In the scenario below the Fund is the *supervised person*, the corporate nominee is the *customer* and the individual is the third party for whom the *customer* is acting.

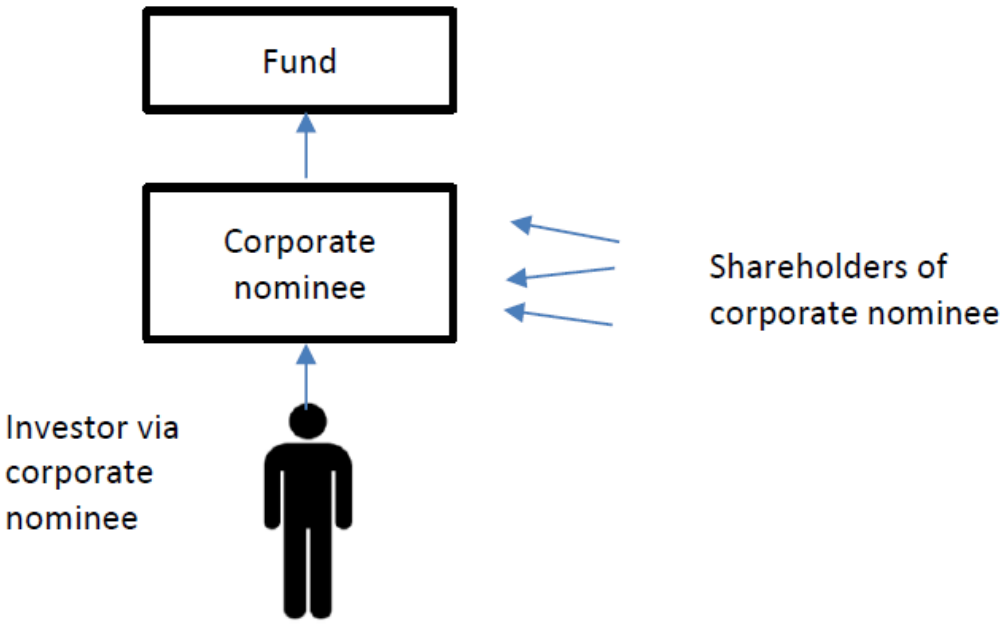
88. The corporate nominee is the *customer* and it will be necessary to identify its *beneficial owners and controllers*. The Three Tier Test will need to be applied to determine the potential *beneficial owner/controllers* of the corporate nominee. In this scenario it will also be necessary to identify

the third party for whom the corporate nominee is acting and determine the *beneficial and ownership and control* of that third party as per Article 3(2)(b) of the *Money Laundering Order*.

Illustrative example of application of the Three Tier Test to

a corporate nominee *(Article 3(2)(c))*		
No	Control through ownership	There are a number of owners and there in no majority shareholder
No	Control through other means	There are no entities/persons that fall into this tier
Yes	Control through positions held	The board of directors control the corporate nominee

an individual whose interest is through the corporate nominee *(Article 3(2)(b))*		
Yes	Control through ownership	Here the principal is an individual
No	Control through other means	Tier 1 applies so no further need to determine potential persons in other tiers
No	Control through positions held	



89. The *supervised person* is required to identify and verify its *customer* – here the corporate nominee – as set out at paragraph 75. Control and ownership of the *customer* must be ascertained applying the Three Tier Test (paragraph 88 above).

90. The third party for whom the *customer* is acting must also be identified and verified. In the diagram above this will be the individual who is investing via the nominee. If the third party in the example above was not an individual then its *beneficial owners and controllers* would also need to be identified and verified.

13.3.8 Fund operators – Residual assets

Funds

Guidance notes

91. On some occasions when a Fund is wound up the Fund Operator may hold residual and/or illiquid assets of the Fund for the benefit of the investors. In this scenario care has to be taken and the following matters should be considered:

    › have the investors now become the Fund Operator's *customers*?

    › does the Fund Operator hold sufficient *CDD* on its *customers*? For example, the Fund Operator may have taken comfort from the *identification measures* applied **by the Fund** but the Fund no longer exists

    › has the Fund Operator updated its *CRA* and *BRA* to take into consideration its new role (regardless of whether the investors are its *customers*)?

13.4 Timing of identification measures

Funds

Overview

92. This section is supplemental to and should be read in conjunction with Sections 4.1 and 4.7 of this Handbook.

93. Article 13(4) of the *Money Laundering Order* provides a concession in relation to the timing of *identification measures*, permitting a delay in obtaining evidence in specific circumstances. However, **in no circumstances** can the obtaining of information be delayed.

Guidance notes

94. Delaying the obtaining of evidence is permitted in certain circumstances but should not be common or standard practice. It **should not** be common practice that verification is deferred until after the first close of a Fund. Where the provisions of Article 13(4) are relied upon to delay the obtaining of evidence of identity, additional measures are required, including the effective management of the associated risk through appropriate authorisation, monitoring and reporting.

95. The obtaining of evidence of identity "as soon as reasonably practicable" should in most cases be a matter of days rather than weeks of months.

13.5 Failure to complete identification measures

Funds

Overview

96. This section is supplemental to and should be read in conjunction with Section 4.8 of this Handbook.

97. Under Article 14 of the *Money Laundering Order*, if a *supervised person* is unable to apply *identification measures* when required to do so then it must terminate that relationship and consider whether to make a *SAR* to the *JFCU*.

98. This requirement may cause conflicts in the case of a *supervised person* that is a Fund where its *customer* is an investor and where:

- the relationship between the Fund and its investor is governed by other legislation or regulatory requirements - e.g. the *CIF(J) Law* and Code of Practice for Certified Funds and
- the termination of a relationship with an investor may have a prejudicial effect on the interests of other investors (e.g. a closed-ended illiquid property fund).

Guidance notes

99. In order to address these potential issues, termination of a business relationship may be **delayed** until such time as compliance with Article 14 of the *Money Laundering Order* does not conflict with another statutory or regulatory requirement, and/or does not have any prejudicial effect on the interests of other *customers* (investors), so long as the risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* is effectively managed.

13.6 Updating identification information

Funds

100. This section is supplemental to and should be read in conjunction with Sections 3.4 and 4.1 of this Handbook.

Guidance notes

101. The *BRA* will enable a *supervised person* to establish procedures to undertake reviews of its *customers* on a risk sensitive basis. In addition to the established pattern of reviews there will be "trigger events" when it may be appropriate to consider whether the identity information and evidence held on a *customer* is relevant and up to date. These should include (in addition to those circumstances set out in Section 3.4 of the *AML/CFT/CPF Handbook*):

    - receipt of significant additional funds to be invested where the delay between contributions is material (including drawdowns)
    - when distributions are being made
    - economic Merger of two Funds which results in the admission of new investors

    The guidance set out at Section 3.5 of this Handbook regarding the taking-on of a new book of business should also be considered, where relevant.

102. It may well be that when a *customer's* information and evidence of identity is reviewed upon a trigger event, it is clear that the information and evidence previously obtained is sufficient and no further updated information is needed. This may be the case when, for example, a regularly scheduled review has recently been undertaken and updated information has been received as a result.

13.7 On-going monitoring: Scrutinising of transactions & activity

Funds

103. This section is supplemental to and should be read in conjunction with Section 6 of this Handbook.

Guidance notes

104. The information about a *customer* obtained at the outset of the relationship as part of *identification measures* should allow a *supervised person* to monitor activity against an expected pattern of activity and transactions. For Funds this will include generic profiles of the expected target investors and the expected target investments. For example, if the Fund's prospectus

indicates that it is going to invest in UK real estate and then invests in oil exploration and extraction businesses, this is not expected activity. Similarly, if the Fund is aiming for investment from European Banks and then receives investment from a Non-Profit Organisation based in Sub-Saharan Africa, this would not be expected activity.

105. It is not sufficient for an administrator/manager who has been delegated the responsibility for monitoring the Fund to simply facilitate the transaction - they are also required to monitor each transaction to determine whether it is inconsistent, unusually complex/large, high risk or follows an unusual pattern. If a transaction does not match the expected profile then the rationale for the transaction should be obtained and documented.

106. Expected activity may change over time if the target market or target investments change. This may also impact on the Fund's *BRA* and *CRAs* which may need to be updated.

13.8 Collation of CDD

Funds

Overview

107. Every Fund and Fund Operator is obliged to comply with the *CDD* requirements placed upon it. However, there may be statutory or contractual provisions operating so that, should one entity in a Fund structure undertake sufficient *CDD*, others in the structure may not need to duplicate certain aspects of *CDD* themselves.

108. The following sections of the *AML/CFT/CPF Handbook* deal with specific provisions regarding scenarios where a *supervised person* may not undertake all of the *CDD* process themselves:

Exemptions from Identification Measures	› Section 7
Reliance on obliged persons	› Section 5
Outsourcing	› Section 2.4.4 › Section 5.1 Paragraphs 12-14

109. Where a *supervised person* **is not** undertaking aspects of *CDD*, including through the application of exemptions, it needs to:

- › document who **is** doing so and on what basis, and
- › ensure that the risks have been properly assessed, considered and documented.

13.8.1 Exemptions from identification measures

Funds

Overview

110. This section is supplemental to and should be read in conjunction with Section 7 of this Handbook.

111. An assessment as to whether exemptions from *identification measures* are appropriate for *customers* and/or in relation to third parties must be conducted and documented. When doing so the statutory prohibitions, stating where exemptions cannot be applied, must be carefully considered in each case:

Circumstances in which exemptions under Part 3A do not apply *(Article 17A)*	
Exemptions under Articles 17 B-D	**Exemptions under Article 18**

› the *supervised person* suspects *money laundering*	› the *supervised person* suspects *money laundering*
› the *supervised person* considers that there is a higher risk of *money laundering*, including the risk of *money laundering* if fail to apply appropriate identification measures or keep records.	› the *supervised person* considers that there is a higher risk of *money laundering*
› the *customer* is resident in a country that is not compliant with the *FATF recommendations*	› the *customer* is resident in a country that is not compliant with the *FATF recommendations*
› the *customer* is a person in respect of whom Article 15(1)(c) applies [specified persons having a *relevant connection* to country/territory in relation to which *FATF* has called for enhanced customer due diligence]	› the *customer* is a person in respect of whom Article 15(1)(c) applies [specified persons having a *relevant connection* to country/territory in relation to which *FATF* has called for enhanced customer due diligence]
› the *customer* is a person in respect of whom Article 15B(1) applies [certain deposit taking businesses with a banking or similar relationship with an institution whose address for that purpose is outside Jersey]	

112. Exemptions from *identification measures* may only be applied in appropriate circumstances. Where specified, this will require an assessment of the risk of applying the exemption, in addition to a *CRA*.

Guidance notes

Funds

113. As noted at Section 7.13 of this Handbook, Articles 18 and 17B-D of the *Money Laundering Order* can be applied to the same *customer* relationship, as they apply to separate identification requirements.

114. Refer to the table set out at Section 7.13 for detail on which aspects of *CDD* must always be undertaken by the *supervised person*.

115. Article 18 applies only to the *customer* and does not extend to third parties. From a Fund Operator's perspective this means, for example, that Article 18 only applies to the general partner or the trustee and not to the limited partnerships or unit trust. Articles 17B-D **do apply** to third parties which would encompass the investors in a limited partnership or a unit trust.

116. Article 18(4)(b) refers to a *customer* that is a body corporate or limited liability company whose securities are listed on an *IOSCO* compliant exchange or on a *regulated market*. As part of the assessment whether simplified due diligence may be applied, the *supervised person* should consider whether the exchange on which the securities are listed is an *IOSCO* compliant exchange or a *regulated market*. The fact that the exchange is listed in a product guide (e.g. listed fund guide) or in an Order (e.g. the *Unregulated Funds Order*) does not necessarily mean it qualifies. Further guidance is provided on this point in Section 7.16.3 of the *AML/CFT/CPF Handbook*.

13.8.2 Reliance on obliged persons

Funds

117. This section is supplemental to and should be read in conjunction with Section 5 of this Handbook.

Guidance notes

118. Care should be taken when placing reliance on an administrator. An administrator may be acting in two capacities when undertaking *CDD*; (i) for itself as Fund Operator and (ii) as a delegate on behalf of the Fund. In such a case, a *supervised person* seeking to rely on *CDD* undertaken by the administrator needs to be clear whether it is the administrator or the Fund that is the *obliged person*.

119. Set out below are some key questions for a *supervised person* to ask themselves:

- what *identification measures* do you need to apply?
- who are you intending to rely upon?
- what identification information and evidence has the *obliged person* obtained?
- does the information and evidence obtained by the *obliged person* being relied upon match your requirements?

120. Each Fund Operator will have its own risk appetite and its own *CRA* of the Fund and the risk ratings allocated by different Fund Operators may not be the same. Where a Fund Operator assesses the Fund as higher risk it may be insufficient to rely on information and evidence obtained by a Fund Operator rating the Fund as lower risk and additional information is likely to be required.

121. Importantly, chains of reliance are not permitted. A *supervised person* cannot rely on an *obliged person* who is in turn relying on someone else.

122. Reliance may be used where the Fund structure has higher *AML/CFT/CPF* risks or the Fund structure and Fund Operators are unregulated (where the Fund Operator cannot apply exemptions from *identification measures*).

123. There are aspects of *CDD* that, in the absence of other provisions, the *supervised person* is required to undertake itself. These are set out in the table at Section 5.1 of this Handbook.

13.8.3 Obtaining copy documentation from a supervised Trust and company service provider in the Crown Dependencies

Funds

Overview

124. This section is supplemental to and should be read in conjunction with Sections 4.4.5 and 4.5.7 of this Handbook.

125. In certain circumstances, it may be appropriate to obtain information from a trust and company service provider that is regulated by the *JFSC*, the Guernsey Financial Services Commission or the Isle of Man Financial Services Authority in order to identify certain individuals.

126. It should be noted that such practice is restricted to a very narrow set of circumstances (e.g. only certain individuals and only certain documents) and is dependent on a number of conditions being met (e.g. a specific risk assessment is carried out and specific confirmations are obtained from the trust and company service provider).

13.8.4 Outsourcing

Funds

Overview

127. This section is supplemental to and should be read in conjunction with Section 2.4.4 and Section 5 (paragraph 14) of this Handbook, along with the *JFSC's* Outsourcing Policy and guidance note.

128. Contractual arrangements may be put in place where another entity undertakes *CDD* for the *supervised person* as a delegate. This is likely to be the case where an administrator and/or manager is appointed to the Fund or where the governing body of the Fund such as a trustee or general partner is a managed entity and reliant on a manager of a managed entity. The *supervised person* always remains responsible for fulfilling its statutory obligations regardless of the activities it outsources to delegates.

129. Procedures and processes must be put in place so that the delegating party retains oversight of the outsourced activities. The *supervised person* needs to be provided with sufficient information by the delegate in order to adequately review and monitor the outsourced activities.

Guidance notes

130. Outsourcing of specific functions to a Fund Operator may form part of the Fund Operator's service level agreement with the Fund. The *supervised person* would be expected to ensure that the terms are adequate to ensure a clear understanding of what activity the delegate is undertaking.

131. Given that the delegate carrying out the outsourced function is likely to have its own *CDD* obligations it will be important to distinguish between measures applied on behalf of the delegating party and measures applied for itself. This will ensure the respective (and potentially differing) obligations are met and will assist if the delegating party moves to another Fund Operator and wishes to take its information/documentation/records with it.

132. Section 2.4.4 provides a table of activities which may be outsourced but also states that *CDD* is always the responsibility of the *supervised person*.

133. Where *CDD* functions are outsourced, consideration will need to be given to the contractual arrangements between the Fund and its investors (*customers*), the Fund and its Fund Operators and any other entities. Below are some important matters to consider (this list is not exhaustive):

- which party has "ownership" of the investor information
- permissions required from the investor for obtaining, holding and using the information for other purposes (data protection)
- the nature and scope of the obligations outsourced and provisions for monitoring, updating, retention and termination.

134. Where a Fund Operator assesses the *AML/CFT/CPF* risk regarding a Fund to be higher or the Fund/Fund Operators are not regulated, the application of exemptions from *identification measures* is prohibited. Therefore, a Fund Operator providing services to a Fund where it has no direct relationship with the investors may need to apply *identification measures* to the investors. This may be in relation to the control of the Fund or its *source of funds*. Rather than gathering this information themselves they will instead seek access to this information which will normally already have been provided to the Fund by investors via subscription agreements/investor questionnaires.

135. Note that specific provisions may be necessary in subscription agreements / investor questionnaires to enable the Fund to pass on information and evidence that it obtains to meet its

own *AML/CFT/CPF* obligations, in order to assist Fund Operators (present and future) involved in the Fund/Fund Structure to meet their own *AML/CFT/CPF* obligations (subject to any data protection requirements).

13.9 Enhanced due diligence measures – Non-Jersey investors

Funds

Overview

136. This section is supplemental to and should be read in conjunction with Sections 7, 7.4 and 7.7 of this Handbook.

137. Funds with overseas investors will need to undertake **enhanced due diligence** on those investors (see Article 15 of the *Money Laundering Order*) as the investors will normally be:

- non-resident *customers* and/or
- not physically present for identification purposes.

138. Enhanced due diligence measures must be applied to address the risk associated with these types of *customer*. Sections 7.4 and 7.7 of the *AML/CFT/CPF Handbook* provide guidance on the same.

Guidance notes

139. A requirement to apply enhanced due diligence does not automatically mean that the *customer* is higher risk. Some enhanced measures are required regardless of risk.

140. It may be possible for investor profiles/subscription agreements to address enhanced due diligence requirements by obtaining additional information if the investor meets certain criteria. For example a question might read “Are you Jersey Resident? If the answer is no, provide the following additional information…”

141. On some occasions the rationale for a non-Jersey investor looking to invest in Jersey may be determined without necessarily needing to ask the *customer* (e.g. it may be obvious if, say, the Fund is a Jersey Fund).

14 ESTATE AGENTS AND HIGH VALUE DEALERS

14.1 Definition of estate agents and high value dealers undertaking Supervised Business

14.1.1 Estate agents

Overview

1. Paragraph 3 of Part B of Schedule 2 to the *Proceeds of Crime Law* defines the relevant transactions and activity of estate agents for the purposes of complying with *AML* requirements in the *Money Laundering Order* as:

    - the business of providing estate agency services for or on behalf of third parties concerning the buying or selling of freehold (including flying freehold) or leasehold property (including commercial and agricultural property), whether the property is situated in Jersey or overseas
    - the business of providing estate agency service for or on behalf of third parties concerning the buying or selling of shares the ownership of which entitles the owner to occupy immovable property, whether the property is situated in Jersey or overseas.

2. International standards require estate agents, when they are involved in transactions for their *customers* concerning the buying and selling of real estate, to be subject to *AML/CFT/CPF* requirements. Consequently, unlike dealers in high value goods, estate agents are automatically included within the scope of the Money Laundering Order, regardless of whether they accept cash. This is irrespective of the fact that a lawyer or advocate is always involved in a property transaction and no capital movements are overseen by estate agents.

3. The main activities conducted by Jersey estate agents concern local and overseas property transactions, and lettings. Jersey has adopted the definition of real estate agents within the *FATF Recommendations*, which covers both local and overseas property transactions, but excludes activities conducted as letting agents.

4. Guidance provided by the Association of Residential Letting Agents provides the following two exceptions:

    - where a letting agent creates a lease/tenancy "which by reason of the level of the rent, the length of the term, or both, has a capital value which may be lawfully realised in the open market" then this transaction **does fall** within the scope of the *Money Laundering Order*. The reason given is that the lease can be reconverted into money. This would almost certainly include situations where a Premium Lease or tenancy agreement at a high value rent is created
    - it is not uncommon for letting agents to become involved in negotiating / arranging / facilitating the purchase of a property by an existing tenant from the landlord *customer*. At that point, the letting agent becomes involved in estate agency work.

14.1.2 High value dealers

Overview

5. Paragraph 4 of Part B of Schedule 2 to the Proceeds of Crime Law defines high value dealers, for the purposes of complying with the requirements in the Money Laundering Order, as being:

    - persons who, by way of business, trade in goods and receive, in respect of any transaction (whether executed in a single operation, or in several operations which appear to be linked), payment or payments in cash or virtual currency of at least €15,000 in total.
    - payment refers to payment in, or by means of **Cash** or **Virtual currency**
    - "Cash" includes, but is not limited to any of the following, in any currency – notes, coins, travellers' cheques, bearer negotiable instruments
    - "virtual currency" means any currency which (whilst not itself being issued by, or legal tender in, any jurisdiction):
        - digitally represents value
        - is a unit of account
        - functions as a medium of exchange
        - is capable of being digitally exchanged for money in any form.

6. The €15,000 threshold in the Proceeds of Crime Law is derived from the FATF Recommendations. See the FATF interpretive note on Recommendations 22 and 23.

7. In respect of high value dealers the requirements also apply to all dealers in high value goods who wish to be able to accept payment in cash of €15,000 or more for one or more transactions, whether executed in a single operation or in several operations which appear to be linked.

    Case study: Group money laundering

    A group of criminals held £50,000 in cash obtained from drug trafficking operations. In order to launder their proceeds of crime, they targeted a high street jewellery business which held a high value dealer licence. Over the course of a few days, each person in the group repeatedly visited the jewellery shop to purchase items. Whilst no one person spent more than €15,000 in any one transaction, together they laundered the full £50,000 into jewellery, which could then be enjoyed or re-sold for a profit.

    The staff who processed these transactions did not identify that the persons were operating together and therefore did not consider the total amount spent by the group. Nor did they realise that the transactions, whilst spread over multiple days, were linked to each other. As a result, they did not identify that the linked transactions carried out by this group exceeded €15,000.

    Had the business had more effective controls in place in line with the Handbook, they would have applied *CDD* measures to the group of money-launderers and may have formed a suspicion that money laundering was taking place.

The business in this example appears to be involved in *money laundering* and may be found guilty of the offence of dealing with criminal property. The business also appears to have failed to have had adequate procedures to prevent and detect *money laundering* in line with the *Money Laundering Order*. As such, they may be found guilty of an offence of contravening or failing to comply with a requirement contained in any Order made under Article 37 of the *Proceeds of Crime Law*. In addition, the business may be found to have contravened *AML/CFT/CPF Codes of Practice* within this Handbook and therefore may be subject to proceedings by the *JFSC*.

Guidance Notes

8. It is important to note that the requirement to register as a high value dealer for the purposes of the *Money Laundering Order* includes businesses that only occasionally accept such payments.

9. Businesses registered as high value dealers need to apply the requirements of the *Money Laundering Order* to their transactions and activities on a risk-based approach. However, as part of demonstrating good practice, high value dealers may wish to consider applying *CDD* measures to any transactions and activity that will be paid in cash or virtual currency with a value of £1,500 or more.

10. Any business that accepts cash or virtual currency over the €15,000 threshold for relevant transactions is required to register as a high value dealer. This means that any business that accepts payments in cash or virtual currency of any amount needs to be aware of the threshold. Some businesses may decide that they will simply not accept payments over the threshold amount. The fact remains, however, that businesses are vulnerable to money launderers as highlighted in the case studies above and below. Businesses that have decided not to register as high value dealers might support their decision by:

› A clearly documented policy known to all staff who accept payment that any significant cash or virtual currency payments will be refused with payments only being accepted by other means (for example, by debit or credit card, or by bank transfer)

› A reasonable threshold, appropriate to the business, below the €15,000 maximum for which payments in cash or virtual currency will be considered as significant, and refused

› It is the JFSC's expectation that this threshold for significant transactions would be approximately £1,500 or another amount that the business is able to clearly justify in its own circumstances.

11. Although the high value dealer population is varied, it mainly consists of retailers and wholesalers of goods who accept cash payments of €15,000 or more. Some common examples of goods sold by high value dealers include:

    - jewellery
    - art and antiques
    - precious metals
    - cars and yachts
    - agricultural goods.

    Other examples of high value dealers include:

    - retailers selling high-end electronics like tablets and smartphones
    - businesses selling alcohol and tobacco
    - wholesale/cash and carry businesses

- businesses which supply tools and equipment to tradespersons, such as plumbers and electricians.

Case study: Less common goods sold by high value dealers

A couple involved in the distribution and sale of illegal substances attempted to launder £20,000 worth of proceeds from their illegal activities. They were handling bundles of Jersey £20 notes whilst trying to:

1. convert the cash into English notes
2. deposit the cash into UK bank accounts
3. purchase goods to be re-sold at a later date.

The couple initially approached local banks. The banks followed their internal policies on handling cash and refused to accept a cash deposit due to the amount and unexplained/undocumented source. Similarly, the couple approached a local car dealership. The dealership was not registered as a high value dealer as its policy did not allow acceptance of significant cash payments. They refused to sell vehicles for cash. The couple then decided to approach a smaller retailer stocking a wide range of electronics. They subsequently purchased a number of expensive laptops, computers and smartphones.

Despite the bill totalling over £20,000, the staff processing the transaction did not become suspicious and did not query the origin of the cash. It was later identified that the retailer did not have policies on accepting significant cash payments. Therefore their staff were unaware of the cash value threshold set out in the Proceeds of Crime Law.

