1 INTRODUCTION

Please Note:

- Whilst no regulatory requirements are set within this section, there are references to Jersey legislation which may be accessed through the JFSC website.
- Where terms appear in the Glossary this is highlighted through the use of italic text. The Glossary is available from the JFSC website.

1. Criminals have responded to the anti-money laundering and countering the *financing of terrorism* (***AML/CFT***) measures taken by the traditional financial sector over the past decade and have sought 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. Professionals such as accountants, lawyers and notaries who interface with the financial sector have frequently been used as a conduit for criminal property to enter the banking and financial systems.

2. In particular, criminals and money launderers will often try to exploit the services offered by accountants, through the business of undertaking 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 valuable, anonymous, route into the banking system. The ´tax management´ excuse is often used by money launderers as a smokescreen to explain away unusual circumstances and transactions that would appear to be suspicious.

3. The inter-governmental agencies and international standard-setting bodies have recognised the access that professionals provide for their clients to financial services and products, and have extended the scope of the international standards and recommendations to cover lawyers and accountants - often referred to as 'gatekeepers'. As a well-regulated jurisdiction operating in the international financial arena, Jersey must adopt the international standards to guard against *money laundering* and the *financing of terrorism* and integrate the requirements into the legal and regulatory system.

4. Accountants, *auditor*s, tax advisers and insolvency practitioners are key professionals in the business and financial world, facilitating vital transactions and activity that underpin Jersey's economy. As such, they have a significant role to play in ensuring that their services are not used to further a criminal purpose. As professionals, accountants must act with integrity and uphold the law, and they must not engage in criminal activity.

5. The continuing ability of Jersey's finance industry to attract legitimate clients 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 accountant in Jersey that assists in laundering the proceeds of crime, or *financing of terrorism*, 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 services

   will face the loss of its reputation, and risk regulatory sanctions, damage the integrity of Jersey's professional and finance industry as a whole, and may risk prosecution for criminal offences.

6. Jersey's defences against the laundering of criminal funds and terrorist financing rely heavily on the vigilance and co-operation of the finance sector. Specific financial sector legislation (the Money Laundering (Jersey) Order 2008 (the ***Money Laundering Order***)) is therefore also in place covering a person carrying on a *financial services business* in or from within Jersey, and a

Jersey body corporate or other legal person registered in Jersey carrying on a *financial services business* anywhere in the world (a ***relevant person***).

7. The primary legislation on *money laundering* and the *financing of terrorism* (the ***money laundering legislation***) is:

   › The Proceeds of Crime (Jersey) Law 1999 (as amended) (the ***Proceeds of Crime Law***)

   › The Terrorism (Jersey) Law 2002 (the ***Terrorism Law***

   › The Money Laundering and Weapons Development (Directions) (Jersey) Law 2012 (the ***Directions Law***)

   › The Sanctions and Asset-Freezing (Jersey) Law 2019

   › Any Regulations or Orders made under the enactment falling within any of the above laws

   › The EU Legislation (Information Accompanying Transfers of Funds) (Jersey) Regulation 2017.

8. A *relevant person* carrying on a business described in paragraph 2 of Part B of Schedule 2 to the *Proceeds of Crime Law* must put in place *systems and controls* to guard against *money laundering* and the *financing of terrorism* in accordance with Jersey requirements and international standards. All '*relevant persons*'[1] fall within the scope of the *Money Laundering Order*.

9. The international standards require that all *relevant person*s must be supervised by an appropriate anti-money laundering supervisory body. Within Jersey, the Jersey Financial Services Commission (the ***Commission***) has been designated as the relevant supervisory body under the Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008 (the ***Supervisory Bodies Law***) for all regulated and *specified Schedule 2 business*es (including *relevant persons* carrying on a business described in paragraph 2 of Part B of Schedule 2 to the *Proceeds of Crime Law*).

10. Every firm offering external accountancy or related services in Jersey must recognise the role that it is required to play in protecting itself, and its employees, from involvement in *money laundering* and the *financing of terrorism*, and also in protecting the Island's reputation of probity. This principle relates not only to business operations within Jersey, but also operations conducted by Jersey businesses outside the Island.