The business was willing to accept transactions that fall within the high value dealer definition in the *Proceeds of Crime Law*. As such the electronics retailer should have been registered as a High Value Dealer. If they had been registered, they should have had appropriate systems and controls in place to identify the suspicious nature of the transaction. Had they been registered and had the relevant controls in place, the apparent money laundering above should have been identified. For example, the business would have applied *CDD* measures to the couple and may have formed a suspicion that money laundering was taking place.

The business in this example appears to be involved in *money laundering* and may be found guilty of the offence of dealing with criminal property. The business also appears to be an unregistered high value dealer and may be found guilty of the offence of carrying on unauthorised *specified Schedule 2 business*. In addition, while they were not registered as a high value dealer, it appears that the business should have been registered with the *JFSC* so may be found to have contravened *AML/CFT/CPF Codes of Practice* within this Handbook and therefore may be subject to proceedings by the *JFSC*.

12. Cash includes, for example, notes, coins, traveller's cheques and bearer negotiable instruments. It does not include cheques or bankers drafts. As noted above the €15,000 threshold may be reached in respect of a single transaction or there may be several linked transactions that together total €15,000 or more.
13. Each business should assess, within its specific circumstances, which transactions it will consider to be linked for the purposes of preventing and detecting crime.
14. Transactions may be linked in the following scenarios (note this list is not exhaustive):

- they are executed by the same individual or group of individuals (including third parties connected with those persons)

- they involve the same asset
- they occur across a specified time period, e.g. a high value item worth €15,000 or more is initially secured with a deposit, then the total value is paid in instalments over time
- they appear designed to achieve an overarching objective (e.g. launder large sums of money)
- they do not have a commercial rationale (e.g. appear to be deliberately structured to avoid the €15,000 threshold).

15. It is important to note that whilst some transactions may appear to be linked from the outset, in other cases this may only become apparent at a later stage.
16. Each business should carefully assess and document the risks specific to its activities, traded goods, customer profiles and payment patterns.
17. Unusual sales or purchase activities may include:
    - delivery methods or payment arrangements that are not consistent with normal practice
    - a new customer with little or no trading history and no trade references
    - a customer travelling to Jersey just to purchase goods, when the goods are readily available near their home location
    - a customer or representative making multiple smaller cash deposits into the business' bank account
    - unusual enquiries regarding the business' refund policy, e.g. customer asking if a refund can be made by cheque, wire transfer or paid to a third party.

14.2 Identification measures: Finding out identity and obtaining evidence

Estate Agents and High Value Dealers

14.2.1 Obligation to find out identity and obtain evidence

Overview

18. This sector-specific section is supplementary to and should be read in conjunction with Section 4.2 of this Handbook.

AML/CFT/CPF Codes of Practice

Estate Agents

19. Following *FATF Recommendation* 22, a *supervised person* that provides *estate agency services* as defined in Paragraph 3 of Part B of Schedule 2 to the *Proceeds of Crime Law*, must comply with *CDD* obligations with respect to both purchasers **and** vendors of the property.

14.2.2 Timing of identification measures

Estate Agents and High Value Dealers

Overview

20. This section is supplementary to and should be read in conjunction with Section 4.7 of this Handbook.

21. As noted in Section 4.7, Article 13(4) of the *Money Laundering Order* allows, in certain circumstances, a *supervised person* a reasonable timeframe to undertake the necessary enquiries for obtaining evidence of identity after the initial establishment of a *business relationship*. No similar concession is available for finding out identity. Where a reasonable excuse for the continued delay in obtaining evidence of identity cannot be provided, in order to comply with Article 14(2) of the *Money Laundering Order*, a *supervised person* must terminate the relationship (see Section 4.8).

AML/CFT/CPF Codes of Practice

Estate Agents and High Value Dealers

22. A *supervised* person must not permit final agreements to be signed or pay away funds to an external party (or to another account in the name of the *customer*), other than to deposit the funds on behalf of the *customer*, until such time as evidence of identity has been obtained.

14.2.3 Timing for 'existing customers'

Estate Agents and High Value Dealers

Overview

23. This section is supplementary to and should be read in conjunction with Section 4.7.2 of this Handbook.

24. As noted in Section 4.7.2, *FATF Recommendation* 10 states that "financial institutions" should be required to apply that *Recommendation* (which deals with *CDD* measures) to "existing customers" on the basis of materiality and risk, and should conduct *CDD* measures on such existing relationships at appropriate times.

25. For the purposes of the *Money Laundering Order*, an existing customer means a *business relationship* established before the *Money Laundering Order* came into force for estate agents and high value dealers on **1 May 2008** and which continues.

26. For the avoidance of doubt, the *identification measures* (finding out identity and obtaining evidence) to be applied to existing customers include the collection of information that is necessary to assess the risk that a *business relationship* involves *money laundering* or the *financing of terrorism* (in line with Article 3(5) of the *Money Laundering Order*). This is likely to be self-evident for an existing customer on the basis that a relationship will have been established on, or before, **30 April 2008**.

27. Except with the agreement of the *JFSC* (in relation to an application from the *supervised* person made on or before 31 December 2014), the effect of Article 13(3A) of the *Money Laundering Order* is to require the identity of a *customer* to have been found out by 31 December 2014. There is no similar deadline for obtaining evidence of identity.

28. Once an existing relationship has been "remediated", then Article 13(1)(c)(ii) of the *Money Laundering Order* will apply to such a relationship in the same way as a relationship established on or after **1 May 2008** (on the basis that documents, data or information will have been obtained under the *CDD* measures prescribed in Article 3).

14.3 Exemptions from *CDD* measures – Jersey property transactions

Estate Agents

Overview

29. This section is supplemental to and should be read in conjunction with Section 7.16 of the *AML/CFT/CPF Handbook*.

30. This section relates to the exemption available under Article 18(6) of the *Money Laundering Order*, which provides that a *supervised person* that is a lawyer or an estate agent, which enters into a *business relationship* or carries out a *one-off transaction* for the purpose of enabling a *customer*, directly or indirectly, to enter into a registered contract within the meaning of the Control of Housing and Work (Jersey) Law 2012 (i.e. where it is to be passed before the Royal Court and registered in the Public Registry of Contracts), need not obtain **evidence of identity** of its *customer*.

AML/CFT/CPF Codes of Practice

Estate Agents

31. A *supervised person* that is an estate agent must obtain and retain documentation establishing that its *customer* is entitled to benefit from the exemption set out in Article 18(6) of the *Money Laundering Order*.

14.4 Business risk assessment

Estate Agents and High Value dealers

14.4.1 Service area vulnerabilities and warning signs – Estate agents

Overview

32. Criminal conduct generates huge amounts of illicit capital and these criminal proceeds need to be integrated into personal lifestyles and business operations. Law enforcement agencies advise that property purchases are one of the most frequently identified methods of *money laundering*. Property can be used either as a vehicle for *money laundering* or as a means of investing laundered funds.

33. Criminals will buy property both for their own use, e.g. as principal residencies or second homes, business or warehouse premises, and as investment vehicles to provide additional income. The Serious Organised Crime Agency in the UK has advised that real property arises in over 85% of all confiscation cases and at least 25% of those investigated hold five or more properties both residential and commercial.

34. The business risk assessment relating to *customers* and services will depend on the *supervised person's* size, type of *customers* and the business area it engages in.

35. *Supervised persons* carrying on Estate Agency business should consider the different types of *money laundering, financing of terrorism,* and *financing of proliferation* risks to which they are exposed when providing services. This service area risk assessment must also be reflected when undertaking a *customer* risk assessment.

36. Further factors to consider when evaluating the risks posed by clients and service areas are set out in Section 3.3.4 of this Handbook.

14.4.2 Criminal use of conveyancing services Estate Agents

Guidance notes

37. The estate agent is but one of the professionals who will be involved in a property transaction. Every property transaction requires a legal practitioner to undertake the conveyancing and this is one of the criminal's most frequently utilised functions. Conveyancing is a comparatively easy and efficient method of laundering money with relatively large amounts of criminal monies cleaned in one transaction. In a stable or rising property market, the *money launderer* will incur no financial loss except fees. Whilst many legal practitioners will be unwitting accomplices, some corrupt legal practitioners will provide deliberate assistance and estate agents should be vigilant for any signs that this is occurring.

38. The purchase of real estate is commonly used as part of the last stage of *money laundering*. Such a purchase offers the criminal an investment which gives the appearance of financial stability. The purchase of a restaurant or hotel, for example, offers particular advantages, as it is often a cash-intensive business, which is the preferred currency of criminals. Cash remains the mainstay of much serious organised criminal activity. It has the obvious advantage that it leaves no audit trail and is the most reliable form of payment, as well as the most flexible. Retail businesses also provide a good front for criminal funds where legitimate earnings can be mixed with the proceeds of crime.

39. Case Study 1 – Drug Trafficking funds a hotel purchase:

    - a financial intelligence unit received information that a previously convicted drug trafficker had made several investments in real estate and was planning to buy a hotel. An assessment of their financial situation did not reveal any legal source of income, and they were subsequently arrested and charged with an offence of *money laundering*. Further investigation substantiated the charge that part of the invested funds were proceeds of their own drug trafficking. They were charged with substantive drug trafficking, *money laundering* and other offences.
    - the criminal's lawyer received the equivalent of approximately US$70,000 cash from their *customer*, placed this money in their *customer's* bank account and later made payments and investments on the *customer's* instructions. They were charged with *money laundering* in relation to these transactions.
    - the drug trafficker was convicted of drug trafficking, sentenced to seven-and-a-half year's imprisonment, and a confiscation order was made for US$450,000. The lawyer was convicted and sentenced to 10 months imprisonment.

40. Case Study 2 – Tobacco smuggling funds a property empire:

- in June 2005 the Northern Ireland Assets Recovery Agency was granted an Interim Receiving Order at the Belfast High Court for assets valued at an estimated £1.4 million.
- the assets in question were held by Stephen Baxter and his wife Denise. In its application to the High Court, the Agency evidenced that Mr Baxter purported to trade as an ice cream salesman with two vans. However, no street trading licence had ever been granted making the vans recoverable property. The Agency also showed that on a number of occasions police had detected Mr Baxter selling smuggled tobacco from his vans. His lifestyle and property acquisitions appeared to be far in excess of his lawful means.
- the assets included:
    - a principal residence in Belfast

- two apartments in Belfast city centre
- an interest in a further eight building developments
- a planned apartment in a prestige Belfast development.

› the Agency advised that they had intervened to prevent Mr Baxter from extending his property portfolio shortly before the hearing.

› the total value of the property subject to the restraint order was estimated to be £1.4 million.

14.4.3 Recognising suspicious behaviour and unusual instructions

Estate Agents

Overview

41. The following are examples of potentially suspicious events, both prior to and during the life of the property transaction.

14.4.3.1 Absence of normal commercial rationale

Guidance notes

Estate Agents

42. Activity that does not appear to make good business sense may indicate that it is linked to criminal activity. For example, where the prospective purchaser is willing to pay significantly over the market value for a property, particularly where the purchase is being undertaken by a cash-rich company.

43. A property sale or purchase that is subject to any significant last minute changes may indicate that there is an attempt to confuse the *CDD* information.

44. A *customer* that has no apparent reason for using a *supervised person* (for example the location of the property or type of business) where another business would be better placed to act, may indicate that the *customer* is trying to make it harder for *CDD* measures to be completed. Alternatively the *customer* may hope that if the transaction is outside the normal size that a *supervised person* handles, or if it is particularly lucrative, the *supervised person* may turn a blind eye to any unusual or suspicious activity.

45. Where a *customer* has declined services that a *supervised person* would normally expect them to use, or shows little interest in the transaction, this may indicate that the property deal is a sham and merely being used to confuse the audit trail for criminal money (i.e. part of the "layering" stage of the *money laundering* process).

14.4.3.2 Ownership issues

Guidance notes

Estate Agents

46. Properties owned by nominee companies or those with complex structures may be used as *money laundering* vehicles to disguise the true owner and/or confuse the audit trail. Last minute changes of instructions concerning the identity of the prospective purchaser in whose name the property is to be registered should give rise to additional due diligence.

47. Changes in the *beneficial ownership* of a company owning and managing a property where the new beneficial owners' *source of funds* for the company purchase is unclear or dubious may indicate that criminal funds have been injected into the company. This risk is heightened if known, reputable lawyers have not been appointed by either or both sides to act for them.

14.4.3.3 Property Values

Guidance notes

Estate Agents

48. A significant discrepancy between the sale price and what would be considered to be normal for such a property may indicate fraud or *money laundering*.

49. Properties sold below the market value to an associate may have the objective of obscuring the title to the property while the original owner still maintains the *beneficial ownership*.

14.4.3.4 Valuations and surveys

Estate Agents

Guidance notes

50. When estate agents provide a valuation service prior to being instructed as selling agents, or when they are providing a service as surveyors, it is important that they are vigilant. If there is any indication that the property is being used for criminal conduct, a *SAR* must be submitted to the *MLRO*. A roomful of randomly stacked high value goods or a greenhouse inexplicably filled with cannabis cannot be ignored.

51. Case Study 3 – A lucrative faming enterprise:

    › in September 2006, a Cannabis Farm was discovered by Dyfed Powys Police. Officers found a large and sophisticated infrastructure for growing cannabis which could have produced close to £2.5 million pounds worth of cannabis over the previous four years. The owner, who was convicted of producing cannabis with intent to supply, was imprisoned for three years and had £375,000 of his assets confiscated.

14.4.3.5 Funding issues

Estate Agents

Guidance notes

52. Whilst lawyers and advocates will normally handle the funds provided for a property purchase, or the sale proceeds, estate agents will often become aware of the funding arrangements. Suspicions should not be ignored merely because a lawyer is also involved and the sale or purchase funds are not passing through the estate agent's client account.

53. For example, a *customer* who advises that the funds from the sale will be going overseas and paid to an unrelated third party may indicate that the funds are being laundered on behalf of that third party. Similarly, where the *source of funds* for a purchase is obscure or appears to be unusual, this may indicate laundering of criminal funds, particularly if the funds are offered in cash or are coming in from an overseas bank account that is unconnected to the purchaser.

54. A cash deposit paid to an estate agent as part of a large property transaction, which is also to be settled in cash, may indicate tax evasion or that criminal proceeds are being used to fund the transaction. Cash is the principal currency of criminals and should always be subject to further enquiries.

55. Situations where a potential purchaser requests the estate agent to hold the potential purchase funds in their client account must be treated with extreme caution. Because large amounts of cash cannot normally be banked without suspicions being raised, criminals will use other professionals as 'gatekeepers'. Placing cash into the banking system through client accounts of professional firms is a classic *money laundering* technique. Where a *customer* withdraws from a transaction after paying money into a client account, the *customer* receives a cheque or electronic transfer from the lawyer or estate agent which makes the funds appear to be legitimate.

56. Estate Agents should be mindful that as lawyers tighten up on the circumstances in which they will hold *customer* money, other targets will be sought by criminals.

14.4.3.6 **Mortgage fraud**

Guidance notes

Estate Agents

57. Where prospective property purchasers overstate or misrepresent their income in an attempt to mislead mortgage lenders, this falls within the definition of mortgage fraud. Alternatively, the value of the property may be inflated with a view to obtaining a mortgage for the full inflated value. Estate agents must avoid becoming complicit in such criminal arrangements. Mortgage fraud is itself a criminal offence, but if the estate agent becomes involved they are also entering into an arrangement to further a criminal act.

58. Unexplained changes in ownership may indicate a form of *money laundering* known as "flipping", which involves a property purchase, often using someone else's identity. The property is then quickly sold for a much higher price to the same buyer using another identity. The proceeds of crime are mixed with mortgage funds for the purchase. This process may be repeated several times.

59. Fraudulent borrowers will often seek to build a portfolio of properties by obtaining many mortgages with several lenders, using fictitious and/or real names. The portfolio is then used for various purposes such as:

    - organised letting (particularly using assisted housing schemes)
    - property development of a site or individual properties
    - 'rollover', where the criminal sells the properties to themselves (in various guises) at inflated prices.

60. Collusive mortgage fraud has become a significant problem in many countries with estate agents, property valuers and legal professionals acting in concert to provide all concerned with maximum benefit.

61. Case Study 4 – Operation Trooper

› A ring of 43 professionals, including several fraudulent valuers, was broken as a result of the largest mortgage fraud investigation ever undertaken in the UK. The fraudsters bought over 200 properties, falsely inflated their values and sold them amongst themselves, fraudulently obtaining mortgages from most of the large lenders. No repayments were ever made on any of the mortgages which totalled £35 million.

14.4.3.7 **Buy to let**

Guidance notes

Estate Agents

62. Buy to let properties are particularly vulnerable to *money laundering* and especially so when linked to self-certification of income by the purchaser. Terrorist organisations may also purchase multi-tenanted property to provide safe haven accommodation for the operatives within their cells. The receipt of rent payments in cash also increases the vulnerabilities of letting agents.

63. To safeguard the position of letting agents who deal with buy to let properties or wish to receive payments of rent in cash, the Association of Residential Letting Agents has recommended that they voluntarily adopt the *AML/CFT/CPF systems and controls* (including *policies and procedures*) that are applicable to estate agents.

64. Case Study 5 – Operation Verge:

› in February 2004, following an investigation by the National Crime Squad and HMRC in the UK, four people were arrested for importing cannabis resin concealed in machines from Spain. One of the defendants offered to plead guilty if no confiscation order was brought against him. The investigation, which spanned several jurisdictions in Europe, had uncovered a property portfolio the defendant wanted to protect. The defendant had purchased several new apartments in various developments to launder the money and rent out the properties. A confiscation order was raised against the defendant amounting to around £2.7m.

14.4.4 Service area vulnerabilities and warning signs – High Value Dealers

Overview

65. The business risk assessment relating to *customers* and services will depend on the *supervised person's* size, type of *customers* and the business area it engages in.

66. *Supervised persons* carrying on the business of a High Value Dealer should consider the different types of *money laundering, financing of terrorism,* and *financing of proliferation* risks to which they are exposed when providing services. This service area risk assessment must also be reflected when undertaking a *customer* risk assessment.

67. Further factors to consider when evaluating the risks posed by clients and service areas are set out in Section 3.3.4 of this Handbook.

14.4.5 Recognising suspicious behaviour and unusual transactions – High Value Dealers

Overview

68. Cash remains the mainstay of much serious organised criminal activity. It has the obvious advantage that it leaves no audit trail and is the most reliable form of payment, as well as the most flexible.

69. As illustrated in the following case study, the €500 note has become the bank note of choice for criminals, replacing the $100 note. Consequently, High Value Dealers should always exercise additional vigilance when accepting a large number of €500 notes from any one *customer*.

70. Case Study 6 – Disappearing €500 Notes:

    › in 2005 the Bank of Spain advised that €500 notes were increasingly being drawn from high street banks and then disappearing. In March 2006, 100 million more notes were issued to Spanish high street banks than were handed in by them. This was of significant concern because at that point Spain used 26% of all €500 notes that were issued within the Eurozone.

    › in response to the Bank of Spain's concern, an investigation was launched by the Spanish Government into the missing notes. The result was that the Spanish Treasury identified 13,500 suspicious transactions totalling €6 billion that had taken place between 2003 and 2006 using €500 notes.

    › by way of example, the deputy mayor of Marbella was found to have €378,000 in €500 notes in their safe when they were arrested by police in April 2006 during the investigation of eastern European crime groups operating on the Costa del Sol.

71. Those in receipt of large sums of cash have the problem of how to dispose of it. The objective of the first stage of *money laundering* – placement – is to move the criminal cash into the financial system. It is extremely difficult to place large amounts of cash into the banking system without raising suspicions. Serious organised criminals frequently launder cash through legitimate and quasi legitimate businesses, typically those with a high cash turnover. The businesses are often owned or part–owned by the criminals or by close associates, although legitimate businesses may also be targeted to provide the means for laundering criminal proceeds. Retail businesses that genuinely accumulate and bank large amounts of cash are natural targets for laundering the cash though genuine purchases.

72. Businesses which find themselves in financial difficulties may also be targeted by criminals. Cash may be placed into the financial system by persuading the owners or managers of the business to deposit criminal money along with their normal takings. The business then transfers the criminal money to the *money launderer's* account, taking a cut along the way.

73. Case Study 7 – Disposal and Exchange of Cash:

    › a number of banks in Madrid were visited by the local drug squad.

    › accounts had been opened for companies running cash-based businesses that received cash from *customers* and paid suppliers in cash.

    › the businesses arranged to deliver cash to the banks in small denomination notes, which would then be exchanged for the larger €500 notes. The €500 notes were then either paid into other bank accounts or smuggled out of Spain. No *SARs* had been made by any of the banks concerned.

14.4.5.1 Recognising stolen cash

Guidance notes

High Value Dealers

74. Stolen cash is frequently laundered through retail outlets. Sterling, and many euro banknotes, become stained with dye when cash boxes are stolen and opened during bank or cash-in-transit robberies. Criminals frequently attempt to clean the notes, but this damages the foil and other security features.

14.4.5.2 High value cash transactions

Guidance notes

High Value Dealers

75. *Money launderers* normally want to move funds quickly in order to avoid detection. This is more easily done in large one-off transactions. The purchase of high value goods, with good portability, paid for in cash, represents an attractive target for *money launderers*. Luxury goods paid for with cash that can easily be sold on (even at a loss) for "clean money" are especially attractive.

76. Equally an asset may be purchased to support a certain lifestyle (e.g. a high performance car or a yacht). Alternatively an asset may be purchased as a form of long term investment (e.g. jewellery, an antique, a work of art etc).

77. Case Study 8 – A High Value Lifestyle:

    - In August 2007, a record £2.8 million was seized from two criminal families who made a fortune from car crime and tax evasion.
    - The two families lived a life of luxury, shopping at Harrods and wearing designer clothes and jewellery and driving top of the range cars. However, it was all paid for through crime.
    - The families made their money by dishonest car dealing – turning back the mileages of cars and then selling them on – and by selling stolen caravans. The scam involved forged documents, altered MOT certificates and fake service histories.
    - The gang of eleven, none of whom had legitimate jobs, then made the money disappear by splashing out on luxury cars, designer jewellery, clothes, perfumes, chinaware and other antiques.
    - When the homes of the gang were raided by 350 officers from four UK police forces, almost £1 million in cash, mostly in £50 notes, was found to be buried in the grounds or hidden around the various houses.
    - Members of the gang pleaded guilty to *money laundering*, criminal conspiracy, obtaining money by deception and possessing criminal property.

14.4.5.3 Gold, precious metals, precious stones and jewellery

Guidance notes

High Value Dealers

78. Criminal funds can be used to purchase gold which is then exported to other jurisdictions and sold, thus legitimising the funds as the proceeds of sale. The use of gold is attractive for many reasons – it is the only raw material comparable to money. It is a universally accepted medium of exchange which is traded on world markets and the *money launderer* can remain anonymous.

79. Case Study 9 – Gold moulded into tools:

    › A New York gold refinery owner was found guilty of laundering money for Colombian drug traffickers by selling them gold moulded into tools, screws and other bulk items that could be shipped to Colombia undetected.

80. The jewellery trade can also become involved in *money laundering*. Precious stones and jewellery are easily transportable and highly concentrated forms of wealth.

81. Case Study 10 – Operation Meltdown:

    › Operation Meltdown was a three-year investigation into drug *money laundering* in Manhattan's diamond district. Dealers agreed to trade 220 pounds of gold and diamonds for more than US$1 million in cash. The probe resulted in 23 arrests, including 11 jewellers and the seizure of more than US$1.5 million in cash, US$1.3 million in gold and 118 kilograms of cocaine.

    › One jeweller was charged with agreeing to exchange diamonds and gold for US$600,000 in cash. He was murdered in June 2004 less than one month before his trial.

82. Case Study 11 – Local Jersey Operation

    › Mr A was convicted in December 2020 of *money laundering* in connection with the importation and supply of drugs in Jersey. The wider investigation resulted in the seizure of drugs with a street value of around £900,000.

    › Mr A owned and ran a jewellery business which allowed him to facilitate the movement of criminal property from Jersey to the UK through the purchase and sale of bullion. This enabled cash to be removed from the Island under the cover of legitimate transactions, and without the cash being physically carried out of the jurisdiction.

    › The process was carried out in four steps:

        - A sum of cash, *from the sale of drugs*, would be handed to Mr A at his jewellery shop.
        - Mr A would deposit that cash into his personal and business bank accounts
        - Mr A would use the cash to purchase gold bullion from a dealer based in Hatton Garden in London.
        - The gold would be collected from the London dealer and sold for cash.

    › The cash would then be available to UK-based members of the criminal enterprise to be used to purchase drugs, or otherwise to cover the operating costs of the enterprise.

14.4.5.4 The motor trade

Guidance notes

High Value Dealers

83. Vehicles may be either the source of the laundered money or the means by which other illegal income is laundered. *Money launderers* often make contacts within trades where the use of cash is accepted, such as dealers in expensive cars.

84. Case Study 12 – Using Cars to facilitate *money laundering*:

- The financial intelligence unit of Country R received a *SAR* on large purchases of Country F currency totalling US$263,000 and carried out by a citizen of Country R.
- The funds in Country F currency were used for the purchase of new motor vehicles in Country F. However, the transactions detected appeared to include only part of the funds moved by the individual and their associates.
- Indeed, the organisation to which the individual belonged regularly acquired new motor vehicles in Country R for payments in cash from a large dealership – which was either in collusion with the organisation or turning a blind eye to the activity.
- The purchased vehicles (worth around US$30,900 each in the verified cases) were delivered and then driven to a neighbouring country where they were received by a close relative of the main individual in the scheme and known by authorities to be involved in narcotics trafficking. The vehicles were then exchanged for large quantities of drugs which were to be resold in Country R. Investigations revealed that the total amount of money involved in the scheme was in excess of US$355,000.

85. Case Study 13 – Car Importer committing tax evasion:

- Mr B bought and sold Porsche, BMW, Mercedes and other high value vehicles. He ordered the cars from mainland Europe and created a network of false identities and addresses to avoid paying import tax on the vehicles. Import documents gave false details and he built up a portfolio of false names and addresses from vehicle registration centres around the country. Police investigators traced the cars back to the importers. They found that numerous individuals had been paid £10 each to receive the vehicle registration documents through the post. Many of the cars were then sold for cash and were ultimately untraceable.
- As a result of the investigations, Cumbria Police secured £1 million in assets following the conviction of Mr B who was jailed for two and a half years for *money laundering* and conspiracy to defraud the Revenue Authorities.

86. Outstanding finance is a big risk faced by dealers who buy second hand cars. HPI Limited have advised that 24 out of every 100 cars offered for sale that are checked by them are still subject to a finance agreement. If the loan remains unpaid when the vehicle is purchased, the second-hand dealer and any subsequent buyer will not acquire good title to it.

14.4.5.5 Behaviours indicative of suspicious transactions

Guidance notes

High Value Dealers

87. The following are examples of potentially suspicious transactions:

- reluctance to make personal contact
- reluctance to provide the required identification information or evidence of identity
- the size of purchase is out of line with the appearance/age of the *customer*
- *customers* who initially indicate that they will be paying for goods over €15,000 by credit card/cheque and then at the last minute present cash as the means of payment
- there appear to be no genuine reasons for paying large sums of money in cash
- cash is unusual for that type of *customer*
- *customers* purchasing goods which are available nearer home at a similar price
- purchases by businesses where the level of cash activity is higher than the underlying business would justify
- the *customer* is paying in small denomination used notes.

14.4.5.6 Goods that are returned for refund

Guidance notes

High Value Dealers

88. Returning high value goods paid for in cash and obtaining a refund by way of a cheque or electronic payment enables the laundering of the "dirty money" by exchanging it for a legitimate retailer's payment. Suspicions may be raised in the following circumstances:
    - the *customer* enquires about the *supervised person's* refund policy prior to purchasing
    - the *customer* seeks a refund for spurious reasons
    - the *customer* seeks the repayment in the form of a cheque or electronic payment when the purchase or a deposit was made in cash.
89. Case Study 14 – The Cash Deposit Scam:
    - A professional criminal *money launderer* developed a simple technique of going into a number of high-priced West End jewellers and asking to inspect very expensive pieces of jewellery, saying that he was looking for a present for his wife. Dressed expensively and presenting himself well, he would choose various pieces and then ask to see the manager. Explaining that he wanted to give his wife the opportunity to choose for herself, he asked if the shop would be prepared to take the items off display, and hold them for his wife's inspection. He explained that he would be prepared to deposit significant sums of cash to be held by the shop as a deposit for the items chosen, and that once his wife had chosen the item she wished, he would pay the balance. He also explained that any sums uncollected could be returned to him in the form of a cheque made payable to one of his corporate entities.
    - On five separate occasions he placed significant sums of cash, a total in excess of £100,000, as 'deposits' for items of valuable jewellery. On each occasion, his 'wife' then went into the shop on the following day and inspected the relevant items. Finding nothing to her taste, she then asked the store to make a cheque payable to her husband's business as previously instructed.

› Both husband and wife were later arrested after one store learned about the unusual couple with so much money to spend but with such particular tastes. They shared the information among their trade members and discovered that the tactic had been used on a number of previous occasions. They then alerted the police.

90. Case Study 15 – Cash into Wine

› A similar technique was discovered by a leading wine trade company who discovered that a number of apparently wealthy Russian businessmen were asking to buy significant volumes of high-value wine, and keeping it held in 'bond' by the firm. The businessmen paid for their purchases in cash, but did not ask for the wine to be released from the bonded warehouse. This was not considered unusual as many wine buyers purchase investment wines in this way. Later, upon request, the businessmen asked for their wines to be re-sold back to the company, sometimes at enhanced rates, depending upon the prevailing sale-room price.

14.4.5.7 **Buying second-hand goods**

Guidance notes

High Value Dealers

91. High value dealers who buy high value second-hand items for trading on should be vigilant to avoid handling stolen property. A *money launderer* who has exchanged criminal cash for a high value asset and then trades it in has a cheque that can be paid into their bank account. They have therefore effectively 'placed' and 'integrated' the laundered money. Jewellers, art and antique dealers should use their networking to exchange information when stolen goods are being offered around for sale.

15 LAWYERS

15.1 Definition of Lawyers undertaking Supervised Business

1. Paragraph 1 of Part B of Schedule 2 to the *Proceeds of Crime Law* defines the relevant transactions and activity of lawyers for the purposes of the complying with *AML* requirements in the *Money Laundering Order* as being:
    - the business of providing services by independent legal professionals
    - independent legal professionals means those who by way of business provide legal or notarial services to third parties when participating in financial or immovable property transactions concerning any of the following:
        - the buying and selling of immovable property or business entities
        - the buying and selling of shares the ownership of which entitles the owner to occupy immovable property
        - the managing of client money, securities or other assets
        - the opening or management of bank, savings or securities accounts
        - the organisation of contributions necessary for the creation, operation or management of companies
        - the creation, operation or management of trusts, companies or similar structures.
2. Legal professionals employed by public authorities or undertakings which do not provide services to third parties are excluded from the definition.
3. A person is defined as participating in a transaction by assisting in the planning or execution of the transaction, or otherwise acting for or on behalf of a third party in a transaction.

15.1.1 Activities to which the Money Laundering Order applies

Overview

4. The *Money Laundering Order* only applies to certain legal activities as defined in Paragraph 1 of Part B of Schedule 2 to the Proceeds of Crime Law. In terms of activities covered it should be noted that:
    - managing *customer* money is narrower than handling it; and
    - operating or managing a bank account is wider than simply opening a client account. It would be likely to cover lawyers acting as a trustee, attorney or receiver.
5. The Attorney General has confirmed that the following would not generally be regarded as participating in Schedule 2 business:
    - payment on account of costs to a legal professional or payment of a lawyer's bill:
        - in respect of payments on account of costs, law firms should ensure that the payment is proportionate to the issue in respect of which the firm is asked to advise
        - in respect of payment of a lawyer's bill, if payment is made out of criminal property, this would constitute an offence under Article 30 of the Proceeds of Crime Law.

- Provision of legal advice:
  - in relation to the provision of legal advice, a lawyer needs to consider whether they are providing legal advice or whether they are a lawyer participating in a transaction by assisting in its planning or its execution. Ultimately, each case will have to be decided on its own facts and it is a matter for each firm to form a view
  - however, generally, the giving of generic advice, or advice specific to a transaction in terms of whether such a transaction is possible under Jersey Law or what factors are taken into account in making such a transaction possible, will only constitute the giving of legal advice where the decision has not already been taken to proceed with the transaction
  - where a decision has already been taken to proceed with a transaction, drafting documentation to enable that transaction to proceed, or seeking information to advise further on the planning or execution of the transaction will fall within the scope of the Money Laundering Order.
- Participation in litigation or a form of alternative dispute resolution:
  - in relation to litigation involving trusts where the proposed resolution includes a change in trusteeship or the application related to asking the Court to approve a future transaction, then the requirements of the *Money Laundering Order* may apply
  - in respect of advising insolvency practitioners relating to individuals or entities, the requirements of the *Money Laundering Order* are likely to apply
  - corporate transactions requiring Court approval, such as schemes of arrangement, are likely to be covered by the requirements of the *Money Laundering Order*.
- Will writing, although firms should consider whether any accompanying taxation advice is covered:
  - in relation to Will writing, any steps taken during the lifetime of the deponent of the Will to enable their wishes to be given effect to as recorded in the Will, may well fall within definition of *Schedule 2 business* in which case the requirements of the Money Laundering Order will apply.
- Publicly funded work:
  - publicly funded work extends to individuals under the legal aid scheme, even if an individual may be required to make a contribution to the fees of the law firm.

6. Whilst the *Money Laundering Order*, and consequently this Handbook, only brings within its scope the business activities of law firms where they are carrying on a *specified Schedule 2 business*, the *Anti-Money Laundering and Counter-Terrorism Legislation* and the general offences and penalties cover all persons and all business activities within Jersey. Consequently, law firms undertaking a significant proportion of *specified Schedule 2 business* may wish to consider applying the *systems and controls* to counter *money laundering,* the *financing of terrorism,* and the *financing of proliferation* across the whole of their business activities.

15.2 Business relationships and one-off transactions

Lawyers

Overview

7. This section is supplemental to and should be read in conjunction with Sections 1.6 and 3.2 of this Handbook.

8. As noted above, where a relationship between a *supervised person* and a *customer* has no "element of duration" and is not a *one-off transaction* within the meaning of Article 4 of the *Money Laundering Order*, identification measures within the meaning of Article 13 of the *Money Laundering Order* are not required unless:

   - the *supervised person* suspects money laundering or the financing of terrorism; or
   - the *supervised person* has doubts about the veracity or adequacy of any documents, data or information previously obtained under the CDD measures.

AML/CFT/CPF Codes of Practice

Lawyers

9. In the circumstances set out in paragraph 8 above, the identity of the person undertaking the transaction must still be found out and recorded.

10. A *supervised person* must record the basis that it has applied for determining the value of a transaction for the purposes of establishing whether it is a *one-off transaction* under Article 4 of the *Money Laundering Order*, and why that basis is appropriate.

11. A *supervised person* must have in place measures to identify when linked transactions are being undertaken which would, in total, amount to 15,000 euros or more (for all *supervised persons* save for money service business, virtual currency exchange business or operating a casino where different thresholds apply as set out in Article 4(1)), and therefore be a *one-off transaction* within the meaning of Article 4 of the *Money Laundering Order*. *Supervised persons* must also consider when the frequency of regular one-off transactions by the same *customer* would constitute a *business relationship*.

12. A *supervised person* must consider the nature of those transactions which are determined not to be a *one-off transaction* as a result of which *identification measures* are not required. Where these transactions are considered to present a higher risk of *money laundering* or the *financing of terrorism*, consideration must be given to applying full *CDD* measures.

13. A *supervised person* must be able to demonstrate that their decision not to apply *identification measures* in respect of such transactions was reasonable taking into account its business risk profile.

Guidance notes

14. A *supervised person* may demonstrate that the basis upon which it has determined the value of a conveyancing transaction for the purposes of Article 4 of the *Money Laundering Order* is appropriate where it applies the value of the property that is the subject of the transaction.

15.3 Business Risk Assessment

Lawyers

15.3.1 Considering and assessing service area vulnerabilities and warning signs

Lawyers

Overview

15. The business risk assessment relating to *customers* and services will depend on the *supervised person's* size, type of *customers* and the practice area it engages in.

16. *Supervised persons* carrying on *supervised* business specified at Paragraph 1, Part B of Schedule 2 of the Proceeds of Crime Law (***Lawyers***) should consider the different types of risk to which they are exposed when providing services. The risks should be considered within the context that a *supervised person* may be used to launder funds or assets through that *supervised person* or, alternatively, that the *customer* or its counterparties may launder criminal funds or assets, but in a way that does not touch the *supervised person*. This service area risk assessment must also be reflected when undertaking a *customer* risk assessment.

17. The following sub-sections set out some key legal service area vulnerabilities drawn from *FATF* and law enforcement guidance and case studies, and some key warning signs that have been drawn up by the Law Society for England and Wales, as an indication of service area vulnerabilities. Further factors to consider when evaluating the risks posed by *customers* and service areas are set out in Section 3.3.4 of this Handbook.

15.3.1.1 Use of Client Accounts

Guidance notes

Lawyers

18. Lawyers should not provide a banking service for their *customers*. However, it can be difficult to draw a distinction between holding *customer* money for a legitimate transaction and acting more like a bank. For example, when the proceeds of a sale are left with a *supervised person* to make payments, these payments may be to mainstream lending companies, but may also be to more obscure recipients, including private individuals, whose identity is difficult or impossible to check.

19. Situations which could give rise to cause for concern are detailed at Section 6.4.2.2 of this Handbook.

20. *Supervised persons* should think carefully before disclosing client account details as this allows money to be deposited into a client account without the *supervised person's* knowledge. If it is necessary to provide account details, *supervised persons* should ask the *customer* where the funds will be coming from. Will it be an account in their name, from Jersey or another jurisdiction? *Supervised persons* should consider whether they are prepared to accept funds from any source that they are concerned about.

21. Circulation of client account details should be kept to a minimum. *Customers* should be discouraged from passing the details on to third parties and should be asked to use the account details only for previously agreed purposes.

15.3.1.2 Establish a Policy on Handling Cash

Guidance notes

Lawyers

22. It is good practice to establish a policy of not accepting cash payments above a certain limit either at the *supervised person's* office or into the *supervised person's* bank account. *Customers* may attempt to circumvent such a policy by depositing cash directly into a client account at a bank. *Supervised persons* may consider advising *customers* in such circumstances that they might encounter a delay in completion of the final transaction. Avoid disclosing client account details as far as possible and make it clear that electronic transfer of funds is expected.

15.3.1.3 Source of Funds

Guidance notes

Lawyers

23. Accounts staff should monitor whether funds received from *customers* are from credible sources. For example, it is reasonable for monies to be received from a company if your *customer* is a director of that company and has the authority to use company money for the transaction.

24. In some circumstances, cleared funds will be essential for transactions and *customers* may want to provide cash to meet a completion deadline. *Supervised persons* should assess the risk in these cases and ask more questions if necessary.

15.3.1.4 Private client work – Administration of estates

Guidance notes

Lawyers

25. A deceased person's estate is very unlikely to be actively utilised by criminals as a means for laundering their funds, however there is still a risk of *money laundering* for those working in this area.

26. When winding up an estate, there is no blanket requirement that *supervised persons* should be satisfied about the history of all of the funds which make up the estate under administration. However, *supervised persons* should be aware of the factors which can increase *money laundering* risks and consider the following:

    - where estate assets have been earned in a foreign jurisdiction, *supervised persons* should be aware of the wide definition of criminal conduct in the *Proceeds of Crime Law* and
    - where estate assets have been earned or are located in a *higher risk country or territory*, *supervised persons* may need to make further checks about the source of those funds.

27. *Supervised persons* should be alert from the outset and monitor throughout so that any disclosure can be considered as soon as knowledge or suspicion is formed and problems of delayed consent can be avoided (see Section 8.4 of this Handbook).

28. *Supervised persons* should bear in mind that an estate may include criminal property. An extreme example would be where the *supervised person* knows or suspects that the deceased person was accused or convicted of acquisitive criminal conduct during their lifetime.

29. If *supervised persons* know or suspect that the deceased person improperly claimed welfare benefit/allowances or had evaded the due payment of tax during their lifetime, criminal property will be included in the estate and so a *money laundering* disclosure may be required.

30. Relevant local laws will apply before assets can be released. For example, a grant of probate will normally be required before UK assets can be released. *Supervised persons* should remain alert to warning signs, for example if the deceased or their business interests are based in a *higher risk country or territory*.

31. If the deceased person is from another jurisdiction and a lawyer is dealing with the matter in the home country, *supervised persons* may find it helpful to ask the lawyer for information about the deceased to gain some assurances that there are no suspicious circumstances surrounding the estate. The issue of the tax payable on the estate may depend on the jurisdiction concerned.

15.3.1.5 **Property transactions**

Guidance notes

Lawyers

32. Criminal conduct generates huge amounts of illicit capital and these criminal proceeds need to be integrated into personal lifestyles and business operations. Law enforcement agencies have advised that property purchases are one of the most frequently identified methods of *money laundering*. Property can be used either as a vehicle for *money laundering* or as a means of investing laundered funds.

33. Criminals will buy property both for their own use, e.g. as principal residencies or second homes, business or warehouse premises, and as investment vehicles to provide additional income. The Serious Organised Crime Agency in the UK has advised that real property arises in over 85% of all confiscation cases and at least 25% of those investigated hold five or more properties both residential and commercial.

34. The purchase of real estate is commonly used as part of the last stage of *money laundering*. Such a purchase offers the criminal an investment which gives the appearance of financial stability. The purchase of a restaurant or hotel, for example, offers particular advantages, as it is often a cash-intensive business, which is the preferred currency of criminals. Cash remains the mainstay of much serious organised criminal activity. It has the obvious advantage that it leaves no audit trail and is the most reliable form of payment, as well as the most flexible. Retail businesses also provide a good front for criminal funds where legitimate earnings can be mixed with the proceeds of crime.

15.3.1.6 Criminal Use of Conveyancing Services

Guidance notes

Lawyers

35. Law enforcement agencies have advised that of all the services offered by legal practitioners, conveyancing is the function most utilised by criminal groups. Conveyancing is a comparatively easy and efficient method of laundering money with relatively large amounts of criminal monies 'cleaned' in one transaction. In a stable or rising property market, the *money launderer* will incur no financial loss except fees. Conveyancing transactions can also be attractive to *money launderers* who are attempting to disguise the audit trail of the proceeds of their crimes. As the property itself can be 'criminal property' for the purposes of the *Proceeds of Crime Law*, lawyers can still be involved in *money laundering* even if no money changes hands.

36. Corrupt lawyers may employ trainees to perform the conveyancing work for criminal groups, thereby distancing themselves from the criminal aspect of the business. Conveyancers should also be alert to instructions which are a deliberate attempt to avoid assets being dealt with in the way intended by the court or through the usual legal process. For example, lawyers may sometimes suspect that instructions are being given to avoid the property forming part of a bankruptcy, or forming part of assets subject to confiscation.

15.3.1.7 Ownership Issues

Guidance notes

Lawyers

37. Properties owned by nominee companies or multiple owners may be used as *money laundering* vehicles to disguise the true owner and/or confuse the audit trail. *Supervised persons* should be alert to sudden or unexplained changes in ownership.

38. Unexplained changes in ownership may indicate a form of *money laundering* known as "flipping", which involves a property purchase, often using someone else's identity. The property is then quickly sold for a much higher price to the same buyer using another identity. The proceeds of crime are mixed with mortgage funds for the purchase. This process may be repeated several times.

39. Another potential cause for concern is where a third party is providing the funding for a purchase, but the property is being registered in someone else's name. There may be legitimate reasons for this, such as a family arrangement, but *supervised persons* should be alert to the possibility of being misled about the true ownership of the property. Further *CDD* measures should be undertaken on the person providing the funding.

15.3.1.8 Methods of Funding

Guidance notes

Lawyers

40. Many properties are bought with a combination of deposit, mortgage and/or equity from a current property. Usually, the lawyer acting for the purchaser will have information about how the *customer* intends to fund the transaction. Lawyers should expect to be updated if those details change, for example, if a mortgage falls through and new funding is obtained.

41. *Supervised persons* should remember that payments made through the mainstream banking system are not guaranteed to be clean.

42. Transactions that do not involve a mortgage or are not being financed wholly from the sale of a previous property have a higher risk of being fraudulent. *Supervised persons* should be alert for large payments from private funds, especially if the *customer* receives payments from a number of individuals or sources. If concerns arise:

    - the *customer* should be asked to explain the *source of funds*. *Supervised persons* should assess whether the explanation appears to be valid – e.g. the money has been received from an inheritance and
    - ensure that the *customer* is the *beneficial owner* of the funds being used in the purchase.

43. Settlements which are to be paid in cash – particularly where cash is to be passed directly between sellers and buyers without adequate explanation – may indicate *money laundering,* the *financing of terrorism,* or the *financing of proliferation*.

44. Third parties often assist with purchases and *supervised persons* may be asked to receive funds directly from third parties, for example relatives often assist first time buyers. Consideration will need to be given as to the extent of due diligence that needs to be undertaken on those third parties. *Supervised persons* should consider whether there are any obvious warning signs and what needs to be known about:

    - the *customer*
    - the third party
    - their relationship and
    - the proportion of the funding being provided by the third party.

45. *Supervised persons* should consider their obligations to the mortgage lender in these circumstances – *supervised persons* are normally required to advise mortgage lenders if the buyers are not funding the balance of the price from their own resources.

15.3.1.9 **Valuations**

Guidance notes

Lawyers

46. An unusual sale price can be an indicator of *money laundering*. Whilst lawyers acting in a property sale are not required to get independent valuations, if a *supervised person* becomes aware of a significant discrepancy between the sale price and what a property would reasonably be asked to sell for, consideration should be given to asking more questions.

47. Properties may also be sold below the market value to an associate, with a view to obscuring the title to the property while the original owner still maintains the beneficial ownership.

15.3.1.10 Mortgage Fraud

Guidance notes

Lawyers

48. A *supervised person* may discover or suspect that a *customer* is attempting to mislead a lender to improperly inflate a mortgage advance – for example, by misrepresenting the borrower's income or because the seller and buyer are conspiring to overstate the sale price. Transactions which are not at arm's length may warrant particular consideration. However, until the improperly obtained mortgage advance is received, there is not any criminal property for the purposes of disclosure obligations to the *JFCU*.

49. If a *supervised person* suspects that a *customer* is making a misrepresentation to a mortgage lender, the *supervised person* must either dissuade them from doing so or consider the ethical implications of continuing with the retainer. Even if a *supervised person* no longer acts for the *customer*, it may still be under a duty to advise the mortgage lender.

50. Large scale mortgage fraud is more sophisticated and will normally involve several properties. It may be committed by criminal groups or by individuals. The buy-to-let market is particularly vulnerable to large scale mortgage fraud, whether through new-build apartment complexes or large scale renovation properties. Occasionally commercial properties will be involved.

51. Fraudsters may use private sources of funding such as property clubs, especially when credit market conditions tighten. These lenders often have lower safeguards than institutional lenders, leaving them vulnerable to organised fraud. Property clubs can be targeted particularly in relation to overseas properties where the property either does not exist, or is a vacant piece of land, not a developed property.

52. Sometimes fraud is achieved by selling the property between related private companies. The transactions will involve inflated values and will not be at arm's length. Increasingly, offshore companies are used with the property sold several times within the group before approaching a lender for a mortgage at an inflated value.

53. *Supervised persons* that discover or suspect that a mortgage advance has already been improperly obtained should consider advising the mortgage lender.

54. *Supervised persons* acting in connection with a re-mortgage who discover or suspect that a previous mortgage has been improperly obtained may need to advise the lender, especially if the re-mortgage is with the same lender. Consideration should also be given to making a disclosure to the *JFCU* as the improperly obtained mortgage advance represents criminal property.

55. If a *customer* has made a deliberate misrepresentation on their mortgage application, it is likely that the crime/fraud exemption to legal professional privilege will apply (see Section 15.5.1 of this Handbook). This means that no waiver of confidentiality will be needed before a disclosure is made. However, such matters will need to be dealt with on a case-by-case basis.

15.3.1.11 Company and Commercial Work

Guidance notes

Lawyers

56. The nature of company structures can make them attractive to *money launderers* because it is possible to obscure true ownership and protect assets for relatively little expense. For this reason, lawyers working with companies and in commercial transactions should remain alert throughout their business relationships, with existing as well as new *customers*.

57. A common operating method amongst serious organised criminals is the use of front companies. These are often used to disguise criminal proceeds as representing the legitimate profits of fictitious business activities. They can also help to make the transportation of suspicious cargoes appear as genuine goods being traded. More often than not, they are used to mask the identity of the true *beneficial owners* and the source of criminally obtained assets. Corporate vehicles are also frequently used to help commit tax fraud, facilitate bribery/corruption, shield assets from creditors, facilitate fraud generally or circumvent disclosure requirements.

58. The lack of transparency concerning the *beneficial ownership and control* of corporate vehicles has proved to be a consistent problem for *money laundering* investigations. Corporations acting as directors and nominee directors can be used to conceal the identity of the natural persons who manage and control a corporate vehicle.

59. Several international reports have highlighted the extent to which private limited companies, shell companies, bearer shares, nominees, front companies and special purpose vehicles have been used in *money laundering* operations. Case studies submitted to the *FATF* have indicated the following common elements in the misuse of corporate vehicles:

- multi-jurisdictional and/or complex structures of corporate entities and trusts
- foreign payments without a clear connection to the actual activities of the corporate entity
- use of offshore bank accounts without clear economic necessity
- use of nominees
- use of shell companies
- tax, financial and legal advisers were generally involved in developing and establishing the structure. In some case studies a lawyer was involved who specialised in providing illicit services for *customers*.