11. For the purpose of this Handbook, within the Overview text, *AML/CFT Codes of Practice* and Guidance Notes (see Section 1.2 of this Handbook) *relevant person*s carrying on Schedule 2 business are referred to as "**accountancy firms**" or "**firms**"[2]. Within the *Money Laundering Order* and references within this Handbook to the Statutory Requirements of the *Money Laundering Order*, all persons and businesses that fall within the scope of the *Money Laundering Order* are referred to as '***relevant persons***'.

12. Throughout this Handbook, references to:

   › ***Client*** (or customer) includes, where appropriate, a prospective client or customer (an applicant for business). A client is a person with whom a business relationship has been formed or one-off transaction conducted.

---

[1] The term relevant person used within this Handbook refers to a person carrying on financial services business as defined in Schedule 2 of the *Proceeds of Crime Law*.

[2] For the avoidance of doubt "accountancy firms" or "firms" include sole practitioners and sole traders.

- *Financing of terrorism* means:
  - conduct that is an offence under any provision of Articles 15 (use and possession etc. of property for purposes of terrorism) and 16 (dealing with terrorist property) of the *Terrorism Law*; or
  - conduct outside Jersey, which, if occurring in Jersey, would be an offence under Articles 15 and 16.
- *Money laundering* means:
  - conduct that is an offence under any provision of Articles 30 (dealing with criminal property) and 31 (concealment etc. of criminal property) of the *Proceeds of Crime Law*;
  - conduct that is an offence under Articles 34A and 34D of the *Proceeds of Crime Law*;
  - conduct that is an offence under Articles 10 to 14 (failing to freeze terrorist funds and making things available to a terrorist) and 16 (licencing offences) of the Sanctions and Asset-Freezing (Jersey) Law 2019; or
  - conduct outside Jersey, which, if occurring in Jersey, would be an offence under any of the above.
- **Schedule 2 business** means a business described in paragraph 2 of Part B of Schedule 2 to the *Proceeds of Crime Law*.

1.1 Objectives of this Handbook

13. The objectives of this Handbook are as follows:
    - to outline the requirements of the *money laundering* legislation;
    - to outline the requirements of the *Money Laundering Order* that supplements the *money laundering* legislation by placing more detailed requirements on *relevant persons*;
    - to outline good practice for implementing the legal requirements;
    - to assist a firm to comply with the requirements of the legislation described above and the *Commission's* requirements, through practical interpretation;
    - to outline good practice in developing *systems and controls* to prevent the accountancy profession from being used to facilitate *money laundering* and the *financing of terrorism*;
    - to provide a base from which a firm can design and implement *systems and controls* and tailor their own *policies and procedures* for the prevention and detection of *money laundering* and the *financing of terrorism* (and which may also help to highlight identity fraud);
    - to ensure that Jersey matches international standards to prevent and detect *money laundering* and combat the *financing of terrorism*;
    - 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 promote the use of a proportionate, risk based approach to customer due diligence measures, which directs resources towards higher risk clients;
    - to emphasise the particular *money laundering* and *financing of terrorism* risks of certain financial services and products; and

› to provide an information resource to be used in training and raising awareness of *money laundering* and the *financing of terrorism*.

14. This 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.

15. This Handbook is intended for use by senior management and compliance staff within the accountancy sector to assist in the development of *systems and controls* and detailed *policies and procedures*. This Handbook is not intended to be used by firms as an internal procedures manual.

16. Where firms are authorised and regulated by the *Commission* under the Financial Services (Jersey) Law 1998 and subject to one or more of the Investment Business, Trust Company Business and Funds Services Business Codes of Practice, they should refer to the separate *AML/CFT Handbook* when drawing up their *policies and procedures* for the prevention of and detection of *money laundering* and the *financing of terrorism* in respect of those regulated activities.

1.2 Structure of this Handbook

17. This Handbook describes Statutory Requirements, sets out principles and detailed requirements (*AML/CFT Codes of Practice*), and presents ways of complying with Statutory Requirements and the *AML/CFT Codes of Practice* (Guidance Notes).