60. The more of the above elements that exist, the greater the likelihood and the risk that the identity of the underlying *beneficial owner* may be able to remain unidentifiable.

15.3.1.12 Shell Corporations

Guidance notes

Lawyers

61. The shell corporation is a tool that appears to be widely used by criminals. Often purchased "off-the-shelf", it can be a convenient vehicle for *money laundering* and for concealing the identity of the *beneficial owner* of the funds. The company records are often more difficult for law enforcement to access because they are held behind a veil of professional privilege or the professionals who run the company act on instructions remotely and anonymously.

62. Shell companies are often used to receive deposits of cash which are then transferred to another jurisdiction, to facilitate false invoicing or to purchase real estate and other assets. They have also been used as the vehicle for the actual predicate offence of bankruptcy fraud on many occasions.

15.3.1.13 Bearer Shares

Guidance notes

Lawyers

63. Bearer shares confer rights of ownership to a company upon the physical holder of the share. They are commonly and legitimately used in a number of countries. However, the high level of anonymity that bearer shares offer provides opportunities for misuse where the identity of the shareholder is not recorded when the share is issued and transferred, ownership of the share is effectively anonymous.

64. Such shares are open to two *money laundering* risks:

- financial assets can be acquired without the purchaser being identified and
- the company owners and controllers may not be capable of being identified.

65. To guard against misuse, a number of jurisdictions have dematerialised or immobilised bearer shares when they are registered in an effort to ensure that the identity of the beneficial owners can be verified. Dematerialisation is achieved by requiring registration upon transfer or requiring registration in order to vote or collect dividends. While physical transfer of bearer shares is possible, it is believed to be rare.

15.3.1.14 Private Equity

Guidance notes

Lawyers

66. Law firms could be involved in any of the following circumstances:

- the start-up phase of a private equity business where individuals or companies seek to establish a private equity firm (and in certain cases, become authorised to conduct investment business)
- the formation of a private equity fund
- ongoing legal issues relating to a private equity fund
- execution of transactions on behalf of a member of a private equity firm's group of companies (a private equity sponsor that will normally involve a vehicle company acting on its behalf).

67. Private equity work may be considered to be low risk for *money laundering,* the *financing of terrorism,* or the *financing of proliferation* for the following reasons:

- private equity firms are also covered by the *Money Laundering Order* and similar legislation in equivalent jurisdictions
- investors are generally large institutions, some of which will also be regulated for *money laundering* purposes

- there are generally detailed due diligence processes followed prior to investors being accepted
- the investment is generally illiquid and the return of capital is unpredictable
- the terms of the investment in the fund generally strictly control the transfer of interests and the return of funds to investors.

68. Factors which may alter this risk assessment include:
    - where the private equity firm, fund manager or an investor is located in a jurisdiction which is not regulated for *money laundering* to a standard which is equivalent to the *FATF* recommendations
    - where the investor is either an individual or an investment vehicle itself (a private equity fund of funds)
    - where the private equity firm is seeking to raise funds for the first time or is approaching a large investor base.

15.4 Corporate governance

Lawyers

15.4.1 The Money Laundering Reporting Officer

Overview

69. This section is supplemental to and should be read in conjunction with Section 2.6 of this Handbook.
70. Section 2.6 sets out statutory requirements under the *Money Laundering Order* and *AML/CFT/CPF Codes of Practice* regarding the appointment a *MLRO* and, where relevant, *deputy MLROs*.

AML/CFT/CPF Codes of Practice

Lawyers

71. A *supervised* person must ensure that the *MLRO* maintains a record of all enquiries received from law enforcement authorities.

15.5 Identification Measures: Finding out identity and obtaining evidence

Lawyers

15.5.1 Timing of Identification Measures

72. Section 4.7 of this Handbook sets out statutory requirements under the *Money Laundering Order* regarding when *identification measures* must be applied, in respect of a *business relationship* or *one-off transaction*.
73. Article 13(4) of the *Money Laundering Order* allows, in certain circumstances, a *supervised person* a reasonable timeframe to undertake the necessary enquiries for obtaining **evidence of identity** after the initial establishment of a relationship.
74. A relationship is considered to be established as soon as a *supervised person* undertakes to act on instructions as to the operation of that relationship, for example, by receiving and accepting signed terms of business from the *customer*.

75. Where the provision of *Schedule 2 business* by the lawyer is urgent, this undertaking may be provided prior to obtaining **evidence of identity** if there is little risk of *money laundering* or the *financing of terrorism* occurring and evidence of identity is obtained as soon as reasonably practicable. Nevertheless, identity is still required to be **found out**.

15.5.2 Timing for "existing clients"

Lawyers

76. This sector-specific section is supplementary to and should be read in conjunction with Section 4.7.2 of this Handbook.

77. For the purposes of the *Money Laundering Order*, an existing customer means a *business relationship* established before the *Money Laundering Order* came into force for lawyers on **1 May 2008** and which continues.

78. For the avoidance of doubt, the *identification measures* (finding out identity and obtaining evidence) to be applied to existing customers include the collection of information that is necessary to assess the risk that a *business relationship* involves *money laundering* or the *financing of terrorism* (in line with Article 3(5) of the *Money Laundering Order*). This is likely to be self-evident for an existing customer on the basis that a relationship will have been established on, or before, **30 April 2008**.

79. Except with the agreement of the *JFSC*, (in relation to an application from the *supervised person* made on or before 31 December 2014), the effect of Article 13(3A) of the *Money Laundering Order* is to require the identity of a *customer* to have been found out by 31 December 2014. There is no similar deadline for obtaining evidence of identity.

80. Once an existing relationship has been "remediated", then Article 13(1)(c)(ii) of the *Money Laundering Order* will apply to such a relationship in the same way as a relationship established on or after **1 May 2008** (on the basis that documents, data or information will have been obtained under the *CDD* measures prescribed in Article 3).

15.5.3 Ascertaining Legal Position

Lawyers

Overview

81. Section 4.8 of this Handbook sets out the statutory requirements under the *Money Laundering Order* to terminate a *business relationship* or not carry out a *one-off transaction* where a *supervised person* is unable to apply *identification measures* in respect of that relationship or one-off transaction.

82. A concession from terminating a *business relationship* is permitted for accountants, lawyers and other professional advisers who are in the course of ascertaining the legal position for their *customer* or performing the task of defending or representing their *customer* in legal proceedings (including advice on instigating or avoiding proceedings).

83. To qualify for the concession the accountant, lawyer or other professional adviser must be a member of a relevant professional body that undertakes competency testing for its members and imposes and maintains professional and ethical standards.

Statutory requirements (paraphrased wording)

Lawyers

84. *Article 14(9) of the Money Laundering Order provides that the prohibition from continuing a business relationship does not apply where the relevant person is a lawyer or other business falling within paragraph 1 or 2 of Part B of Schedule 2 to the Proceeds of Crime Law and is in the course of ascertaining the legal position for that person's client or performing the task of defending or representing the client in, or concerning legal proceedings, including advice on instituting or avoiding proceedings.*

Guidance notes

85. *CDD* information will still need to be collected within a reasonable timescale in order to comply with Article 13 of the *Money Laundering Order*.

86. Accountants, lawyers and other relevant professional advisers are encouraged to consider their position very carefully before applying the above concession to ensure that the type of work and their professional status falls within the conditions contained in Article 14(9) of the Money Laundering Order.

87. For example, the concession applies to litigation but not transactional work, so lawyers should be mindful of the distinction between advice, litigation work and transactional work.

15.6 Exemptions from CDD measures

Lawyers

15.6.1 Exemption from applying third party identification requirements in relation to certain relevant customers involved in *trust company business*

Overview

88. This section is supplemental to and should be read in conjunction with Section 7.15 of this *Handbook*.

89. Article 17C(1)(c)(ii) of the *Money Laundering Order* provides that a *supervised person* that is a lawyer is exempt from applying third party identification requirements in relation to a third party for which a relevant customer is acting if the relevant customer carries on *trust company business* and is registered to carry on such business under the FS(J) Law, or *equivalent business*.

90. Article 17C(2) of the *Money Laundering Order* requires that a *supervised person* who does not apply third party identification requirements must be satisfied, by reason of the nature of the relationship with the relevant customer, that there is little risk of *money laundering* occurring.

Guidance notes

91. In relation to the exemption set out at Article 17C(1)(c)(ii) of the *Money Laundering Order*, a *supervised person* may be satisfied that there is little risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* occurring where:

- The service provided to a *trust company business* relevant customer is drafting (including incidental reviewing and advising (insofar as the *Money Laundering Order* is applicable)) of one or more of the following and
- It considers the extent of the service provided.

In respect of trusts (except employee benefit schemes) administered by a relevant customer carrying on *trust company business*, the service provided by the *supervised person* is drafting:

- a trust deed
- a supplemental trust deed of:
    - appointment
    - advancement
    - disclaimer
    - indemnity or release
    - appointment, retirement and indemnity
    - addition
    - exclusion
    - amendment
    - change of proper law
    - revocation or termination.
- a loan agreement or loan assignment or novation
- factual confirmations covering matters such as the existence and status of a trust and its trustee's capacity to enter into transactional documentation.

In respect of companies or partnerships administered by a relevant customer carrying on *trust company business*, the service provided by the *supervised person* is drafting:

- incorporation documents
- a loan agreement or loan assignment or novation
- minutes and other corporate authorisations
- stock transfer forms and share certificates
- memoranda and articles of association
- factual confirmations covering matters such as the existence and status of a company or partnership and its capacity to enter into transactional documentation.

In respect of employee benefit schemes (including pension schemes) controlled or administered by a relevant customer carrying on *trust company business*, the service provided by the *supervised person* is drafting:

- a trust deed
- a supplemental trust deed of:
    - appointment
    - advancement
    - disclaimer
    - indemnity or release
    - appointment, retirement and indemnity
    - addition

- exclusion
- amendment
- change of proper law
- revocation or termination.

› a loan agreement or loan assignment or novation

› factual confirmations covering matters such as the existence and status of a trust (or other vehicle by which the scheme is structured) and its capacity to enter into transactional documentation.

In respect of a foundation administered by a relevant customer carrying on *trust company business*, the service provided by the *supervised person* is drafting:

› statutory forms

› charters and regulations

› supplemental deeds of:

- initial and further endowments
- transfers of assets
- indemnities and releases
- distributions
- amendments and variations
- changes of proper law
- continuance and mergers, revocation, termination, winding up or dissolution
- appointment/removal of guardian or any other person appointed under the regulations of the foundation to carry out a function in respect of the foundation
- guardian sanctioning of council actions;
- addition and removal of beneficiaries and changes of purposes
- addition, amendment, removal, exercise, assignment of founders' rights
- appointment and removal of council members
- releases of powers
- delegation of council powers.

› factual confirmations covering matters such as the existence and status of a foundation and its capacity to enter into transactional documentation.

92. The above is not intended to be an exhaustive list of documents for which drafting services are provided and a *supervised person* may be able to demonstrate that other drafting services present little risk of *money laundering*, *terrorist financing,* or *proliferation financing*.

93. A *supervised person* may demonstrate that it has considered the extent of the service provided to the relevant customer when it considers:

› whether the service provided is "off the shelf" or bespoke

› the need for and extent to which an "off the shelf" service is to be modified and

› the fee that is to be charged.

94. For example, the provision of a standard trust deed that requires very little modification, may be described as "off the shelf" and attracts only a nominal fee, may be illustrative of a relationship presenting little risk of *money laundering*. By contrast, the provision of a bespoke trust deed that requires detailed information on the trust to be collected and which attracts more than a nominal fee, may not.

15.6.2 Jersey property transfers

Lawyers

Overview

95. This section is supplemental to and should be read in conjunction with Section 7.16 of this *Handbook*.

96. This section relates to the exemption available under Article 18(6) of the *Money Laundering Order*, which provides that a *supervised person* that is a lawyer or an estate agent, which enters into a *business relationship* or carries out a *one-off transaction* for the purpose of enabling a *customer*, directly or indirectly, to enter into a registered contract within the meaning of the Control of Housing and Work (Jersey) Law 2012 (i.e. where it is to be passed before the Royal Court and registered in the Public Registry of Contracts), need not obtain **evidence of identity** of its *customer*.

AML/CFT/CPF Codes of Practice

Lawyers

97. For each case described in Article 18 of the *Money Laundering Order*, a *supervised person* must obtain information on the purpose and intended nature of the *business relationship* or *one-off transaction*.

98. A *supervised person* that is a *lawyer* must obtain and retain documentation establishing that its *customer* is entitled to benefit from the exemption set out in Article 18(6) of the *Money Laundering Order*.

15.7 Reporting Money Laundering and Terrorist Financing Activity

Lawyers

Overview

99. This section is supplemental to and should be read in conjunction with the *AML/CFT/CPF Codes of Practice* and *guidance notes* set out at Section 8 above.

15.7.1 Legal Professional Privilege (LPP)

Overview

100. Lawyers are under a duty to keep the affairs of their *customers* confidential, and the circumstances in which they are able to disclose *customer* communications are strictly limited.

101. However, the *Proceeds of Crime Law* and *Terrorism Law* contain provisions requiring the disclosure of confidential information in certain circumstances to the police (or a *MLRO/deputy MLRO*) by persons working in *Schedule 2 businesses*. These laws also provide individuals working for law firms which conduct *Schedule 2 business* with certain defences against proceedings for breaching any duty of confidentiality, or for an offence such as *money laundering*, if they make a disclosure to the police or to a *MLRO/deputy MLRO* in accordance with the procedures set down by their employer.

102. This section examines some of the tensions which may arise between a lawyer's duty of confidentiality to their *customer* and the disclosure requirements set out in the *Proceeds of Crime Law* and *Terrorism Law*.

Statutory requirements (paraphrased wording)

Lawyers

103. Article 34D of the Proceeds of Crime Law and Article 21 of the Terrorism Law contain comparable provisions. Those provisions provide that a person employed in a Schedule 2 business commits an offence if they come into possession of information in the course of that business which leads them to know or suspect, or have reasonable grounds to know or suspect, that another person is engaged in money laundering (e.g. the offences set out at Articles 30 and 31 of the Proceeds of Crime Law) or is committing an offence under Articles 15 and 16 of the Terrorism Law, or conduct outside Jersey which if occurring in Jersey would constitute one of the above offences. The offence is committed, unless the person reports their knowledge, suspicion or reasonable grounds to a police officer or to the MLRO (or deputy MLRO) in accordance with their employer's procedures.

104. The Money Laundering Order requires that any person who conducts a financial services business in Jersey must have procedures in place for reporting such knowledge or suspicion to the JFCU.

105. However, the Proceeds of Crime Law and Terrorism Law also include exemptions from the requirement to make such disclosures for professional legal advisers acting in privileged circumstances (see Article 34D(5) of the Proceeds of Crime Law, for example). Legal privilege is defined in the three laws referenced above. The exemptions do not apply to information or other matters communicated or given with a view to furthering a criminal purpose.

106. Article 35 of the Proceeds of Crime Law and Article 35 of the Terrorism Law prohibit disclosure of information in circumstances where a suspicious activity report has been made and/or where it would prejudice an existing or proposed investigation. However, an exception is also provided in respect of these offences where a professional legal adviser discloses any information or other matter:

- *to a customer or to a representative of a customer of the legal adviser in connection with the giving of legal advice by the adviser to the customer or*
- *to any person for the purpose of actual or contemplated legal proceedings.*

Again, this exemption does not apply in relation to any information or other matter that is disclosed with a view to furthering a criminal purpose.

15.7.1.1 Duty of confidentiality

Overview

Lawyers

107. *Lawyers* are professionally and legally obliged to keep the affairs of their *customers* confidential. This obligation extends to all matters revealed to a lawyer, from whatever source, by a *customer* or someone acting on the *customer's* behalf.

108. In exceptional circumstances, this obligation may be overridden. The most relevant instances are where a court orders disclosure or disclosure is required by statute.

15.7.1.2 Application of LPP

109. Certain confidential communications between a lawyer and their *customer* will fall into a category known as *LPP*. *LPP* is a privilege against disclosure, ensuring *customers* know that certain documents and information provided to lawyers cannot be disclosed without the *customer's* consent. It recognises a *customer's* right to be open with their legal adviser, without fear of later disclosure to their prejudice. *LPP* cannot be overridden by any other public interest, but can be waived or overridden by statute.

110. *LPP* only covers those confidential communications falling under either **advice privilege** or **litigation privilege**. It does not cover all information/matters which lawyers have a duty to keep confidential.

111. For the purposes of *LPP*, the term "lawyers" includes Advocates, Écrivains, barristers, solicitors, in-house lawyers and their employees.

15.7.1.3 Advice Privilege

Guidance notes

Lawyers

112. Communications between a lawyer and a *customer* are subject to **advice privilege** if:

- the lawyer is communicating with the customer in their capacity as a lawyer
- the communications are confidential and
- the communications are being made for the purpose of seeking advice from a lawyer or providing it to a *customer*.

113. Communications are not privileged simply because a *customer* is speaking or writing to their lawyer. The protection applies only to those communications which directly seek or provide advice or which are given in a legal context, that involve the lawyer using their legal skills and which are directly related to the performance of the lawyer's professional duties.

114. Some examples of what is/is not covered by advice privilege, as established through case law, are set out below:

- communications **subject** to advice privilege:
  - a lawyer's bill of costs and statement of account
  - information imparted by prospective *customers* in advance of a retainer, if the communications were made for the purpose of indicating the advice required.
- communications **not subject** to advice privilege:
  - notes of open court proceedings are not privileged as the content of the communication is not confidential
  - a client account ledger maintained in relation to the *customer's* money
  - an appointments diary or time record on an attendance note, time sheet or fee record relating to a *customer*
  - conveyancing documents (these documents are not communicated and therefore are not subject to advice privilege).

15.7.1.4 Advice within a transaction

115. All communications between a lawyer and their *customer* relating to a **transaction** in which the lawyer has been instructed for the purpose of obtaining legal advice are covered by advice privilege, provided that they are directly related to the performance by the lawyer of their professional duty as legal adviser of their *customer*.

116. This means that where a lawyer is providing legal advice in a transactional matter (such as conveyancing) the advice privilege will cover all:

- communications with
- instructions from and
- advice given to

The *customer*, including any working papers and drafts prepared, as long as they are directly related to the lawyer's performance of their professional duties as a legal adviser.

15.7.1.5 Litigation Privilege

Guidance notes

Lawyers

117. **Litigation privilege** is wider than advice privilege and protects confidential communications made in pursuance or contemplation of litigation, between either:

- a lawyer and a *customer*
- a lawyer and an agent, whether or not that agent is a lawyer or
- a lawyer and a third party.

118. Such communications must be **for the sole or dominant purpose of litigation**, namely:

- for seeking or giving advice in relation to it
- for obtaining evidence to be used in it or
- for obtaining information leading to obtaining such evidence.

15.7.1.6 What is covered by LPP – Further points to consider

119. An original document not brought into existence for privileged purposes, and thus not already privileged, does not become privileged simply by being given to a lawyer for advice or another privileged purpose.

120. Furthermore, where a lawyer has a *customer* which is a body corporate, communication between the lawyer and the employees of the corporate *customer* may not be protected by LPP if those employees are not considered to be the *customer* for the purpose of the retainer. As such, some employees will be *customers*, while others will not.

121. It is not a breach of *LPP* to discuss a matter with your *MLRO* (or *deputy MLRO*) for the purpose of receiving guidance on whether to make a disclosure. Privilege will continue to apply whilst such a determination is being made.

15.7.1.7 Crime/Fraud Exception

Guidance notes

Lawyers

122. *LPP* protects advice a lawyer gives to a *customer* on avoiding committing a crime or warning them that proposed actions could attract prosecution. *LPP* **does not extend** to documents which themselves form part of a criminal or fraudulent act, or communications which take place in order to obtain advice with the intention of carrying out an offence. It is irrelevant whether or not the lawyer is aware that they are being used for that purpose.

123. Article 32 of the *Proceeds of Crime Law* and Article 22 of the *Terrorism Law* provide that, if a lawyer discloses information under those laws, the disclosure will not be treated as a breach of any restriction on disclosure contained in any statute, contract or otherwise.

124. It is not just a ***customer's*** intention which is relevant for ascertaining whether information was communicated for the furtherance of a criminal purpose. In addition to the circumstances described above, *LPP* **also does not extend** to a situation where a **third party** intends the lawyer-*client* communication to be made for the furtherance of a criminal purpose (e.g. the innocent client is being used by a criminal third party).

15.7.1.8 Determining when to submit a *SAR*

125. The reporting obligations and offences contained in Article 34D of the Proceeds of Crime Law and Article 21 of the Terrorism Law do not apply to a *lawyer's* knowledge or suspicion, or reasonable grounds for knowledge or suspicion, arising from information obtained in "privileged circumstances" (as defined by the above laws). The *Money Laundering Order* also makes a provision in respect of privileged circumstances at Article 21(5). A *lawyer* may, however, wish to consider making a joint report with their *customer*. The agreement of the lawyer's *customer* to waive *LPP* is necessary in order for this to be possible.

126. If information leading to knowledge, suspicion or reasonable grounds for knowledge or suspicion is obtained in circumstances that are not covered by *LPP*, a disclosure should be made to avoid the commission of an offence of failing to disclose. Lawyers will not be in breach of their professional duty of confidentiality if they make a report in these circumstances.

127. If a lawyer commits an offence under Article 30 of the *Proceeds of Crime Law* or Article 16 of the *Terrorism Law* they should make a disclosure to a police officer or their *MLRO*/*deputy MLRO*, otherwise they will not be able to avail themselves to the defences which operate under those Articles.

128. As the application of *LPP* is complex, *supervised persons* carrying on legal business may wish to consider maintaining procedures which require reports to be made to the *MLRO* (or *deputy MLRO*) **on each occasion** that there is knowledge, suspicion, or reasonable grounds to suspect *money laundering* or the *financing of terrorism*. The *MLRO* (or *deputy MLRO*) can then discuss the situation with the employee concerned and, as necessary, take advice from an appropriate partner.

15.7.1.9 **CDD measures and LPP**

Guidance notes

Lawyers

129. In order to assist in complying with the requirements of the *Proceeds of Crime Law*, *supervised persons* carrying on legal business may wish to consider separating all material on *customer* files so that it is clear what material is non-privileged and what material is covered by *LPP*.

130. *CDD* and risk assessment documents should be completed, where possible, in a way which distinguishes privileged and non-privileged information. *Supervised persons* carrying on legal business may wish to consider including guidance to this effect in their procedures. This will assist in ensuring that the *JFSC* can request information from and conduct examinations of *supervised persons* with the minimum disruption to business, thus aiding in the *supervised person's* compliance with their obligations to the *JFSC*.

16 ACCOUNTANTS

16.1 Definition and overview of Accountants undertaking supervised business

1. Paragraph 2 of Part B of Schedule 2 to the *Proceeds of Crime Law* defines the relevant transactions and activity of accountants for the purposes of complying with *AML* requirements in the *Money Laundering Order* as:

   - the business of providing any of the following:
     - *external accountancy services*
     - advice about the tax affairs of another person (*tax advisers*)
     - *audit services* or
     - *insolvency services*.

16.1.1 Accountancy Services

Overview

2. For the purposes of this Handbook, *accountancy services* is limited to services provided under a contract for services. Examples may include, but are not limited to, the recording, review, analysis, calculation or reporting of financial information.

3. Businesses that are not providing *Schedule 2 business* are outside the scope of the *AML/CFT/CPF Handbook*. However *Schedule 2 business* provided in the course of business will be covered by this Handbook, even if provided to a client on a *pro-bono* or unremunerated basis.

4. Accountants providing services privately on an unremunerated voluntary basis are not covered by this Handbook as they are not providing services 'by way of business'. However, all persons and businesses within Jersey are covered by the primary legislation covering *money laundering,* the *financing of terrorism,* and the *financing of proliferation*.

5. Accountants involved in the provision of management consultancy or interim management should be alert to the possibility that they could fall within the scope of the Money Laundering Order and by extension this Handbook to the extent that they provide any *Schedule 2 business* when acting under a contract for services in the course of business.

16.1.2 Tax Advisers

Accountants

Overview

6. Refer to the Glossary above for a definition of *tax advisers*.

7. It is the view of the *JFSC* that the provision of **tax compliance services** falls within the scope of the above-referenced definition.

8. A *tax adviser* should be aware of the *JFSC's* responsibility to regulate trust and company business, which may impinge upon the work they undertake for their *customers*.

9. Whilst *tax advisers* are more likely to identify tax offences, they need to be aware of the potential requirement to report knowledge or suspicion of proceeds derived from any criminal conduct (as defined in Article 1 of the *Proceeds of Crime Law*) which is encountered in the course of business as a *tax adviser*.

16.1.3 Audit Services

Accountants

Overview

10. Refer to the Glossary above for a definition of *audit services*.

11. For the purposes of this Handbook, all persons who are directly involved in the acceptance and performance of a particular audit are considered to be part of the audit 'engagement team' and fall under the umbrella term of 'auditors'. This includes the audit team, professional personnel from other disciplines involved in the audit engagement and those who provide quality control or direct oversight of the audit engagement. However, it does not include experts contracted by the *supervised person*.

12. The extent to which the *Anti-Money Laundering and Counter-Terrorism Legislation* affects the *auditor's* work differs between two broad categories of audit – audits of *supervised persons* and audits of other types of entity.

16.1.3.1 Audits of supervised persons

Guidance notes

13. *Supervised persons* carrying on *supervised business* (except *supervised persons* which are Prescribed NPOs under the meaning of the (Non-Profit Organisations (Prescribed NPOs – Additional Obligations) (Jersey) Order 2022) are required to comply with the *Money Laundering Order* which places obligations on them to combat *money laundering,* and the *financing of terrorism*. All such businesses are required to comply with the *AML/CFT/CPF Codes of Practice* and *guidance notes* issued by the *JFSC* (see Section 2.5 of this Handbook, which covers the monitoring of compliance with the same).

14. In addition to reporting on their financial statements, *auditors* of such businesses are required to report to the *JFSC* on matters of significance that come to their attention in the course of their work. This includes non-compliance with legislation, departures from its requirements and suspicions that the directors and management of such entities are implicated in *money laundering* (see Section 8 of this Handbook). Therefore, *auditors* of such businesses should not only be aware of the key provisions contained in the Money Laundering Order as they affect *auditors* themselves, but also the requirements of the wider *AML/CFT/CPF Handbook*, including any sector-specific *AML/CFT/CPF Codes of Practice* and *guidance notes* relevant to the business that they are auditing.

16.1.3.2 Audits of other types of entity

Guidance notes

Accountants

15. In general, *auditors* of other types of entity not covered by the *Money Laundering Order* are required only to take appropriate steps in response to factors encountered in the course of their work which lead them to suspect that *money laundering,* the *financing of terrorism,* or the *financing of proliferation* is taking place.

16.1.3.3 Detection of money laundering, the financing of terrorism, and the financing of proliferation

Guidance notes

Accountants

16. Whilst *auditors* have no statutory responsibility to undertake work solely for the purpose of detecting *money laundering,* the *financing of terrorism,* and/or the *financing of proliferation*, they nevertheless need to take the possibility of *money laundering,* the *financing of terrorism,* and the *financing of proliferation* into account in the course of carrying out procedures relating to fraud and compliance with the *Anti-Money Laundering and Counter-Terrorism Legislation*. An *auditor's* wide access to documents and systems, and the need to understand the business, can make them ideally suited to spot such issues as they arise.

17. However, auditors cannot be held responsible for the prevention of, and failure to detect, *money laundering*, *financing of terrorism,* and *financing of proliferation* activities in the entities they audit. External *auditors* performing financial statement audits within a short timescale may be less likely than other professional accountants (such as forensic accountants and accountants in management positions) to encounter signs of possible *money laundering, financing of terrorism,* or *financing of proliferation*. Nor is it the *auditors'* responsibility to detect suspicious activity in connection with a compliance or operational audit of an *AML/CFT/CPF* programme or testing a suspicious activity reporting process.

16.1.4 Insolvency services

Accountants

Overview

18. The terms *insolvency services and insolvency practitioners* are defined in the Glossary above.

16.1.5 Accountants undertaking Supervised Business

Accountants

Overview

19. Accountants may also provide other services that could bring them within the scope of mainstream financial services. These include:

- undertaking investment related activity, including acting as a financial intermediary
- advising on the setting up of trusts, companies or other bodies
- acting as trustee, nominee or company director
- giving advice on capital structures, acquisitions and securities issues

- providing safe custody services
- arranging loans.

20. Consequently, some *supervised persons* providing *accountancy services* are authorised and regulated by the *JFSC* under the *FS(J) Law* and subject to one or more of the Investment Business, Trust Company Business and Funds Services Business Codes of Practice. *Supervised persons* who are so regulated should therefore have regard to any relevant sector-specific sections of the *AML/CFT/CPF Handbook* when drawing up their *policies and procedures* for the prevention and detection of *money laundering,* the countering of terrorist *financing,* and the countering of *proliferation financing* in respect of those regulated activities.

16.2 Business Risk Assessment

Accountants

16.2.1 Considering customer and service risks to the business

Overview

21. The business risk assessment relating to *customers* and services will depend on the *supervised person's* size, type of *customers* and the practice area it engages in.

22. *Supervised persons* should consider the different types of risk to which they are exposed within the different service areas as set out below. The risks should be considered within the context that a *supervised person* may be used to launder funds or assets through the *supervised person* or, alternatively, that the *customer* or its counterparties may launder criminal funds or assets, but in a way that does not touch the *supervised person*. This service area risk assessment must also be reflected when undertaking a *customer* risk assessment.

23. Whilst the *Money Laundering Order*, and consequently this Handbook, only brings within its scope the business activities of accountancy firms where they are carrying on a *specified Schedule 2 business*, the *Anti-Money Laundering and Counter-Terrorism Legislation* and the general offences and penalties cover all persons and all business activities within Jersey. Consequently, accountancy firms undertaking *specified Schedule 2 business* may wish to consider applying the *systems and controls* to counter *money laundering,* the *financing of terrorism,* and the *financing of proliferation* across the whole of their business activities.

24. Further factors to consider when evaluating the risks posed by clients and service areas are set out in Section 3.3.4 of this Handbook.

16.2.1.1 Accountancy, Audit and Insolvency Service Risk

Guidance notes

25. Those providing *accountancy services, audit services* or *insolvency services* will primarily need to consider their business risk assessment in respect of the nature of their *customer* base, the business sectors in which their *customers* operate and the geographical location of their *customers*. The standing of *customers* and adherence to sound corporate governance principles will also have an impact including those *customers* that have previously been prosecuted or fined for criminal or regulatory offences.

26. The business risk assessment should take account of the following risks:

- setting up, winding up, or effecting recovery for high cash turnover businesses for *customers* which may provide a front for criminal money

- being used in an active sense to launder money through the handling of cash or assets or through payments that are made to, or received from, third parties, particularly with a cross-border element
- becoming concerned in an arrangement which facilitates *money laundering* through the provision of investment services
- becoming a party to serious fraud on the part of senior management or failing to recognise the warning signs relating to management fraud and
- the potential for *money laundering,* the *financing of terrorism,* and the *financing of proliferation* to become attached to the *customer* and/or those who trade with or otherwise interact with *customers*.
- those providing accountancy services should also consider the risks when:
    - providing assistance in setting up trusts or company structures which could be used to obscure beneficial ownership of monies and assets settled into trust and
    - handling the financial affairs, or setting up companies, trusts or other structures for politically exposed persons whose assets and wealth may be derived from the proceeds of corruption (see Section 7.6 of this Handbook).

27. Specialisation within a sector that undertakes higher risk activity from a *money laundering, terrorist financing,* and/or *proliferation financing* perspective will affect the business risk assessment. Examples of higher risk sectors and sensitive business areas for *money laundering*, *financing of terrorism,* and *financing of proliferation* purposes are:
    - *financial services businesses* (including money services businesses)
    - high cash turnover businesses: bars and clubs, taxi firms, launderettes, takeaway restaurants, market traders
    - gaming and gambling businesses
    - real estate and construction
    - computers and high technology, telecommunications and mobile phone businesses
    - arms and armaments.
28. *Customers* who are *supervised persons* - such as *financial services businesses*, money services businesses and estate agents that are covered by the *Money Laundering Order* - should have taken steps to mitigate their risks by implementing robust internal controls.

16.2.1.2 **Taxation Service Risk**

Guidance notes

Accountants

29. *Tax advisers* are not required to be experts in criminal law, but they are expected to be aware of the offences which can give rise to the proceeds of crime. For example, *tax advisers* should be aware of the boundaries between deliberate understatement or other tax evasion and simple cases of error or genuine differences in the interpretation of tax law. The main areas where offences may arise which might increase the risks of the *tax adviser* becoming concerned during an engagement are (note the below list is not exhaustive):
    - tax evasion, including making false returns (including supporting documents), accounts or financial statements or deliberate failure to submit returns
    - deliberate refusal to correct known errors
    - fraudulent or dishonest conduct
    - fraudulent evasion of *VAT* by *customers* operating within the *EU* including the possession and dealing in goods on which *VAT* has been evaded (e.g. Missing Trader Intra Community/Carousel fraud).

16.3 Risk-based approach to Identification Measures

Accountants

Overview

30. This section must be read in conjunction with, and is supplemental to, the *Guidance Notes* set out at Section 3.3.2 of this Handbook (Information for Assessing Risk – Stage 1.4).
31. The *guidance notes* set out below provide sector-specific guidance on additional factors *supervised persons* providing *accountancy services* may need to consider, in order to appropriately assess the risk that a *business relationship* or *one-off transaction* will involve *money laundering,* the *financing of terrorism,* or the *financing of proliferation*.

16.3.1.1 **Insolvency Cases**

Guidance notes

Accountants

32. In the context of insolvency work, the *customer* is considered to be the insolvent. An *insolvency practitioner* should risk assess, identify and verify the *customer* over which they are appointed.
33. A situation where an *insolvency practitioner* is required may be urgent, for example if there is a risk of dissipation of assets and erosion of value. It is therefore important for an *insolvency practitioner* to be certain about the identity of the *customer* over which they are taking appointment.

16.3.1.2 Auditing Standards on Acceptance of Client Relationships

Guidance notes

Accountants

34. Auditing standards on quality control for audits state that acceptance of *business relationships* and specific audit engagements includes considering the integrity of the principal owners, key management and those charged with governance of the *customer*. This involves the *auditor* making appropriate enquiries and may involve discussions with third parties, the obtaining of written references and searches of relevant databases.

35. The extent of knowledge a *supervised person* providing *audit services* will have regarding the integrity of a *customer* will generally grow within the context of an ongoing *business relationship* with that *customer*. However, useful information may be obtained at the outset of a *business relationship* including, for example:

    - the reasons for the proposed appointment of the *supervised person* and non-reappointment of the previous *auditors*
    - communications with existing or previous providers of professional accountancy, banking and legal services to the *customer*
    - background searches and the review of relevant databases.

36. Whilst adherence to auditing standards may provide some relevant *customer* identification information, they will not be sufficient on their own to comply with the requirements of the *Money Laundering Order* and this Handbook.

16.4 Identification Measures

Accountants

16.4.1 Obligation to find out identity and obtain evidence: Individuals

Overview

37. This sector-specific section is supplementary to and should be read in conjunction with Section 4.3 of this Handbook.

16.4.1.1 Insolvency Cases

38. It may not always be possible or necessary to obtain identification evidence direct from individuals, individual shareholders or directors in respect of an insolvent company as their co-operation may not be forthcoming.

Guidance notes

39. An *insolvency practitioner* may demonstrate compliance with Article 3 of the *Money Laundering Order* where it obtains evidence of the identity of the person or entity over which they are appointed. Acceptable evidence may include a court order, a court endorsed appointment, or an appointment made by a debenture holder or creditors meeting supported by a company search or similar.

16.4.2 Timing of identification measures

Accountants

40. Section 4.7 of this Handbook sets out statutory requirements under the Money Laundering Order regarding when identification measures must be applied, in respect of a *business relationship* or *one-off transaction*.

41. Article 13(4) of the *Money Laundering Order* allows, in certain circumstances, a *supervised person* a reasonable timeframe to undertake the necessary enquiries for obtaining **evidence of identity** after the initial establishment of a relationship.

42. A relationship is considered to be established as soon as a *supervised person* undertakes to act on instructions as to the operation of that relationship, for example, by receiving and accepting signed terms of business from the *customer*.

43. Where the provision of *Schedule 2 business* by the accountant is urgent, this undertaking may be provided prior to obtaining evidence of identity if there is little risk of *money laundering* or the *financing of terrorism* occurring and **evidence of identity** is obtained as soon as reasonably practicable.

16.4.3 Timing for "Existing Clients"

Accountants

44. This sector-specific section is supplementary to and should be read in conjunction with Section 4.7.2 of this Handbook.

45. For the purposes of the *Money Laundering Order*, an existing customer means a *business relationship* established before the *Money Laundering Order* came into force for accountants on **1 May 2008** and which continues.

46. For the avoidance of doubt, the *identification measures* (finding out identity and obtaining evidence) to be applied to existing customers include the collection of information that is necessary to assess the risk that a *business relationship* involves *money laundering* or the *financing of terrorism* (in line with Article 3(5) of the *Money Laundering Order*). This is likely to be self-evident for an existing customer on the basis that a relationship will have been established on, or before, **30 April 2008**.

47. Except with the agreement of the *JFSC* (in relation to an application from the *supervised person* made on or before 31 December 2014), the effect of Article 13(3A) of the *Money Laundering Order* is to require the identity of a *customer* to have been found out by 31 December 2014. There is no similar deadline for obtaining evidence of identity.

48. Once an existing relationship has been "remediated", then Article 13(1)(c)(ii) of the *Money Laundering Order* will apply to such a relationship in the same way as a relationship established on or after **1 May 2008** (on the basis that documents, data or information will have been obtained under the *CDD* measures prescribed in Article 3).

16.4.4 Ascertaining Legal Position

Accountants

Overview

49. Section 4.8 of this Handbook sets out the statutory requirements under the *Money Laundering Order* to terminate a *business relationship* or not carry out a *one-off transaction* where a *supervised person* is unable to apply *identification measures* in respect of that relationship or *one-off transaction*.

50. A concession from terminating a *business relationship* is permitted for accountants, lawyers and other professional advisers who are in the course of ascertaining the legal position for their *customer* or performing the task of defending or representing their *customer* in legal proceedings (including advice on instigating or avoiding proceedings).

51. To qualify for the concession the accountant, lawyer or other professional adviser must be a member of a *supervised* professional body that undertakes competency testing for its members and imposes and maintains professional and ethical standards.

Statutory requirements (paraphrased wording)

52. Article 14(9) of the Money Laundering Order provides that the prohibition from continuing a business relationship does not apply where the relevant person is a lawyer or other business falling within paragraph 1 or 2 of Part B of Schedule 2 to the Proceeds of Crime Law and is in the course of ascertaining the legal position for that person's client or performing the task of defending or representing the client in, or concerning legal proceedings, including advice on instituting or avoiding proceedings.

Guidance notes

53. *CDD* information will still need to be collected within a reasonable timescale in order to comply with Article 13 of the Money Laundering Order.

54. Accountants, lawyers and other *supervised* professional advisers are encouraged to consider their position very carefully before applying this concession to ensure that the type of work and their professional status falls within the conditions contained in Article 14(9) of the Money Laundering Order.

16.5 Exemptions from CDD Measures

Accountants

Overview

55. This section is supplemental to and should be read in conjunction with Section 7.15 of this *Handbook*.

56. Article 17C(1)(c)(iii) of the Money Laundering Order provides that a *supervised person* that is an accountant is exempt from applying *third party identification requirements* in relation to a third party for which a relevant customer is acting if the relevant customer carries on *trust company business* and is registered to carry on such business under the FS(J) Law, or *equivalent business*.

57. Article 17C(2) of the Money Laundering Order requires that a *supervised person* who does not apply third party identification requirements must be satisfied, by reason of the nature of the relationship with the relevant customer, that there is little risk of *money laundering* occurring.

Guidance notes

58. In relation to the exemption set out at Article 17C(1)(c)(iii) of the *Money Laundering Order*, a *supervised person* may demonstrate that due to the nature of the relationship with the relevant customer, there is little risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* occurring where the service being provided to the relevant customer is the provision of:

    - generic information on Jersey accounting requirements for the preparation of financial statements or
    - generic information on Jersey tax requirements and
    - it considers the extent of the service provided.

59. A *supervised person* may demonstrate that it has considered the extent of the service provided when it considers:

    - the extent of any further explanation of the Jersey accounting or tax requirements that may subsequently be needed and
    - the fee that is to be charged.

60. For example, the provision of generic information on Jersey accounting or tax requirements that requires no more than an **explanation** of a Jersey accounting or tax requirement and attracts only a nominal fee, may be illustrative of a service which presents little risk of *money laundering*. By contrast, the provision of detailed and complex **tax structuring services** that require detailed information of the person or arrangement in question to be collected and attracts more than a nominal fee, may indicate a higher risk of *money laundering*.

16.6 Money laundering, terrorist financing, and proliferation financing warning signs for the Accountancy Sector

Accountants

Overview

61. This section must be read in conjunction with, and is supplemental to, the warning signs set out at Section 6.4 of this Handbook.

62. Article 13 of the *Money Laundering Order* requires a *supervised person* to apply on-going monitoring throughout the course of a business relationship and take steps to be aware of transactions with heightened *money laundering* and *financing of terrorism* risks. The *Proceeds of Crime Law* requires a *supervised person* to report suspicious transactions and activity (see Section 8 of this Handbook).

63. This section highlights a number of warning signs for *supervised persons* providing *accountancy services* to help them decide whether there may be reasons for concern or the basis for a reportable suspicion.

64. *Supervised persons* providing *accountancy services* should have regard both to the sector-specific warning signs set out below and the general indicators described at Section 6.4 of this Handbook, where they may become vulnerable to *money laundering,* the *financing of terrorism,* or the *financing of proliferation*. These warning signs apply both to circumstances that may arise at the start of a business relationship and to those arising during on-going monitoring.

65. Because money launderers, terrorist financers and proliferators are always developing new techniques, no list of examples can be fully comprehensive. However, the following are some key factors indicating activity or transactions which might heighten a *customer's* risk profile, or give cause for concern.

16.6.1 Accountancy and Audit Services

Accountants

16.6.1.1 General warning signs

66. Any of the following general warning signs should prompt additional questions or investigation by those offering *accountancy services* and *audit services*:

- use of many different firms of auditors and advisers for connected companies and businesses
- the client has a history of changing bookkeepers or accountants yearly
- company records consistently reflect sales at less than cost, thus putting the company into a loss position, but the company continues to operate without reasonable explanation of the continued loss.

16.6.2 Tax Advisers

Accountants

67. There are a number of tax offences which can give rise to the proceeds of crime and therefore require the submission of a *SAR* to the *JFCU*. A *tax adviser* is not required to be an expert in criminal law, but they would be expected to be aware of the boundaries between deliberate understatement or other tax evasion and simple cases of error or genuine differences in the interpretation of tax law, and be able to identify conduct in relation to direct and indirect taxation which is punishable by the criminal law.

68. There will however, be no question of criminality where the *customer* has adopted in good faith, honestly and without mis-statement, a technical position with which a revenue authority disagrees.

69. The main areas where offences may arise in relation to direct taxation are:

- tax evasion, including making false returns (including supporting documents), accounts or financial statements or deliberate failure to submit returns; and
- deliberate refusal to correct known errors.

16.6.2.1 Innocent or negligent error

70. It is not uncommon for *tax advisers* to become aware of errors or omissions, in current or past years, from *customer's* tax returns, or any calculations or statements appertaining to any liability, or an underpayment of tax, for example, because a payment date has been missed. If the *tax adviser* has no cause to doubt that these came about as a result of an innocent mistake or negligence, then they will not have formed a suspicion. However, in some cases the *tax adviser* may form a suspicion that the original irregularity was criminal in nature and this will then become a reportable suspicion.

16.6.2.2 Unwillingness or refusal to disclose to a revenue authority

71. Where a *customer* indicates that they are unwilling, or refuse, to disclose the matter to a revenue authority (e.g. HMRC, Revenue Jersey etc) in order to avoid paying the tax due, the *customer* appears to have formed a criminal intent and therefore a reporting obligation arises. The *tax adviser* should also consider whether they can continue to act and should consult their professional body's guidance on such matters. This paragraph applies equally to potential *customers* for whom the *tax adviser* has declined to act.

16.6.2.3 Adjusting subsequent returns

72. Where the legislation permits the correction of small errors by subsequent tax adjustments, and the original error was not attributable to any criminal conduct, then the adjustment itself will not give rise to the need to report, since no crime will have been committed.

16.6.2.4 Intention to underpay

73. A *customer* may suggest that they will, in the future, underpay tax. This would be tax evasion and also a *money laundering* offence when it occurs. A *tax advisor* can and should apply their professional body's normal ethical guidance to persuade the *customer* to comply with the legislation. Should the *customer's* intention in this regard still remain in doubt, the *tax adviser* should consider carefully whether they can commence or continue to act, and if in doubt should seek specialist legal advice. A *SAR* may well be required in such cases.

16.6.2.5 Offences applicable to Value Added Tax

74. A *customer* which is a business resident in the UK or an *EU* Member State will normally be subject to *VAT*. Guidance on the offences applicable to *VAT*, for example fraudulent evasion of *VAT* and production or sending of false documents or statements, is set out in the 'Supplementary Anti Money Laundering Guidance for Tax Practitioners' produced as an appendix to the *AML/CFT* Guidance for the Accountancy Sector released by the UK Consultative Committee of Accountancy Bodies (**CCAB**).

16.6.3 Business recovery or receiverships

Accountants

75. *Insolvency practitioners* will often encounter criminal activity when winding up or effecting recovery for a business. Serious fraud which has resulted in benefit either for the business or an individual will be reportable to the *JFCU* as will incidences where the business has been used to launder the proceeds of crime. Examples may be where:

- fraud has caused or contributed to the failure of the business
- there has been illegal siphoning off or transfer of assets by directors/shareholders
- false accounting or misrepresentation of profits has been applied to maintain share value
- the Directors or members of senior management have been guilty of illegal trading or market abuse
- tax fraud has been committed by reducing income or profits or
- a white knight (a form of hostile takeover defence by a 'friendly' buyer) has invested criminal funds.

16.6.3.1 Observation of unlawful conduct resulting in advice

76. It should be borne in mind that for property to be criminal property, not only must it constitute a person's benefit from criminal conduct, but the alleged offender must know or suspect that the property constitutes such a benefit. This means, for example, that if someone has made an innocent error, even if such an error resulted in benefit and constituted a strict liability criminal offence, then the proceeds are not criminal property and no *money laundering* offence has arisen until the offender becomes aware of the error.

77. Examples of unlawful behaviour which may be observed, and may well result in advice to a *customer* to correct an issue, but which are not reportable as *money laundering*, are set out below:

- offences where no proceeds or benefit results, such as the late filing of company accounts. However, *supervised persons* should be alert to the possibility that persistent failure to file accounts could represent part of a larger offence with proceeds, such as fraudulent trading or credit fraud involving the concealment of a poor financial position;
- mis-statements in tax returns, for whatever cause, but which are corrected before the date when the tax becomes due;
- attempted fraud where the attempt has failed and so no benefit has accrued (although this may still be an offence in some jurisdictions e.g. the UK); and
- where a *customer* refuses to correct, or unreasonably delays in correcting, an innocent error that gave rise to proceeds and which was unlawful, firms should consider what that indicates about the client's intent and whether the property has now become criminal property.

16.7 Reporting Money Laundering and Terrorist Financing activity

Accountants

16.7.1 Further enquiries by auditors

Overview

78. This section is supplemental to and should be read in conjunction with Section 8.2 of this Handbook (Reporting Knowledge or Suspicion).

79. Section 8.2 states that there is a reporting requirement under Article 34D of the *Proceeds of Crime Law* and Article 21 of the *Terrorism Law* to make a *SAR* when there is knowledge, suspicion or reasonable grounds for suspecting that:

- another person is engaged in *money laundering* or the *financing of terrorism*; or
- any property constitutes or represents proceeds of criminal conduct; or
- any property has been, is being or is intended to be used in criminal conduct; or
- any property is or may be terrorist property.

80. Once an auditor suspects a possible breach of legislation which may require a report under the laws referenced above, further enquiries will need to be made. Auditing standards require that when the auditor becomes aware of information concerning a possible breach, the auditor should obtain an understanding of the nature of the act and the circumstances in which it has occurred. Sufficient information should be obtained to evaluate the possible effect on the *customer's* financial statements.

81. However, the *Anti-Money Laundering and Counter-Terrorism Legislation* does not require an auditor to undertake any additional enquiries to determine further details of the predicate criminal offence (i.e. the offence giving rise to the proceeds of crime). To help mitigate the risk of tipping-off, it is important that any further enquiries only represent steps that the auditor would have performed as part of the normal audit work and that the *MLRO* (or *deputy MLRO*) is consulted before any further enquiry is performed. If an employee of the auditor is genuinely uncertain as to whether or not there are grounds to make a *SAR*, they may wish to seek advice from their *MLRO* (or *deputy MLRO*).

82. During the course of the audit work, the auditor might obtain knowledge or form a suspicion about a proposed act that would be a criminal offence, but has yet to occur. Because attempting or conspiring to commit a *money laundering* offence is itself a criminal act, a *SAR* may need to be made in some circumstances.

83. Where the auditor makes an internal *SAR* to the *MLRO* (or *deputy MLRO*) and it is decided that further enquiry is necessary, the *auditor* will need to be made aware of the outcome of the enquiry to determine whether there are any implications for the audit report or the decision to accept reappointment as auditor.