18. **Statutory Requirements** describes the statutory provisions that must be adhered to by a *relevant person* (natural or legal) when carrying on a *financial services business*, in particular requirements set out in the *Money Laundering Order*. Failure to follow a Statutory Requirement is a criminal offence and may also attract regulatory sanction.

19. The ***AML/CFT Code of Practice*** sets out principles and detailed requirements for compliance with Statutory Requirements. In particular, the *AML/CFT Code of Practice* comprises a number of individual *AML/CFT Codes of Practice*: (i) to be followed in the area of corporate governance, which it is considered must be in place in order for a *relevant person* to comply with Statutory Requirements; and (ii) that explain in more detail how a Statutory Requirement is to be complied with. Failure to follow any *AML/CFT Codes of Practice* may attract regulatory sanction[3].

20. **Guidance Notes** present ways of complying with the Statutory Requirements and *AML/ CFT Codes of Practice* and must always be read in conjunction with these. A firm may adopt other appropriate 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 Codes of Practice*. This allows a firm discretion as to how to apply requirements in the particular circumstances of its business, products, services, transactions and clients. The soundly reasoned application of the provisions contained within the Guidance Notes will provide a good indication that a firm is in compliance with the Statutory Requirements and *AML/ CFT Codes of Practice*.

21. The provisions of the Statutory Requirements and of the *AML/CFT Codes of Practice* are described using the term **must**, indicating that they are mandatory. However, in exceptional

[3] AML/CFT Codes of Practice and the Guidance Notes shall also be relevant in determining whether or not requirements contained in the Money Laundering Order or in Article 21 of the *Terrorism (Jersey) Law 2002* have been complied with.

circumstances, where strict adherence to any of the *AML/CFT Codes of Practice* would produce an anomalous result, a *relevant person* may apply in advance in writing to the *Commission* for a variance from the requirement. For further information refer to Part 3, Section 1.3 of the *AML/CFT Handbook*.

22. 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 Codes of Practice*. References to must and may elsewhere in this Handbook should be similarly construed.

23. This Handbook also contains **Overview** text which provides some background information relevant to particular sections or sub-sections of this Handbook.

24. This Handbook is not intended to provide an exhaustive list of *systems and controls* to counter *money laundering* and the *financing of terrorism*. In complying with the Statutory Requirements and *AML/CFT Codes of Practice*, and in applying the Guidance Notes, firms should (where permitted) adopt an appropriate and intelligent 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 either to launder money or to finance terrorism.

25. The Statutory Requirements text necessarily paraphrase provisions contained in the *money laundering* legislation and the *Money Laundering Order* and should always be read and understood in conjunction with the full text of each law. Statutory Requirements are presented "boxed" and in italics, to distinguish them from other text.

26. Part 2 of the *AML/CFT Handbook* contains an information resource to be used in training and raising awareness of *money laundering* and the *financing of terrorism*.

27. Part 3 of the *AML/CFT Handbook* sets out the *Commission*'*s* policy for the supervision of compliance by a *relevant person* carrying on Schedule 2 business with the Statutory Requirements and *AML/CFT Codes of Practice*.

28. All references within this Handbook to any Parts or Appendices of the *AML/CFT Handbook* are adopted as if a Part or Appendix to this Handbook.

1.3 Legal status of this Handbook and Sanctions for Non-Compliance

1.3.1 This Handbook

29. This Handbook is issued by the *Commission*:

- pursuant to its powers under Article 22 of the *Supervisory Bodies Law* (which provides for an *AML/CFT Code of Practice* to be prepared and issued for the purpose of setting out principles and detailed requirements), and
- in the light of Article 37 of the *Proceeds of Crime Law* (which provides for the *Money Laundering Order* to prescribe measures to be taken).

30. The *AML/CFT Codes of Practice* in this Handbook cover *relevant person*s carrying on Schedule 2 business.

1.3.2 Money Laundering Order

31. The *Money Laundering Order* is made by the Chief Minister under Article 37 of the *Proceeds of Crime Law*. The *Money Laundering Order* prescribes measures to be taken (including measures not to be taken) by persons who carry on *financial services business* (a term that is defined in Article 36 of the *Proceeds of Crime Law*), for the purposes of preventing and detecting *money laundering* and the *financing of terrorism*.

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 firm 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 any guidance provided (for this purpose guidance will include the *AML/CFT Code of Practice* read in conjunction with Overview text and the Guidance Notes), 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. Where a breach of the *Money Laundering Order* by a firm is proved to have been committed with the consent of, or to be attributable to any neglect on the part of, a partner, member, director, manager or other similar officer, that individual, as well as the firm shall be guilty of the offence and subject to criminal sanctions.

34. Similarly, 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 required to take account of the contents of this Handbook. 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.

35. Nevertheless, this Handbook is not a substitute for the *money laundering* legislation and compliance with it is not of itself a defence to offences under the principal legislation. However, courts will generally have regard to regulatory guidance when considering the standards of a professional person's conduct and whether they acted reasonably, honestly, and appropriately, and took all reasonable steps and exercised all due diligence to avoid committing the offence.

AML/CFT Code of Practice

36. A Code of Practice is prepared and issued by the *Commission* under Article 22 of the *Supervisory Bodies Law*. The Code of Practice sets out the principles and detailed requirements that must be complied with in order to meet certain requirements of the *Supervisory Bodies Law*, the *Money Laundering Order* and the *money laundering* legislation by persons in relation to whom the *Commission* has supervisory functions. The *AML/CFT Code of Practice* comprises a number of individual *AML/CFT Codes of Practice*.

37. Article 5 of the *Supervisory Bodies Law* states that the *Commission* shall be the supervisory body to exercise supervisory functions in respect of a "*regulated person*" (a term that is defined in Article 1 of the *Supervisory Bodies Law*). The *Commission* 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*" (a term that is defined in Article 1 of the *Supervisory Bodies Law*). The effect of these provisions is to give the *Commission* supervisory functions in respect of every *relevant person*.

38. Compliance with the *AML/CFT Code of Practice* will be considered by the *Commission* in the conduct of its supervisory programme, including on-site examinations.

39. The consequences of non-compliance with any *AML/CFT Codes of Practice* could include an investigation by or on behalf of the *Commission*, the imposition of regulatory sanctions, and criminal prosecution of the *relevant person* and its employees. Regulatory sanctions available under the *Supervisory Bodies Law* include:

- issuing a public statement;
- imposing a registration condition;
- imposing a direction and making this public, including preventing an individual from working in a *relevant person*; and
- revocation of a registration.

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

1.4.1 Application of the Money Laundering Order and AML/CFT Codes of Practice to Schedule 2 business carried on in Jersey

40. By virtue of the definition of *relevant person* in Article 1(1), the *Money Laundering Order* applies to any person who is carrying on a *financial services business* (including Schedule 2 business) in, or from within, Jersey. This will include Jersey-based offices of firms incorporated outside Jersey conducting Schedule 2 business in Jersey.

41. By virtue of Articles 5, 6 and 22 of the *Supervisory Bodies Law*, *AML/CFT Codes of Practice* apply to any person who is carrying on *financial services business* in or from within Jersey.

42. The *AML/CFT Codes of Practice* in this Handbook cover *relevant person*s carrying on a business described in paragraph 2 of Part B of Schedule 2 to the *Proceeds of Crime Law*.

1.4.2 Application of the Money Laundering Order to Schedule 2 Business Carried on Outside Jersey (overseas)

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

44. However, Article 10A(9) of the *Money Laundering Order* explains that a *relevant person* need not comply with paragraphs (2), (3) and (4) in a country or territory outside Jersey in respect of any Schedule 2 business.

45. Notwithstanding the above, all of the provisions of the *Money Laundering Order* apply to a *relevant person* that is a legal person carrying out *financial services business* anywhere in the world.

1.4.3 Application of AML/CFT Codes of Practice to Schedule 2 Business Carried on Outside Jersey (overseas)

46. By virtue of Articles 5, 6 and 22 of the *Supervisory Bodies Law*, a company incorporated in Jersey that carries on a *financial services business* through an overseas branch must comply with the *AML/CFT Code of Practice* in respect of that business, irrespective of whether it also carries on *financial services business* in or from within Jersey.