84. The auditor will need to consider whether continuing to act for the *customer* could itself constitute a *money laundering offence*. For example, if it amounted to aiding or abetting the commission of one of the principal *money laundering* offences such as becoming involved in an arrangement. In those circumstances the auditor may wish to consider resigning, but should first contact their *MLRO* (or *deputy MLRO*) in order to report the suspicion and seek guidance in respect of tipping-off. If the auditor wishes to continue to conduct the audit, appropriate consent may be required from the *JFCU*.

85. Partners and employees of *supervised persons* carrying on *audit services* will need to follow their internal reporting procedures when considering whether to include documentation relating to *money laundering* reporting in the audit working papers.

16.7.2 Auditor's responsibility for monitoring compliance

Accountants

Overview

86. The International Standard on Auditing's Policy Paper ISA 250 establishes standards and provides guidance on the auditor's **responsibility to consider legislation** in an audit of financial statements. The *Anti-Money Laundering and Counter-Terrorism Legislation* does not require the auditor to extend the scope of an audit except as set out in Section 16.7.3 below, but regular audit work could still give rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion, that will need to be reported. Such knowledge or suspicion may arise in relation to:

    - legislation linked directly to the preparation of the financial statements
    - legislation which provides a legal framework within which the *customer* conducts its business and
    - other legislation.

87. Auditing standards relating to legislation require the auditor to obtain sufficient appropriate audit evidence regarding **compliance** with the legislation that has an effect on the determination of material amounts and disclosures in the financial statements. This may result in the auditor becoming suspicious that, for example, fraud or tax offences have taken place, which may be criminal offences resulting in the acquisition of criminal property.

88. Auditing standards on legislation also require the auditor to carry out procedures to help identify possible or actual instances of **non-compliance** with the legislation which provides a legal framework within which the *customer* conducts its business and is therefore central to its financial statements. These procedures involve:

    - obtaining a general understanding of the legal and regulatory framework applicable to the *customer* and it's wider industry, and of the procedures followed to ensure compliance with that framework
    - inspecting correspondence with the relevant licensing and regulatory authorities
    - making enquiries to the Board/senior management of the *customer* as to whether they are on notice of any such possible instances of **non-compliance** with those laws or regulations and
    - obtaining written representation that the Board/senior management have disclosed to the *auditor* all known actual or possible instances of **non-compliance** with legislation whose effects should be considered when preparing financial statements, together with - where applicable - the actual or contingent consequences which may arise from the **non-compliance** (i.e. regulatory fines, public censure etc).

89. This work may give the *auditor* grounds to suspect that criminal offences have been committed and which may need to be reported to the *JFCU*.

90. If the *customer* falls within the definition of a *financial services business*, legislation relating to *money laundering* will be central to the operation of their business. When auditing the financial statements of such *customers*, the *auditor* must review the steps taken by the *customer* to comply with the *Money Laundering Order* and the *JFSC's* other regulatory requirements, assess their effectiveness and obtain Board/*senior management* representations concerning compliance with them. If the *customer's systems and controls* (including *policies and procedures*) appear to be ineffective, the *auditor* must consider whether there is an obligation to report a matter of "material significance" to the *JFSC* and the possible impact of any regulatory action which may arise from the same (see Section 16.7.3 of this Handbook for further information).

91. The *auditor* will need to give consideration to whether any **contingent liabilities** may arise in this area. For example, there may be criminal fines for **non-compliance** with the *Anti-Money Laundering and Counter-Terrorism Legislation*. In certain circumstances, civil claims or confiscation proceedings may occur, giving rise to contingent liabilities. The *auditor* will also need to remain alert to the fact that discussions with the *customer* on such matters may create a risk of tipping off (see Section 8.5 of this Handbook).

92. In some situations, the *auditor's customer* may have obtained legal advice to the effect that certain actions or circumstances do not give rise to criminal conduct and therefore cannot give rise to criminal property. Determining whether an act constitutes **non-compliance** with the *Anti-Money Laundering and Counter-Terrorism Legislation* may involve consideration of matters which do not lie within the competence and experience of the *auditor*. As a result, provided that the *auditor* considers that the advice has been obtained from a suitably qualified and independent lawyer and the lawyer was made aware of all relevant circumstances known to the *auditor*, then the *auditor* may rely on such advice, provided the *auditor* has complied with auditing standards on using the work of an expert.

16.7.3 Reporting to regulators

Accountants

Overview

93. Making a *SAR* to the *JFCU* does not relieve the *auditor* of its other statutory reporting duties. Examples of these responsibilities include:

- **audits of *customers* carrying on *financial services business*:** The *auditor* has a statutory duty to report matters of "material significance" to the *JFSC* which come to the *auditor's* attention in the course of its audit work
- **audits of *customers* in the public sector:** A*uditors* of some *customers* which operate in the public sector may be required to report on the *customer's* **compliance** with regulatory requirements around financial transactions. Activity connected with *money laundering* may constitute a breach of those requirements
- **audits of other types of *customer*:** A*uditors* of some other types of *customers* are also required to report matters of "material significance" to regulators (for example, charities and occupational pension schemes).

16.7.4 Balancing Professional Work and Post-Reporting Requirements

Accountants

Overview

94. Continuation of audit work following the submission of an external *SAR* may require discussion of matters relating to the suspicions that were formed with the *customer's* Board/*senior management*. Care must be taken to select appropriate and non-complicit members of the Board/*senior management* for such discussions, keeping in mind the need to avoid tipping-off. It is important to confine enquiries to those required in the ordinary course of business and not attempt to further investigate a matter reported upon, unless this is within the scope of the professional work commissioned.

95. In more complex circumstances, consultation with the *JFCU* may be necessary before enquiries are continued. It should be noted that neither the *JFCU* nor other law enforcement agencies may give consent to tipping-off.

96. *Supervised persons* carrying on audit business may wish to engage their *MLRO/deputy MLRO* or another suitable specialist (for example a lawyer) if there are tipping-off concerns. In particular, it is important that before any document referring to the subject matter of a *SAR* is released to a third party, the *MLRO* (or *deputy MLRO*) is consulted along with, where necessary, law enforcement. Some typical examples of documents released to third parties include but are not limited to:

- public audit or other attest reports
- public record reports to regulators
- confidential reports to regulators
- statements on the resignation of a *supervised person* as *auditor*
- professional clearance/etiquette letters or
- communications to *customers* of a *supervised person's* intention to resign.

97. There is no legal mechanism for obtaining consent from the *JFCU* regarding the contents of statements or other documents relating to an *auditor's* resignation. However in complex cases, *supervised persons* carrying on audit business may still wish to discuss the matter with the *JFCU* in order to understand their perspective and document such discussion.

98. *MLRO*s may on occasion need advice to assist them in formulating their instructions to the *supervised person*. Legal advice may be sought from a suitably skilled and knowledgeable professional legal adviser, and recourse may also be had to helplines and support services provided by professional bodies. Discussion with the *JFCU* may well be valuable, but *MLRO*s should bear in mind that the *JFCU* and law enforcement are not able to advise, nor are they entitled to dictate, how professional relationships should be conducted.

16.7.5 Auditor's report on financial statements

Accountants

Overview

99. Where it is suspected that *money laundering* or the *financing of terrorism* has occurred, the auditor will need to apply the concept of materiality when considering whether the auditor's report on the *customer's* financial statements needs to be qualified or modified, taking into account whether:

- the crime itself has a material effect on the financial statements
- the consequences of the crime have a material effect on the financial statements or
- the outcome of any subsequent investigation by the investigating agencies may have a material effect on the financial statements.

100. If it is known that *money laundering* or the *financing of terrorism* has occurred and members of the *customer's* Board or *senior management* were knowingly involved, the *auditor* will need to consider whether their report will include a qualified opinion on the financial statements disclosing the same. Any such disclosure in the auditor's report will be subject to the tipping off requirements set out at Section 8.5 of this Handbook. It might be necessary for the *auditor*, through the *MLRO* (or *deputy MLRO*), to discuss with the relevant law enforcement agency whether disclosure in their report on the financial statements could constitute a tipping-off offence. If so the auditor, through the *MLRO* (or *deputy MLRO*), will need to seek guidance on an acceptable form of words with the *JFCU*.

101. As noted at Section 8.4 of this Handbook, the *JFCU* is not able to advise or instruct in respect of a *supervised person's* professional conduct. Auditors must therefore bear this in mind when discussing a potential form of words with the *JFCU* which can then be used in communicating with the *customer*. In circumstances like these, the auditor may also wish to consider seeking legal advice in order to reduce the risk of committing a tipping off offence.

102. A delay in issuing the audit report pending the outcome of an investigation may not be practicable for the auditor and could itself create a risk of tipping off.

103. If it is concluded that a qualified audit report must be issued, the *supervised person* may need to seek legal advice before issuing the report. In exceptional circumstances, it may be necessary to make an application to the court in respect of the content of the qualified audit report.

16.7.6 Resignation as auditor

Accountants

104. If an auditor, having filed a *SAR*, wishes to terminate a *business relationship* and is concerned that in doing so it may prejudice an investigation, it should seek guidance from the *JFCU*. This will help reduce the risk of tipping-off. However, the *JFCU* cannot instruct a *supervised person* to continue a *business relationship* that it wishes to terminate.

105. An auditor may wish to resign if it is believed that the *customer* or an employee of the *customer* is engaged in *money laundering*, the *financing of terrorism*, or any other illegal act, particularly where a normal relationship of trust can no longer be maintained. Where the auditor intends to resign, there may be a conflict between the requirements to bring certain matters to the attention of the *customer's* members or creditors and the risk of tipping-off. In such circumstances the auditor should seek guidance from the *JFCU* and the appropriate investigating agency to discuss an appropriate course of action and an acceptable form of words. If necessary, legal advice or the direction of the court may need to be sought.

106. The risk of tipping-off may also cause a conflict with the need to communicate with the prospective successor auditor in accordance with ethical requirements relating to changes in professional appointments. Whilst the existing *auditor* might feel obliged to advise the incoming auditor of their suspicions of *money laundering,* the *financing of terrorism*, or any other illegal act, to do so would run the risk of tipping-off. Expressing suspicions orally rather than in writing **does not** constitute a mitigation of the tipping-off risk. In circumstances where it is considered necessary to communicate the underlying circumstances which gave rise to the *SAR*, guidance should be sought from the *MLRO* (or *deputy MLRO*) who may then need to seek an opinion from the *JFCU*.

17 PRESCRIBED NON-PROFIT ORGANISATIONS

Key

The below table is applicable to Section 17 of this Handbook concerning Prescribed NPOs only:

Section	Colour	Obligation explained
Section heading	**Blue**	Relates to Prescribed NPOs only
Sub heading	**Grey**	Relates to Prescribed NPOs only
Statutory requirements	**Light blue**	Mandatory for Prescribed NPOs only
Codes of Practice	**Magenta**	Mandatory for Prescribed NPOs only
Guidance notes	**Green**	Guidance for Prescribed NPOs only

17.1 Introduction

1. This section replicates the statutory requirements of the *Prescribed NPO Order* using paraphrased wording.

2. Prescribed Non-Profit Organisations (***Prescribed NPOs***) are *supervised persons* under Article 1 of *the Supervisory Bodies Law*. They are therefore subject to supervision by the *JFSC* for compliance with the *Prescribed NPO Order.*

3. *Prescribed NPOs* is a sub-section of the non-profit sector which has been identified as being at a heightened risk and vulnerability of being abused for *terrorist financing* purposes.

4. Article 1 of the *Prescribed NPO Order* advises that a *NPO* will be considered a *Prescribed NPO* where, during the preceding 12 months it has:

   › raised NPO Funds exceeding £1,000 from outside Jersey, Guernsey, the Isle of Man, England and Wales and Scotland, or

   › disbursed NPO Funds exceeding £1,000 outside those jurisdictions.

5. The *JFSC* will apply a risk-based approach to determine how a *Prescribed NPO* is supervised for compliance with the *Prescribed NPO Order* and Section 17 of *the Handbook*. See the NPO Section of our website for more details.

6. *Prescribed NPOs* are required by the *Prescribed NPO Order* to:

   › prepare an annual financial statement, and make it available to the JFSC upon request

   › have appropriate systems and controls to ensure that NPO Funds are fully accounted for

   › keep records of NPO Owners and Controllers

   › keep records of significant donors, and

   › take reasonable steps to identify, obtain information on, and confirm that its associate NPOs and NPO Beneficiaries are not assisting, or being used to assist, terrorist activities.

7. Parts of this section headed “Statutory Requirements” and “Codes of Practice” **are mandatory** and *Prescribed NPOs* are required to comply with them. Parts of this section headed “Guidance notes” **are not mandatory** and provide examples of how *Prescribed NPOs* might demonstrate compliance with the requirements of the *Prescribed NPO Order* and *Codes of Practice*.

8. Unless otherwise stated:

   a. the *AML/CFT/CPF Codes of Practice* set out in Sections 2-16 of *the Handbook* do not apply to *Prescribed NPOs*.

   b. *Prescribed NPOs* need to apply the requirements of the *Prescribed NPO Order* and Section 17 of *the Handbook* to all of their relationships with *NPO Beneficiaries* and *associate NPOs*, not just those which are connected to higher risk jurisdictions.

9. Other acceptable methods of complying with the *Prescribed NPO Order* and *Codes of Practice*, outside those described in the *Guidance notes*, may be possible provided they are equally as robust in demonstrating compliance with the mandatory requirements.

10. A *Prescribed NPO* should apply a risk-based approach to determine what kind of measures might be appropriate to demonstrate compliance with the *Prescribed NPO Order* and *Codes of Practice*.

11. Whether any particular measure outside those described in the *Guidance notes* is in compliance with the mandatory requirements will be determined on a case-by-case basis. A *Prescribed NPO* will be expected to demonstrate how the measure applied is equally as robust. This may be facilitated, for example, by documenting how the specific measure meets the requirements of the *Prescribed NPO Order* and *NPO Beneficiary*.

17.2 Vulnerabilities of Prescribed NPOs

Overview

12. The April 2022 the National Risk Assessment for NPOs (the ***NPO NRA***) identified around 11% of Jersey-based *NPOs* as being particularly vulnerable to being abused for *terrorist financing purposes*.

13. This sub-sector of *NPOs* may be more vulnerable to *terrorist financing* abuse due to one or more of the following factors:

- operating in higher-risk jurisdictions, such as conflict zones, failed states and disaster areas, where support such as humanitarian aid and disaster relief is desperately needed, and which equally are areas where terrorists also are known to undertake activities
- using associate NPOs
- using money remittance methods, such as hawala and cash, which may render the tracing of funds to legitimate NPO Beneficiaries more challenging.

14. *Diversion* is the principal way in which *NPOs* may be abused for *terrorist financing*. The Glossary of *the Handbook* defines *Diversion* as "transactions by *NPO Representatives* or external parties such as *associate NPOs* that divert funds away from the *NPO's* legitimately intended purposes to a terrorist, terrorist cell or terrorist organisation for them to benefit from, directly or indirectly".

15. Examples of how *Diversion* may take place include:

- terrorists posing as legitimate NPO Beneficiaries to benefit from NPO programmes, such as receiving NPO Funds
- terrorists appearing to act as ordinary associate NPOs, at the same time as abusing NPO Resources by diverting NPO Funds to support their activities.

16. *Diversion* risk may increase where a *NPO*:

- does not properly invest in its terrorist financing risk control framework on grounds of cost
- is too focused on assisting NPO Beneficiaries at the expense of accountability or effective risk management
- has a high risk appetite, and a low level of terrorist financing risk controls
- takes the view that if no incidents are reported, or that the diverted value is small, the risk of terrorist financing abuse is negligible. It is worth reflecting that even when utilising small amounts, a bad actor can cause great harm. For example, the cost of assembling a dangerous homemade explosive device can require only a relatively small amount of funds.

17. *Diversion* risk can also increase where a *NPO* does not adequately manage "transfer risk", i.e. the risk that *Diversion* will take place where funds are transferred to *associate NPOs*. High-quality *associate NPOs* can reduce *terrorist financing* risk, with their local knowledge and relationships providing an additional level of information and control to the *NPO*. However, poor due diligence can increase the *terrorist financing* risk. Some *associate NPOs* may be sympathetic to, infiltrated by, or under the control of, terrorist elements. Alternatively, they may not have strong *terrorist financing* controls and may inadvertently finance terrorist activities.

18. Ceding control of funds does not cede responsibility for their destination. *Associate NPO* selection, due diligence and oversight forms a crucial part of responsible *NPO* activity.

19. The offence of *terrorist financing* is broad in nature and scope. For the purposes of *the Handbook*, it is defined as:

- Conduct which is an offence under any provision of Articles 15, 16 and 16A of the Terrorism (Jersey) Law 2002 (the Terrorism Law)
- Conduct outside Jersey which, if occurring in Jersey, would be an offence under Articles 15, 16 and 16A of the Terrorism Law
- Conduct which is an offence under any provision of Article 21 of the Terrorism Law
- Conduct which is an offence under any provision of Parts 3, 4 and 6 of the Sanctions and Asset-Freezing (Jersey) Law 2019 (the Sanctions and Asset-Freezing Law).

17.3 Risk-based approach

Statutory requirements (paraphrased wording)

20. *Article 6 of the Prescribed NPO Order requires a Prescribed NPO to take reasonable steps to:*

- *identify its associate NPOs and NPO Beneficiaries*
- *obtain information about:*
  - *the activities of each associate NPO and NPO Beneficiary, and*
  - *the nature and purpose of its relationship with each associate NPO and NPO Beneficiary and*
- *confirm, so far as possible, that its associate NPOs and NPO Beneficiaries are not assisting or being used to assist terrorism or the financing of terrorism.*

21. *In Article 6:*

- *"associate NPO" means an NPO with which the Prescribed NPO collaborates or works jointly in carrying out its activities*
- *"beneficiary" means a person who receives assistance through the activities of the Prescribed NPO.*

17.3.1 NPO programme risk assessment (NPO PRA) and associated *activities*

Codes of Practice

22. A *Prescribed NPO* must assess and mitigate the risk of being used to assist terrorism, or the *financing of terrorism*.

23. A *Prescribed NPO* must define and document their approach to *Diversion* risk in a risk appetite statement.

24. A *Prescribed NPO* must have internal systems and controls in place to mitigate *Diversion* risks.

Guidance notes

25. *Prescribed NPOs* are expected to apply enhanced controls to demonstrate that they are effectively identifying, assessing, managing and mitigating *terrorist financing* risks. These risks may include, but are not limited to:

- operating in jurisdictions with higher terrorist financing risks, such as those identified in Appendix D2 of this Handbook, including, for example, conflict zones, failed states, and disaster areas
- utilising certain payment remittance methods which fall outside the formal banking system, such as Hawala, mobile money, preloaded cards, virtual assets, cash (outside Jersey) etc.
- funds being diverted from intended beneficiaries of the NPO programme to any other third party with weak terrorist financing controls.

26. A risk-based approach is not intended to prevent or obstruct aid from reaching legitimate *NPO Beneficiaries*. It is a way of ensuring it reaches them in the safest way. Transparency is critical for mitigating *diversion* risk. Without assessing risk in a meaningful way, it is not possible to ascertain if the systems and controls in place are effective. Adequate systems and controls can also safeguard the non-profit sector, and Jersey, from reputational damage. Robust controls provide confidence to donors, financial institutions, such as banks, and the regulator. It can also mitigate civil litigation from donors.

27. A risk-based approach can be established through the completion of a *NPO* programme risk assessment (***NPO PRA***). These should be undertaken by the charity governors, board members, trustees, senior officers (or equivalent, whether or not they are remunerated). The *NPO PRA* should be:

- undertaken as soon as reasonably practicable before the NPO commences the programme, and
- recorded to assist the NPO in demonstrating its rationale.

28. Whilst it is the responsibility of each *Prescribed NPO* to identify and define their NPO programme(s) of activity, examples may include:

- the delivery of food parcels to rural communities in X country
- providing emergency shelters and supplies to victims of an earthquake and tsunami in Y country
- funding of an animal shelter in Z country.

29. A *Prescribed NPO* may consider it appropriate to conduct a separate risk assessment for each *NPO* programme of activity undertaken. This might be appropriate where only one *NPO* programme of activity is conducted at a time.

30. Where a *Prescribed NPO* undertakes a large number of *NPO* programmes simultaneously, e.g. aid operations in multiple countries, it may be more suitable to conduct one *NPO PRA* for the whole body of work conducted.

31. A *NPO PRA* should be reviewed at any point where there is a perceived change in the risk profile of the *NPO* programme(s) which have been assessed (e.g. if civil unrest develops in the region where the *NPO* programme is taking place)

32. The *NPO PRA* should have regard to all relevant risk factors. These may include, but are not limited to:

- the nature, scale, complexity and the diversity of its operations (including geographical diversity), the volume and size of its transactions, and the degree of risk associated with each area of its operation
- jurisdictions, territories or areas where it is not uncommon that terrorist organisations may demand that people they direct should be involved in a NPO programme, for example where the terrorists may be political actors, or where terrorists otherwise control the area
- operating in environments where gifts form part of cultural interactions, and where terrorist organisations may exert pressure to comply with such donations
- operating in environments where taxes and fees are collected by terrorist organisations or their sympathisers, and where this is a known and regular occurrence
- location remoteness and intensity of local conflict and factions, potentially intensified by legitimate security and policing forces not having a presence
- carrying out distribution work in jurisdictions, territories or areas that are controlled by terrorist organisations where the NPO may be directed or demanded to provide aid to certain parties
- the characteristics of activities and services the NPO offers, and the associated vulnerabilities posed by each activity and service
- any degree of third party involvement in the NPO programme, including, for example, using associate NPOs
- jurisdictions, territories or areas where NPOs require the support of local associate NPOs to be able to operate safely and where terrorist organisations have political support and influence
- circumstances where it is difficult to adequately screen a person's background or establish their associates
- any risk presented by the Prescribed NPO's donors or NPO Beneficiaries
- any risk presented by the technology utilised by the Prescribed NPO, including communications channels, fund-raising platforms and payment mechanisms
- being the target of a cyber-attack, such as through phishing. An example of a cyber-attack might be where an attacker sends an e-mail to the Prescribed NPO, pretending to be from

one of their suppliers. The e-mail includes an invoice and states that the supplier has changed their bank and requires the NPO to amend the account details of where to send payments. The invoice has been doctored and the new account details are those of the attacker. The money is then transferred directly to the attacker, potentially for the benefit of terrorists.

33. When conducting a *NPO PRA* care should be taken not to focus too much on any single factor. All aspects of the political, economic, geographical, technological, social and sanction risk environment in the area of the *NPO's* operations should be considered. *Prescribed NPOs* should also take into account any risks identified by a *NPO NRA,* or similar documents.

34. Risk should also be considered on a cumulative basis. The overall exposure from all risks aggregated together may be greater than if they were each considered individually.

35. An example of a *NPO PRA* checklist can be downloaded from our website and modified, as appropriate: draft programme risk assessment checklist. This template is not intended to be rigid or prescriptive. A *NPO* may wish to make amendments to the checklist to account for the specific risks relevant to its activities.

36. To support the assessment of risks presented by a particular *NPO* programme of work, it may be appropriate to prepare a risk appetite statement. This statement sets out what level of *terrorist financing* risk the *Prescribed NPO* is prepared to tolerate. A clear position, set out in writing, can assist a *Prescribed NPO* in deciding whether a proposed *NPO* programme of work creates too much risk exposure to be undertaken.

37. It is our expectation that a risk appetite statement should confirm, at a minimum, that the *Prescribed NPO* will not tolerate *diversion*, nor parties that enable *diversion*. It may also consider and discuss:

- whether there are certain jurisdictions, territories or areas in which the NPO is comfortable to operate, such as where it has previous experience and is engaged with known associate NPOs. There may be other places where the NPO is unwilling to operate
- if the Prescribed NPO will avoid certain routes or geographical areas, or particular relationships, or the use of certain payment methods (e.g. cash, pre-paid cards, hawala, mobile money, virtual assets etc.)
- if working alongside certain associate NPOs falls outside the NPO's risk appetite
- what contractual arrangements and terms it will be prepared to put in place working with an associate NPO, for example seeking undertakings of non-tolerance for diversion
- what types of donors it will accept funding from
- who it will distribute benefits to and where
- certain conflict levels which it will not tolerate, such as delivering aid in an active warzone.

38. When preparing the *NPO PRA* and risk appetite statement, it is important to recognise that a *NPO's* risk management capabilities are not always transferrable from one *NPO* programme to another. If adequate safeguards cannot be put in place regarding a particular *NPO* programme, it should be considered whether another *NPO,* with greater capability, ought to carry out the *NPO* programme instead.

39. A *Prescribed NPO* may consider that it is able to establish a risk-based approach through methods other than conducting a *NPO PRA,* and/or risk appetite statement. In these circumstances, the *Prescribed NPO* is expected to demonstrate how its alternative measures achieve the same outcome as those set out above.

40. Where a *Prescribed NPO* is receiving services from a regulated *TCSP* (as defined in Section 4.4.5 of *the Handbook*), it may be appropriate for the regulated *TCSP* to add the output of the *NPO PRA* and risk appetite statement to their own *BRA* (see Section 2.3.1 of *the Handbook*).

41. A regulated *TCSP* may also consider it appropriate to integrate any periodic testing of the *Prescribed NPO's* systems and controls into the testing undertaken for their *TCSP* business (see Section 2.4.2 of *the Handbook*).

17.3.1.1 Prescribed NPOs solely remitting to charities in equivalent jurisdictions

42. For guidance in terms of what is meant by an equivalent jurisdiction, see Appendix B of *the Handbook*.

43. A number of *NPOs* established in Jersey conduct no activity apart from disbursing funds to charities which are operating in equivalent jurisdictions. Examples of this type of operating model include:

- a faith-based NPO sending funds to a larger faith-based organisation, based in an equivalent jurisdiction, which conducts mission activities across the world
- a Jersey branch of a global aid organisation sending funds to its headquarters based in an equivalent jurisdiction.

44. When conducting their *NPO PRA* (or equivalent), *Prescribed NPOs* undertaking no activity apart from disbursing funds to charities which are operating in equivalent jurisdictions, should take into account the following factors:

- what jurisdictions does the recipient organisation operate in?
- how has the Prescribed NPO concluded that the country in which the recipient organisation operates is an equivalent jurisdiction (see Sections 1.8.2 and 1.8.3 and Appendix B of the Handbook for further guidance)?
- will the funds sent by the Prescribed NPO be applied for a specific purpose, or does the recipient organisation have the freedom to apply the funds to whatever activities it sees fit?
- what assurances has the recipient organisation given in terms of their systems and controls to mitigate the risk of Diversion?

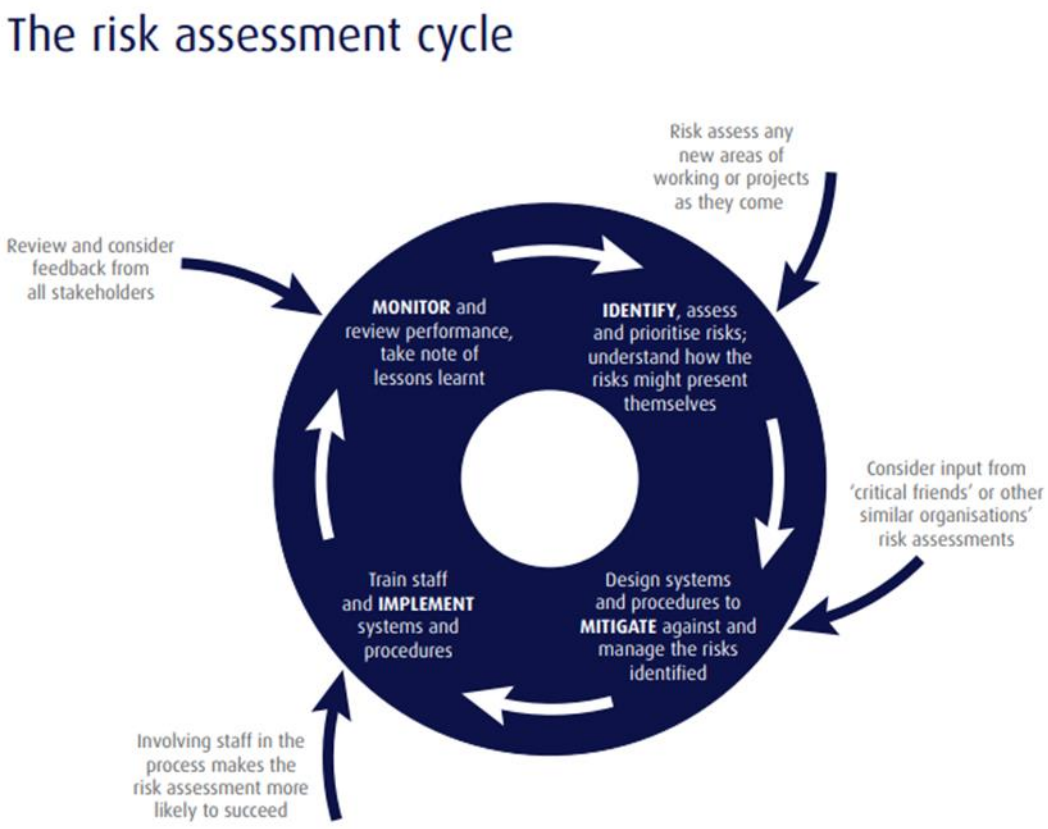
45. Set out below is a case study demonstrating how a *Prescribed NPO* acting in this manner might carry out their *NPO PRA* (or equivalent):

- a Prescribed NPO has been established to raise funds in Jersey, in order to support a charity based abroad which rescues and rehomes stray dogs from across the world. That charity operates in a number of higher-risk jurisdictions for terrorist financing purposes as per Appendix D2 of the Handbook.
- the Prescribed NPO sends NPO Funds to the charity with no caveats in terms of how it should be applied, and the charity is free to use the money as it chooses

- the Prescribed NPO is aware of the risk that the NPO Funds they have donated may be diverted for terrorist financing purposes once they reach the higher-risk jurisdictions. Therefore, they ask the charity to provide details of their systems and controls to counter terrorist financing. This may include speaking with the charity's Head of CFT, reviewing their policy manual and finding out who their associate NPOs are. The Prescribed NPO may also consider the track record of the charity and their associate NPOs through a search for adverse news articles on Google. The Prescribed NPO may check that the charity remains in good standing with the regulator in the jurisdiction where the charity is supervised
- after considering the above, the governing body of the Prescribed NPO decides they are satisfied that the charity has sufficient controls to mitigate the risk of Diversion. The Prescribed NPO records their checks, and the rationale for their decision, in their NPO PRA and proceed to remit NPO Funds to the charity
- As part of their ongoing risk monitoring, the governing body of the Prescribed NPO decides to check for adverse news articles on the charity via Google on an annual basis.

17.3.2 Ongoing risk monitoring

46. Risk monitoring of a *NPO* programme is a dynamic and cyclical process. It ensures that any new risks are addressed as they arise and establishes how previously identified risks may have changed. The below diagram from the UK Charities Commission illustrates the risk assessment cycle:



47. A *Prescribed NPO* may demonstrate that *terrorist financing* risks are being monitored on an on-going basis by:

- ensuring that the identification, assessment, management and mitigation of risk is linked to the achievement of the Prescribed NPO's operational objectives
- ensuring that the assessment process reflects the charity governors', Board members', trustees', senior officers' (or equivalent, whether or not they are remunerated) view of acceptable risk
- reviewing and considering the results of risk identification, evaluation and management
- considering the risks attached to significant new activities or opportunities
- considering external factors, such as new legislation, sanctions or regulations
- considering the financial impact of risk as part of budget planning
- documenting how the charity governor's, board member's, trustee's, senior officers (or equivalent, whether or not they are remunerated) have decided how the identified risks should be treated and managed.

48. A *Prescribed NPO* may demonstrate they are adequately monitoring risk by keeping records of their monitoring activities in a *Diversion* risk register. An example of a *Diversion* risk register can be downloaded from our website: draft diversion risk register template.

49. This template is not intended to be rigid or prescriptive. A *Prescribed NPO* may decide, with reference to its *NPO PRA* and/or risk appetite statement (or equivalents) that it should carry out monitoring on more, less or different risks than those listed in the template *Diversion* risk register.

50. When completing the *Diversion* risk register, a *Prescribed NPO* should refer to their *NPO PRA* and/or risk appetite statement (or equivalents) to help them conclude the risk level of a particular area, and what controls should be put in place. For example:

- a risk area assessed as low risk may only need minimal controls
- a risk area assessed as medium risk may need some additional controls and
- a higher risk activity may need significant additional controls. If it is judged that the risk cannot be mitigated by the Prescribed NPO to an acceptable level, it would be appropriate to leave this work to another party that can effectively manage the risk.

51. It is recommended that a periodic review of a *NPO's* risks is conducted at least annually. Through the application of a risk-based approach, it can be determined whether certain risks should be monitored more or less frequently. For example:

- A Prescribed NPO whose sole activity is disbursing funds to a reputable charity which only carries out activity in an equivalent jurisdiction may only need to review their exposure to higher-risk jurisdictions on an annual basis; for example by seeking confirmation from the overseas charity that it continues to only act within their home jurisdiction
- If a Prescribed NPO is supporting displaced persons in a country undergoing civil conflict its activity is potentially exposed to the risk of being extorted for a portion of the NPO Funds to gain access to the NPO Beneficiaries. In this case it would be more appropriate to monitor the risk of association with a target of financial sanctions related to terrorism on a more regular basis at an interval that is appropriate in the circumstances, e.g. quarterly.

52. In all cases, the outcome of periodic reviews should be documented. A *Prescribed NPO* should be able to explain and justify why it has chosen to conduct its risk monitoring in a certain manner, and at a certain interval.

17.4 NPO Beneficiaries, Associate NPOs and donors

17.4.1 NPO Beneficiaries

Statutory requirements (paraphrased wording)

53. *Article 6 of the Prescribed NPO Order requires a Prescribed NPO to take reasonable steps to:*

- *identify its associate NPOs and NPO Beneficiaries*
- *obtain information about:*
  - *the activities of each associate NPO and NPO Beneficiary and*
  - *the nature and purpose of its relationship with each associate NPO and NPO Beneficiary and*
- *confirm, so far as possible, that its associate NPOs and NPO Beneficiaries are not assisting or being used to assist terrorism or the financing of terrorism.*

Overview

54. *NPO Beneficiaries* are defined in the Glossary above. As noted, this term captures natural persons, as well as groups of natural persons.

55. For the purposes of *the Handbook,* a *Prescribed NPO* establishes a relationship with an *NPO Beneficiary*.

56. To comply with the *Prescribed NPO Order*, a *Prescribed NPO* will need to apply a level of due diligence on its *NPO Beneficiaries*. The due diligence in this respect is not intended to follow that of financial services businesses, since this would not be proportionate, nor appropriate. Instead, the *NPO* should identify its *NPO Beneficiaries* by applying a risk-based approach.

57. In the context of *NPO Beneficiaries*, a risk-based approach means applying sufficient measures, having regard to the *NPO PRA* and risk appetite statement (or equivalent documents), to be satisfied that the *NPO Beneficiary* is not involved in terrorism or *terrorist financing*. A higher level of risk may require more stringent measures to be applied, whilst a lower level of risk might require less.

58. Throughout Section 17 of *the Handbook*, it may be relevant for a *Prescribed NPO* to refer to other sections of this Handbook for additional guidance. When reviewing these sections, a *Prescribed NPO* should consider the term 'customer' to refer to *NPO Beneficiaries*.

59. Where a *Prescribed NPO* is receiving services from a regulated TCSP (as defined in Section 4.4.5 of *the Handbook*) and it is considered appropriate to do so, the *NPO* may choose to apply due diligence measures which are aligned with those set out in Sections 3 and 4 of *the Handbook*.

Guidance notes – Identifying NPO Beneficiaries

60. Where an *NPO Beneficiary* is **a single person**, a *Prescribed NPO* may demonstrate that it has taken reasonable measures to identify that person where it obtains the following information:

- Name
- Date of birth (if possible)
- Country of birth
- Current area of residence.

61. The amount of identity information requested may differ based on the outcome of the *NPO PRA* (or equivalent).

62. Identity information for an individual may be obtained directly from the *NPO Beneficiary*, or their representative.

63. Where an *NPO Beneficiary* is **a group of persons**, for example refugees from a particular conflict, there is no requirement to identify each individual person.

64. In these cases, the *Prescribed NPO* may demonstrate that is has taken reasonable measures to identify the group if the characteristics of that group are consistent with the purpose and objectives set out in the *Prescribed NPO's* constitutional documents (or their equivalent).

65. For example, if the *Prescribed NPO's* constitutional documents state that its objective is to provide humanitarian support to victims of conflict, this would be consistent with a group of *NPO Beneficiaries* who are a group of refugees from such conflicts.

66. However, the *Prescribed NPO* should be alive to the fact that different classes of *NPO Beneficiaries* will present different levels of risk from a *terrorist financing* perspective based on their location and proximity to terrorist organisations etc.

67. Identity information for a group of persons may be obtained from a representative of that group.

Guidance notes – Nature and purpose of relationship with NPO Beneficiary

68. As part of its reasonable measures in respect of *NPO Beneficiaries*, a *Prescribed NPO* will need to obtain information on the nature and purpose of their relationship with the *NPO Beneficiary.* It should do this by requesting and documenting the information at the establishment of the relationship.

69. The "nature" of a relationship may include:

- the amount and type of NPO funds which would be applied to the NPO Beneficiary/(-ies)
- whether any associate NPOs are involved, and their purpose.

70. The "purpose" of a relationship may include:

- what the activity is aiming to achieve, such as building a pump to provide a rural community with access to clean water or distributing food to victims of a drought.

Guidance notes – Confirming NPO beneficiaries are not involved in terrorism

71. Where a *NPO Beneficiary* is a single person, a *Prescribed NPO* may demonstrate that it has taken reasonable measures to confirm that person is not assisting, or being used to assist, terrorism/the *financing of terrorism,* where it takes steps to ascertain whether the person is a legitimate *NPO Beneficiary*. Such steps may include:

- seeking a reference from an independent person to corroborate the information provided by or regarding the *NPO Beneficiary*. For example, if the *NPO Beneficiary* is a child staying in an orphanage, the reference should confirm that the child is in fact staying there
- visiting the location where the *NPO Funds* will be applied to consider whether the amount(s) to be applied appear reasonable given what is proposed to be done with them
- considering if the amount(s) to be applied to the *NPO Beneficiary* makes sense when compared to previous relationships with similar characteristics
- reviewing the correspondence held with the *NPO Beneficiary*, their representatives and relevant *associate NPOs*, then considering if the proposed relationship makes sense based on what they have said

72. Where a *NPO Beneficiary* is a group of persons, for example refugees from a war zone, there is no requirement to obtain a confirmation for each individual person. The *Prescribed NPO* should still take account of the particular characteristics of the group of *NPO Beneficiaries* when preparing its *NPO PRA* (or equivalent).

73. In these cases, the *Prescribed NPO* may demonstrate compliance with the *Prescribed NPO Order* by taking measures to ensure the group of persons are legitimate *NPO Beneficiaries*. This may be achieved by, for example:

- visiting the location where the *NPO Funds* will be applied and by considering whether the amount(s) to be applied appear to be reasonable given what is proposed to be done with them
- considering if the amount(s) to be applied to the group of *NPO Beneficiaries* makes sense when compared to previous relationships with similar characteristics
- reviewing the correspondence held with the group of *NPO Beneficiaries*, their representatives and relevant *associate NPOs,* then considering if the proposed business relationship or one-off transaction makes sense based on what they have said.

74. Based on the assessed risk of the relationship with the *NPO Beneficiaries*, one or more of the above measures may be appropriate.

17.4.2 Associate NPOs

Statutory requirements (paraphrased wording)

75. *Article 6 of the Prescribed NPO Order requires a Prescribed NPO to take reasonable steps to:*

- *identify its associate NPOs and NPO Beneficiaries*
- *obtain information about:*

- *the activities of each associate NPO and NPO Beneficiary and*
- *the nature and purpose of its relationship with each associate NPO and NPO Beneficiary and*

› *confirm, so far as possible, that its associate NPOs and NPO Beneficiaries are not assisting or being used to assist terrorism or the financing of terrorism.*

Overview

76. Article 6(2) of the *Prescribed NPO Order* defines an *associate NPO* as "an NPO with which the prescribed NPO collaborates or works jointly in carrying out its activities". *Associate NPOs* may sometimes be referred to as "Partners".

77. An *associate NPO* might be based in Jersey, or they might be based in another jurisdiction.

78. For the purposes of this Handbook, a *Prescribed NPO* establishes a relationship with its *associate NPOs.*

79. To comply with the *Prescribed NPO Order*, a *Prescribed NPO* will need to apply a level of due diligence to its *associate NPOs*.

80. *Prescribed NPOs* should refer to their *NPO PRA* (or equivalent) and use their judgement to determine how much identity information needs to be obtained in each case, and how that information should be verified.

81. The *Prescribed NPO* is expected to make this decision by applying a risk-based approach, making reference to its risk appetite statement, documenting its decision-making and keeping it under regular review.

82. Where a *Prescribed NPO* is receiving services from a regulated *TCSP* (as defined in Section 4.4.5 of *the Handbook*) and it is considered appropriate to do so, the *NPO* may choose to apply due diligence measures which are aligned with those set out in Sections 3 and 4 of *the Handbook*.

Guidance notes – Identifying an associate NPO

83. Where an *associate NPO* is **a natural person**, a *Prescribed NPO* may demonstrate that it has taken reasonable measures to identify that *associate NPO* where it obtains the following information:

- › Name
- › Date of birth (if possible)
- › Country of birth
- › Current area of residence
- › Principal area of operations.

84. Where an *associate NPO* is **a legal person** (such as a company) **or a legal arrangement** (such as a trust), a *Prescribed NPO* should obtain the following information:

- › date of incorporation or establishment
- › country of incorporation or establishment
- › principal area of operations
- › names of the *associate NPO Controllers*, e.g. Board members or trustees.

85. Identity information may be obtained directly from the *associate NPO*, or their representative.

86. The amount of identity information obtained may differ through the taking of a risk-based approach, based on the outcome of the *NPO PRA* and the *NPO's* risk appetite statement. For example, where the *NPO PRA* produces a higher risk outcome the *Prescribed NPO* may wish to also obtain the names of the *associate NPO's Owners*, e.g. shareholders or partners of a partnership arrangement.

Guidance notes – Nature and purpose of relationship

87. A *Prescribed NPO* may demonstrate that it has obtained information on the nature and purpose of a relationship where it requests and documents this information at the establishment of a relationship.

88. The "nature" of a relationship may include:

- the type of activity the *associate NPO* will undertake on behalf of the *Prescribed NPO,* e.g. delivering medical supplies to a disaster area
- how that activity is intended to be carried out, e.g. the *associate NPO* will utilise its fleet of heavy-duty vehicles.

89. The "purpose" of a relationship may include:

- the reason the *Prescribed NPO* is engaging with the *associate NPO*, e.g. the *associate NPO* is able to access areas of a country which, for security reasons, the *Prescribed NPO* is otherwise unable to reach.

Guidance notes – Confirming associate NPOs are not involved in terrorism

90. A *Prescribed NPO* may demonstrate that it has taken reasonable measures to confirm an *associate NPO* is not assisting, or being used to assist, terrorism/the *financing of terrorism* where it does so through the use of robust, independent data sources.

91. Based on the outcome of the *NPO PRA*, a greater or lesser level of measures may be necessary to mitigate the risk of the *associate NPO* being involved in *terrorist financing*. However, *Prescribed NPOs* should always include the following checks in their due diligence measures relating to *associate NPOs*:

- screening against the UK and Jersey lists of proscribed terrorist organisations
- the OFSI Consolidated sanctions list and the UK sanctions list.

92. A *Prescribed NPO* may undertake screening in respect of sanctions through several different methods. These should be tailored so they are appropriate to its size and complexity. Examples may include:

- a *Prescribed NPO* which is receiving services from a regulated TCSP (as defined in Section 4.4.5 of *the* Handbook) might utilise a screening program developed by a professional due diligence firm to which the service provider already has access
- if checks which substantively achieve what is set out in paragraphs 90 and 91 above have recently been carried out by the *Prescribed NPO's* service provider in compliance with its requirements under Sections 3 of *the Handbook*, it is not necessary for the service provider to repeat them

- where a *Prescribed NPO* is small and individuals participate on a part-time/voluntary basis, the checks may be carried out by a person directly accessing the above-referenced lists and searching for the required names via the "Find" function of their internet browser.

93. The *Prescribed NPO* needs to be cognisant that when undertaking screening, it is important to remember that the connection to *sanctioned/designated persons* and proscribed terrorist organisations is more likely to be hidden, meaning that the person the *NPO* is engaging with is not necessarily directly captured in the lists the *Prescribed NPO* is checking against. Instead, they may be indirectly captured via their associations with terrorists, which may not be immediately apparent, but which can be brought to light through undertaking additional enquiries.

94. The independent data sources used should seek to confirm that the *associate NPO* is a legitimate person or operation. Set out below are some examples of due diligence which may be carried out at different levels of risk. The *Prescribed NPO* should document its decision in each case regarding how much due diligence it has decided to undertake:

- Lower risk
    - obtaining details of the legal person or arrangement from an online registry
    - seeking references from other *NPOs* to corroborate the information *the associate NPO* has provided
    - undertaking an open-source check (e.g. Google) to ascertain if the *associate NPO* has been subject to any adverse media coverage.
- Medium risk
    - review of registration documentation
    - understanding how long an *associate NPO* has been operating, e.g. has it been set up "overnight" to capitalise on a market opportunity?
- Higher risk
    - inspecting the *associate NPO's* site of operations to view their activities first-hand (or commissioning a trusted third party to do so)
    - inspections of *associate NPO* records and financial statements
    - requesting details of their anti-*Diversion* systems and controls and testing them.

95. There may be circumstances where a *Prescribed NPO* has a long-term relationship with an *associate NPO*. In this scenario, they may consider that additional verification of the *associate NPO's* identity, as set out above, is not required. If the *NPO* takes this decision, they should ensure their rationale for undertaking no further verification is documented. An example is set out below:

- a Prescribed NPO in Jersey provides monetary aid to several rural communities in a foreign country. The *NPO Funds* are sent to their *associate NPO*, where a local faith leader is responsible for ensuring *NPO Funds* are distributed where they are most needed, to legitimate *NPO Beneficiaries*. The *Prescribed NPO* has worked with the *associate NPO* for over a decade and several members of the governing body have met with the local faith leader personally. Through this relationship, they are satisfied that the faith leader is a

respectable person of good standing. The *Prescribed NPO* considers that no further verification is required. The governing body records their rationale at the next general meeting.

96. To help mitigate *terrorist financing* risk, a *Prescribed NPO* may wish to consider putting a partnership agreement in place to govern the relationship with the *associate NPO.* This agreement might include certain clauses to ensure a strong CFT framework is put together and maintained. Example clauses include:

- an explanation of what *terrorist financing* and *Diversion* is
- an undertaking that the *associate NPO* has appropriate measures in place to mitigate the risks of *terrorist financing,* and commits the *associate NPO*, on a best endeavours basis, to preventing it from occurring
- permitting the *Prescribed NPO* to request whatever information is necessary from the *associate NPO* to satisfy its due diligence requirements
- agreeing to the *Prescribed NPO* carrying out spot-checks on the activities of the *associate NPO* or its representative. Where a physical visit is not possible due to, for example, safety concerns, other measures of verification may be permitted such as video calls, requesting copies of invoices etc.
- requiring the *associate NPO* to maintain an audit trail of its activities and provide it to the *Prescribed NPO* upon request (may also extend to formal financial records)
- the *Prescribed NPO* reserving the right to terminate the business relationship or one-off transaction should the outcome of any checks be unsatisfactory, or if it is identified that *Diversion* has taken place.

97. There may be circumstances where a *Prescribed NPO* concludes that it is not possible, nor necessary, to put a partnership agreement, or one with *CFT* clauses, in place. If this is the case, the *NPO* should be able to explain why they took that decision and how they consider the risk of *Diversion* to be mitigated without a partnership agreement, or *CFT* clauses, being in place.

17.4.2.1 **Exceptional circumstances**

Guidance notes

98. There may be exceptional circumstances where a relationship with an *associate NPO* may need to be established or carried out rapidly. An example may be a humanitarian disaster, like a flood or earthquake which cuts off a community from food and water. Such disasters require an urgent response. Undertaking due diligence at the outset of the relationship in the way that would otherwise be expected is likely to be inappropriate.

99. Of course, this does not mean that *Prescribed NPOs* should undertake a lesser level of due diligence compared to where the need is less urgent. A *Prescribed NPO* which intends to operate in emergency scenarios will need to demonstrate they are prepared and able to implement effective controls when engaging *associate NPOs* for this purpose.

100. A *Prescribed NPO* may therefore demonstrate compliance with Article 6 of the *Prescribed NPO Order* where it:

- establishes and maintains effective procedures governing how it will identify and engage appropriate *associate NPOs* in any given scenario
- undertakes as much due diligence at the outset as can be done without unduly delaying the establishment of the relationship and
- undertakes the remaining checks deemed appropriate by the *NPO PRA* as soon as possible following the commencement of the relationship, e.g. whilst the *associate NPO* is operating 'on the ground' in the local area where distributions are carried out.

101. Where the above approach has been taken, a *Prescribed NPO* should clearly document its rationale for applying this exception and set out a timeframe during which the remaining checks will be carried out and such allowances should also be documented in its *NPO* risk appetite statement.

102. The *Prescribed NPO* should consider including a clause in its partnership agreement whereby it reserves the right to terminate the relationship should the outcome of the checks be unsatisfactory.

103. Equally, a *Prescribed NPO* may consider utilising a "preferred partner"/*associate NPO* which has already been through the due diligence process before the exceptional event occurs.

17.4.3 NPO donors

Statutory requirements (paraphrased wording)

104. *Article 5 of the Prescribed NPO Order requires a Prescribed NPO to keep records of donors who, during the preceding 12 months, have donated (as a single donation or cumulatively) –*

- *£10,000 or above or*
- *over 50% of total donations made to the Prescribed NPO during that period.*

Overview

105. Donations to *Prescribed NPOs* are diverse. For example, a significant contribution made by a wealthy individual or institution, or a small monthly contribution made by a member of the public.

106. For the purposes of *the Handbook*, the relationship between a *Prescribed NPO* and its donors is not considered to constitute a business relationship or one-off transaction.

107. As noted above, Article 5 of the *Prescribed NPO Order* requires *Prescribed NPOs* to keep a record of "significant donors", i.e. those falling within Article 5(1)(a) and 5(1)(b) of the *Prescribed NPO Order*.

108. To comply with the *Prescribed NPO Order*, a *Prescribed NPO* will need to apply a level of due diligence to its significant donors.

109. *Prescribed NPOs* should refer to their *NPO PRA* and their risk appetite statement (or equivalent documents) and use their judgement to determine how much identity information needs to be obtained in each case to mitigate the risk of *Diversion.*

110. There is no requirement in *the Prescribed NPO Order* to **verify** the identity information collected for significant donors. However, in some circumstances, such as when the *NPO PRA* (or equivalent) produces a higher-risk outcome, the *Prescribed NPO* may consider it necessary to do so. In these cases, the *NPO* should utilise robust, independent data sources to confirm the significant donor is a legitimate person or operation – see the guidance in Section 17.4.2 of *the Handbook*.

111. Where a *Prescribed NPO* is receiving services from a regulated *TCSP* (as defined in Section 4.4.5 of *the Handbook*) and it is considered appropriate to do so, the *NPO* may choose to apply due diligence measures which are aligned with those set out in Sections 3 and 4 of *the Handbook*.

112. For the avoidance of doubt, there is no statutory or *Code of Practice* requirement to make the identities of any significant donors public, for example via a *Prescribed NPO's* annual financial statement.

Guidance notes – Identifying significant donors

113. Where a significant donor is a natural person, a *Prescribed NPO* may demonstrate that it has taken reasonable measures to **identify** that person where it obtains the following information:

- Name
- Date of birth
- Country of birth
- Current residential address.

114. Where a significant donor is a legal person (such as a company) or a legal arrangement (such as a trust), a *Prescribed NPO* should obtain the following information:

- date of incorporation or establishment
- country of incorporation or establishment
- registered address
- names of the significant donor's controllers, e.g. board members or trustees
- names of the significant donor's owners, e.g. shareholders or partners of a partnership arrangement.

115. Information collected on significant Donors may be kept in a register, list, or similar format.

116. As noted above, it may be considered necessary to obtain additional identity information based on the outcome of the *NPO PRA* and the *NPO's* risk appetite statement (or equivalent documents). For example, a higher-risk rating might mean the *Prescribed NPO* requests further information from their significant donors.

117. Based on the outcome of the *NPO PRA* and the *NPO's* risk appetite statement (or equivalent documents), and where a significant donor is not a natural person, it may be considered necessary to understand the ownership structure of that significant donor and the persons who control it. For example, a *Prescribed NPO* may consider it necessary where a higher-risk rating is produced. In these situations, *Prescribed NPOs* should follow the guidance set out in the relevant sections of *the Handbook* listed below, in respect of identifying beneficial owners and controllers:

- Trusts – Section 4.4.1

- Limited Partnerships – Section 4.4.3
- Companies – 4.5.1
- Foundations – 4.5.3
- Partnerships – 4.5.5.

118. Where a significant donor makes regular payments to a *Prescribed NPO,* it is not necessary to obtain identity information every time a donation is received from that donor. In these cases, *Prescribed NPOs* should seek to re-confirm the donor's identity information at least every two years. The re-confirmation should be undertaken sooner where it is known that there has been a change in the significant donor's information, e.g. a natural person has changed residential address, or the Board of a corporate significant donor has changed.

17.5 Identification, screening and training of relevant volunteers, relevant employees, owners and controllers

17.5.1 Overview of section

119. *Prescribed NPOs* also have a specific legal requirement to maintain certain information on their *NPO Owners and Controllers*. This section sets out the statutory requirements and provides guidance on how *Prescribed NPOs* may demonstrate compliance with those requirements.

120. This section also provides guidance on how a *Prescribed NPO* might carry out due diligence on, and provide training to, certain volunteers and employees.

121. The presence of competent individuals, who are well-trained and have integrity, will assist *Prescribed NPOs* to maintain effective systems and controls to counter *terrorist financing*.

122. This section of *the Handbook* does not require *Prescribed NPOs* to carry out screening or training through mandatory *Code of Practice* requirements. Nor are there any statutory requirements in the *Prescribed NPO Order* for screening or training. Sections 17.5.3 and 17.5.4 are provided as guidance on best practice.

17.5.2 Identifying NPO owners and controllers

Statutory requirements (paraphrased wording)

123. *Article 4 of the Prescribed NPO Order requires a Prescribed NPO to keep records that are sufficient to identify:*

- *any person who owns the NPO, or controls or directs the NPO's activities, including as appropriate, a senior officer, board member, director or trustee and*
- *any other person who exercises, or has the right to exercise, significant influence or control over the activities of the NPO.*

Overview

124. As noted in the Glossary above, for the purposes of *the Handbook* "*NPO Owners and Controllers*" are those persons set out in Article 4(1)(a) and 4(1)(b) of the *Prescribed NPO Order.*

125. Examples of *NPO Owners* include, but are not limited to:

- Shareholders and
- Partners of a partnership.

126. Depending on the legal form of a *Prescribed NPO*, it may not have any *NPO Owners*. An example would be a *NPO* established as a trust. *NPOs* established in such a way are not required to comply with that element of Article 4(1)(a) of the *Prescribed NPO Order*, nor apply any of the below measures in respect of *NPO Owners*.

127. *NPO Controllers* will include charity governors, board members, trustees and senior officers (or equivalent, whether or not they are remunerated).

128. It is important to emphasise that remuneration is irrelevant when considering if a person is an *NPO Controller*. The test is whether that person can exercise control over, or direct, the activities of the *Prescribed NPO*.

129. It is possible for an individual to be considered a *NPO Owner* or *NPO Controller* where they hold their ownership interest or exercise control through indirect means. For example:

- where a Prescribed *NPO* is established as a company, an individual who holds shares in the *NPO* through an intermediate holding vehicle will be considered a *NPO Owner*
- an individual who does not sit on the governing body of the *NPO*, but in accordance with whose directions the governing body are nevertheless accustomed to act will be a *NPO Controller*.

Code of Practice

130. Where a *Prescribed NPO* is a registered Jersey charity, they must maintain a fit and proper person declaration for each charity governor and declare it has done so to the Jersey Charity Commissioner at each annual return to that body.

Guidance notes

131. A *Prescribed NPO* may demonstrate compliance with Article 4 of the *Prescribed NPO Order* where it obtains the following information from each *NPO Owner and Controller:*

- Name
- Date of birth
- Place of birth
- Permanent residential address
- The capacity in which they are acting, e.g. a board member, shareholder etc.

132. Where any of the information set out above changes, e.g. the *NPO Owner or Controller* moves to a new permanent residence, the *Prescribed NPO* should update the information held in their records.

133. A *Prescribed NPO* may wish to consider requiring its *NPO Owners and Controllers* to make a periodic confirmation that the information held on file remains correct.

17.5.3 Screening of relevant volunteers, relevant employees and controllers

Overview

134. As noted in Section 17.5.1 above, this section is provided as guidance on best practice. There are no mandatory *Code of Practice* requirements set out in this section.

135. For the purposes of this section, the term "relevant employees" means an individual who is working under a contract of employment and undertakes one or more of the following as part of their role:

- Acts as a NPO *Controller,* and/or
- Is responsible for the disbursement, and/or raising, of *NPO Funds* outside of Jersey, Guernsey, the Isle of Man, England and Wales, or Scotland.

136. It includes temporary and contract employees, and the employee of any external party fulfilling a function in relation to a *Prescribed NPO* under an outsourcing agreement.

137. For the purposes of this section, the term "relevant volunteer" means an individual who carries out their duties for a *Prescribed NPO* on a voluntary, non-remunerated basis, and undertakes one or more of the following as part of their role:

- Acts as a *NPO Controller,* and/or
- Is responsible for the disbursement, and/or raising, of *NPO Funds* outside of Jersey, Guernsey, the Isle of Man, England and Wales, or Scotland.

138. Examples of roles where an individual is responsible for the disbursement, and/or raising, of *NPO Funds* may include:

- researching and recommending regions, or *NPO Beneficiaries,* where *NPO Funds* should be disbursed
- approving and/or executing a transaction which disburses *NPO Funds* to outside of Jersey, Guernsey, the Isle of Man, England and Wales, or Scotland, whether electronically or through the handing over of cash in the field.

139. It is expected that the terms "relevant employee" and "relevant volunteer" will, between them, capture all *NPO Controllers*.

140. *NPO Owners* are not subject to the requirements set out below.

Guidance notes

141. A *Prescribed NPO* may wish to screen their *NPO Controllers* against:

- the UK and Jersey lists of proscribed terrorist organisations

- the OFSI Consolidated sanctions list and the UK sanctions list.

142. A *Prescribed NPO* may undertake screening in respect of sanctions through several different methods. These should be tailored so they are appropriate to its size and complexity. Examples may include:

- a *Prescribed NPO* which is receiving services from a regulated *TCSP* (as defined in Section 4.4.5 of *the* Handbook) might utilise a screening program developed by a professional due diligence firm to which the service provider already has access
- if checks which are substantively the same as those described at paragraph 141 above have recently been carried out by the *Prescribed NPO's* service provider in compliance with their requirements at Section 9.2 of *the Handbook*, it is not necessary for the service provider to repeat them
- where a *Prescribed NPO* is small and individuals participate on a part-time/voluntary basis, the checks may be carried out by a person directly accessing the above-referenced lists and searching for the required names via the "Find" function of their internet browser.

143. In addition to completing the checks listed at paragraph 141 above, a *Prescribed NPO* may demonstrate that its relevant volunteers and relevant employees are screened where it does one or more of the following, as appropriate for the nature of the relevant volunteer or relevant employee's role and responsibilities, and on a risk-based approach:

- obtains and confirms references provided
- obtains and confirms employment history and qualifications disclosed
- obtains details of any regulatory action taken against the individual (or absence of such action)
- obtains and confirms details of any criminal convictions (or absence of such convictions).

144. Enquiries into an individual's criminal past are required to be subject to the Rehabilitation of Offenders (Jersey) Law 2001, which prevents *supervised persons* from requesting information from its directors, senior managers and other employees (and prospective directors, senior managers and other employees) about convictions that are "spent", except where provided for by the Rehabilitation of Offenders (Exceptions) (Jersey) Regulations 2002.

145. A *Prescribed NPO* may also wish to consider requiring its relevant employees, relevant volunteers and all *NPO Controllers* to make a signed confirmation that they are not, nor have ever been, members of a proscribed terrorist organisation.

146. It may also be appropriate for any contract or agreement issued to a relevant volunteer, relevant employee or *NPO Controller* to include a clause stating that non-compliance with policies and procedures, or evidence the person may have been involved in *terrorist financing*, will lead to disciplinary processes.

17.5.4 Training and awareness of relevant volunteers, relevant employees and controllers

17.5.4.1 Promoting awareness and providing training

Guidance notes

147. As noted in Section 17.5.1 above, this section is provided as guidance on best practice. There are no mandatory *Code of Practice* requirements set out in this section.

148. Where a *Prescribed NPO* decides to provide training to its relevant volunteers and relevant employees (which should include all *NPO Controllers*), such training should cover:

- the specific *terrorist* financing risks to which the *Prescribed NPO* may be exposed, and
- how it might be abused for *terrorist financing* purposes.

149. The overall objective of the training delivered should be to promote an anti-*diversion* culture within the *Prescribed NPO*.

150. When designing the training, the *Prescribed NPO* should ensure it is relevant to any *NPO PRA*, *Diversion* risk register and risk appetite statement (or their equivalents) which they have prepared. It should also be tailored so it is specific to the person(s) receiving the training.

151. The training may include guidance on specific red flags and risk indicators which are relevant to the *Prescribed NPO's* programme of activity. They may include, but are not limited to:

- anomalies in the *NPO* programme delivery, e.g. unusual events, or meetings/ relationships which are not expected
- transactions with unexpected parties, where the transactions do not make sense
- behaviours that indicate a party may be sympathising with a terrorist organisation or having extremist/radicalised views
- high turnover of staff in an *associate NPO* or the *Prescribed NPO* itself
- non-compliance with procedures by *NPO* staff, or frequent management overrides
- the ability of an *associate NPO* to gain access to an area when other *associate NPOs*/non-governmental organisations cannot do so
- failure of *associate NPOs*, *NPO Beneficiaries* or their representatives to comply in a timely manner with reasonable requests for information or documentation
- incomplete records of donation delivery by *NPO* staff or *associate NPOs*
- *NPO* branded donation items appear in local markets
- vague records of expenses without additional specification in accounts and supporting documentation, e.g. references to "logistics", "security", "miscellaneous".

152. The training may also include reference to the *JFSC's* whistleblowing line – see our website for more information.

153. Materials which may be useful in the delivery of training may include:

- publications by academics and the Government of Jersey, such as the *NPO NRA*
- guidance documents regarding *terrorist financing* and sanctions published by *JFSC*

- Additional information sources attached as Appendices to *the Handbook*.

154. Examples of the different types of training which may be delivered to relevant volunteers and relevant employees include:

- A *Prescribed NPO* is designing training for a relevant volunteer who will travel to a region of a higher-risk jurisdiction with significant levels of local government corruption and lawlessness. The relevant volunteer will be responsible for handing out *NPO Funds* to be used in the local area, in collaboration with some *associate NPOs.* The *NPO* considers that it is important for the training to cover specific warning signs when physically working with *associate NPOs* in the region and what to do if unusual events occur such as meetings or relationships which are not expected

- A *Prescribed NPO* raises *NPO Funds* in Jersey and disburses them to a small *associate NPOs* which helps disadvantaged young people abroad. The *NPO* considers that it is important for the relevant volunteers and relevant employees to be trained on general warning signs when working with *associate NPOs,* such as incomplete records of donation delivery.

155. It is important for training to be delivered at appropriate frequencies, for example:

- induction training to be delivered within 10 working days of the commencement of employment (or its equivalent) and, if appropriate, where there is a material change in an individual's role and responsibilities.

- refresher training to be delivered on a regular basis. This may be annually, or at some other frequency deemed appropriate based on the *Prescribed NPO's NPO PRA* or equivalent document.

17.5.4.2 Monitoring and maintaining awareness

Overview

156. As noted in Section 17.5.1 above, this section is provided as guidance on best practice. There are no mandatory *Code of Practice* requirements set out in this section.

157. As time passes, the level of awareness of *terrorist financing* risks can decrease. Having a framework in place to maintain a high level of awareness can keep a *Prescribed NPO's* defences against *Diversion* in good condition.

158. Where a *Prescribed NPO* delivers training to relevant volunteers and relevant employees (see Section 17.5.4.1 above), they should monitor and test their relevant volunteers' and relevant employees' (including all *NPO Controllers'*) level of awareness of *terrorist financing* risks.

Guidance notes

159. A *Prescribed NPO* may demonstrate that it monitors and tests their volunteers', employees' and *NPO Controllers'* level of awareness where it periodically tests the awareness of:

- terrorist financing risks

- the *Prescribed NPO's* policies and procedures and

- relevant statutory obligations.

160. Where awareness is deemed to be insufficient, the *Prescribed NPO* should take action to remedy the situation as soon as practicable.

161. When a relevant volunteer's, relevant employee's, or *NPO Controller's* contract with a *Prescribed NPO* comes to an end, it may be appropriate for the *Prescribed NPO* to conduct an exit interview. The interview could seek feedback on any training and monitoring the person received and how it may be improved.

162. Factors which may influence whether a *Prescribed NPO* considers an exit interview to be necessary may include:

- the level of risk assessed in the *Prescribed NPO's NPO PRA* (or equivalent), e.g. if the *NPO PRA* generates a higher risk level, it may be appropriate for all relevant volunteers and relevant employees involved in that particular *NPO* programme of work to have an exit interview
- the level of *terrorist financing* risk which the individual's role involved.

17.6 Accounting for funds

Statutory requirements (paraphrased wording)

163. *Article 2(1) of the Prescribed NPO Order requires a Prescribed NPO to prepare annually a financial statement for a period of not more than 12 months.*

164. *Article 2(2) states that the period referenced above:*

- *must begin on or before the date the NPO became a Prescribed NPO (e.g. if the NPO became a Prescribed NPO on 15 March 2023, the period must begin on or before 15 March 2023), but*
- *if the NPO has previously prepared and provided a financial statement under paragraph (1), the period must begin at the end of the period covered by its most recent financial statement.*

165. *Article 2(3) states that the financial statement must be in a form published or approved for the purpose by the JFSC.*

166. *Article 2(4) states that a Prescribed NPO must provide a financial statement prepared under paragraph (1) to the JFSC if required to do so by the JFSC.*

167. *Article 3 of the Prescribed NPO Order requires Prescribed NPOs to have in place appropriate accounting systems and controls to ensure that its funds are fully accounted for.*

Codes of Practice

168. A *Prescribed NPO* must maintain accounting records that are sufficient to show and explain its transactions. The accounting records must:

- disclose with reasonable accuracy, at any time, the financial position of the *NPO* at that time and
- enable the *Prescribed NPO* to verify that funds have been received and spent in a manner consistent with the purpose and objectives of the *Prescribed NPO*.

Guidance notes

169. A *Prescribed NPO* may demonstrate compliance with the *Code of Practice* set out above by regularly reconciling their transactions. The frequency of reconciliation may be determined by reference to the *NPO PRA* and the *NPO's* risk appetite statement (or equivalent documents). For example, if the assessment outcome is 'higher risk', the accounting records are likely to be reconciled more regularly. If the assessment outcome is 'lower risk', it may be more appropriate to reconcile less regularly.

170. The financial statements' level of complexity will depend on the nature and scale of a *Prescribed NPO's* operations, as well as their type. For example:

- a small organisation with a relatively simple and low level of activity may consider it sufficient to prepare a statement of income and expenditure
- NPOs may be subject to other, at times more stringent, requirements depending on their type. For example, NPOs may be subject to the requirements of the Companies Law.

171. A *Prescribed NPO* may wish to consider presenting its financial statements for approval by its governing body, e.g. its trustees, board of directors etc. The governing body considers whether the financial statements represent a true and accurate reflection of the *Prescribed NPO's* financial position and record their decision on the same.

17.7 Record-keeping

17.7.1 Overview and general requirements

Overview

172. This section supplements the statutory provisions of the *Prescribed NPO Order* relevant to record-keeping with additional *Codes of Practice* and *Guidance notes* so that *Prescribed NPOs* may demonstrate compliance with the legal requirements. More general obligations on *Prescribed NPOs* to maintain records (such as those in other Jersey laws) are not addressed in this section. It should be noted, however, that such general obligations may extend the period for which records must be kept.

173. Record-keeping is essential to facilitate effective supervision by the *JFSC* and, where necessary, effective investigation by law enforcement. Good record-keeping helps a *Prescribed NPO* to demonstrate compliance with their statutory and *Code of Practice* requirements, as well as assisting law enforcement in tracing funds which may have been used to finance terrorism through the financial system.

174. Where the financial statements of a *Prescribed NPO* are audited, records also provide context for any opinion which may be issued on the financial statements by the *Prescribed NPO's* auditor.

175. Records can be kept in the following forms:

- original documents
- copies of original documents (certified where appropriate)
- scanned copies or

› computerised/electronic copies.

176. Where a *Prescribed NPO* is receiving services from a regulated *TCSP* (as defined in Section 4.4.5 of *the Handbook*) it is likely that record-keeping measures will already in place to meet the requirements of Section 10 of *the Handbook*. Where these measures substantively meet the requirements set out throughout Section 17.7, it is not necessary for the service provider to duplicate them.

Statutory requirements (paraphrased wording)

177. *Article 4(2) of the Prescribed NPO Order requires Prescribed NPOs to retain records kept under Article 4(1) (owners, controllers etc) for at least 5 years.*

178. *Article 5(3) of the Prescribed NPO Order requires Prescribed NPOs to retain records kept under Article 5(1) (significant donors) for at least 5 years.*

Codes of Practice

179. A *Prescribed NPO* must keep, for a period of at least five years, copies of their annual financial statements and the underlying accounting records.

180. A *Prescribed NPO* must keep, for a period of at least five years, copies of any:

› NPO PRAs

› Risk appetite statements and

› *Diversion* risk registers,

or equivalent documents which they have produced.

181. Where a *Prescribed NPO* delivers the training described in Section 17.5.4 of this Handbook to relevant volunteers and relevant employees, records of said training must be kept for a period of at least five years after the end of the calendar year in which the training was provided. The records must include the following information:

› the dates on which training was provided

› the nature of the training provided

› names of relevant volunteers and/or relevant employees who received the training and

› records of testing subsequently carried out to measure volunteers and/or employee's understanding of the training provided, including pass rates and details of any action taken in cases of failure.

182. A *Prescribed NPO* must keep, for a period of at least five years, records of due diligence collected for their *NPO Beneficiaries* and *associate NPOs*, to include both **identity information** and **evidence** used to confirm that those persons are not involved in terrorist activities.

183. A *Prescribed NPO* must keep, for a period of at least five years, records of due diligence (i.e., the identity information) collected for their significant donors.

184. A *Prescribed NPO* must keep records of transactions undertaken, whether the transactions are done through the formal banking system or using a non-banking platform/method, for a period of at least five years from the date when the transaction was completed.

17.7.2 Access and retrieval of records

Codes of Practice

185. A *Prescribed NPO* must keep documents, data or information obtained when establishing a *business relationship* in a way that facilitates on-going monitoring of the *NPO* programme.

186. All records kept by a *Prescribed NPO* must be readily accessible and retrievable by the *Prescribed NPO*. Unless otherwise specified, records relating to a relationship with a *NPO Beneficiary* or *associate NPO* must be accessible and retrievable **within five working days** (whether kept in or outside of Jersey), or such longer period as agreed with the *JFSC*. Other records must be accessible and retrievable **within 10 working days** (whether kept in or outside of Jersey), or such longer period as agreed with the *JFSC*.

187. A *Prescribed NPO* must periodically review the condition of paper and electronic records and consider the adequacy of its record-keeping arrangements. The frequency of said reviews must be determined with reference to its *NPO PRA* (or equivalent).

188. A *Prescribed NPO* must periodically test procedures regarding access to and retrieval of its records. The frequency of said testing must be determined with reference to its *NPO PRA* (or equivalent).

189. Records must be maintained in a **readable format**. Where records are kept other than in readable form, they must be maintained such that they can be produced in readable form at a computer terminal in Jersey.

190. When original documents that would ordinarily have been destroyed are requested for investigation purposes, a *Prescribed NPO* must ascertain whether the documents have in fact been destroyed.

191. All documents (or parts thereof) held under the requirements of the *Prescribed NPO Order* and/or the *Codes of Practice* in Section 17.7 must be understandable (i.e. in a language understood by a relevant volunteer or relevant employee of the *Prescribed NPO*), and must be translated into English at the request of the *JFSC* or any other authority which by law has the power to request them.

17.7.3 External records

Overview

192. Where records are kept by another person (whether they are part of the *Prescribed NPO's* group or otherwise), or kept outside Jersey, such as under an outsourcing or storage arrangement, this will present additional factors for a *Prescribed NPO* to consider. Regardless of the particular circumstances, the *Prescribed NPO* remains responsible for compliance with all record-keeping requirements.

Code of Practice

193. A *Prescribed NPO* must not:

- allow another person (group or otherwise) to keep records or
- keep records outside Jersey,

where access and retrieval of records (by that person, the *JFSC* and/or law enforcement) is likely to be impeded by confidentiality or data protection restrictions.

17.7.4 Reorganisation or termination

Overview

194. Record-keeping requirements persist and are unaffected where a *Prescribed NPO*:

- merges with another organisation
- continues as another organisation, e.g. changing from being incorporated under the laws of one jurisdiction to another
- is taken over by another organisation
- is subject to internal reorganisation, e.g. the *Prescribed NPO* changes its internal divisions and amends their scope/remit
- terminates its activities
- transfers responsibility for a portion of their *NPO Beneficiaries* or donors to another organisation or
- transfers contracts or arrangements with *associate NPOs* to another organisation.

Code of Practice

195. A *Prescribed NPO* that undergoes mergers, continuance, takeovers or internal reorganisations, must ensure that records remain readily accessible and retrievable for the required periods stated above. This extends to the rationalising of computer systems and storage arrangements.

196. Record-keeping arrangements must be agreed with the *JFSC* where a *Prescribed NPO*:

- terminates its activities
- transfers responsibility for a portion of their *NPO Beneficiaries*, or donors to another organisation or
- transfers contracts or arrangements with *associate NPOs* to another organisation.