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

48. By virtue of the *AML/CFT Codes of Practice* set in Section 2.7, a person who (i) is a legal person registered, incorporated or otherwise established under Jersey law[4], but who is not a Jersey incorporated company; and (ii) carries on a *financial services business* in or from within Jersey, must apply measures that are at least equivalent to *AML/CFT Codes of Practice* in respect of any *financial services business* carried on by that person through an overseas branch. This requirement will apply to a foundation or partnership established under Jersey law.

49. Where overseas provisions prohibit compliance with one or more of the *AML/CFT Codes of Practice* (or measures that are at least equivalent), then by virtue of the *AML/CFT Codes of*

[4] 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. 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.

Practice set in section 2.7, requirements do not apply and the *Commission* must be informed that this is the case. In such circumstances, the *AML/CFT Codes of Practice* require a person to take other reasonable steps to effectively deal with the risk of *money laundering* and the *financing of terrorism*.

1.5 Definition and overview of Accountants undertaking Schedule 2 Business

50. Article 36 of the *Proceeds of Crime Law* defines "*financial services business*" through Schedule 2 to the *Proceeds of Crime Law*.

51. 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 anti-money laundering 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;
  - *audit services*; and
  - *insolvency services*.
- **'*External accountancy services*'** means *accountancy services* provided to third parties and excludes services provided by accountants employed by public authorities or by undertakings which do not by way of business provide *accountancy services* to third parties.
- **'*Audit services*'** are *audit services* provided by way of business pursuant to any function under any enactment.
- **'*Insolvency services*'** are services provided by a person if, by way of business, that person accepts appointment as:
- a liquidator under Chapter 4 of Part 21 of the Companies (Jersey) Law 1991;
- an insolvency manager appointed under Part 5 of the Limited Liability Partnership (Jersey) Law 1997 as that Law has effect in its application to insolvent limited liability partnerships pursuant to the Limited Liability Partnerships (Insolvency Partnerships) (Jersey) Regulations 1998; or
- as agent of an official functionary appointed in the case of a remise de biens, cession, or désastre.

1.5.1 Accountancy Services

52. For the purpose of this Handbook, '*accountancy services*' includes any service provided under a contract for services (i.e. not a contract of employment) which pertains to the recording, review, analysis, calculation or reporting of financial information.

53. Businesses that are not providing Schedule 2 business are outside the scope of this 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.

54. 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* and the *financing of terrorism*.

55. 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 supply any Schedule 2 business when acting under a contract for services in the course of business.

1.5.2 Tax Advisers

56. For the purpose of this Handbook, those in business offering tax services are referred to as 'tax advisers'.

57. The meaning of 'advice' can be widely interpreted and the *Commission* believes it would be prudent to take the view that the provision of tax compliance services come within its definition.

58. A tax adviser should be aware of the *Commission's* responsibility to regulate trust and company business, which may impinge upon the work they undertake for their clients.

59. Whilst tax advisers are more likely to identify offences relating to the avoidance or detection of tax offences, they need to be aware of the potential requirement to report knowledge or suspicion of proceeds derived from any serious crime[5] which is encountered in the course of business as a tax adviser.

1.5.3 Audit Services

60. The use of the term '*auditor*' in this Handbook means anyone who is part of the *engagement team* (not necessarily only those employed by an audit firm). The *engagement team* comprises all persons who are directly involved in the acceptance and performance of a particular audit. 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 firm.

61. The extent to which *money laundering* legislation affects the *auditor*'s work differs between two broad categories of audit:

    › **Audits of relevant persons**. Regulated *financial services businesses* and those undertaking Schedule 2 business are required to comply with the requirements of the *Money Laundering Order* which place additional obligations on them to combat *money laundering* and the *financing of terrorism*. All such businesses are required to comply with the *AML/CFT Codes of Practice* and best practice guidance issued by the *Commission* (see Section 2.5.3 of this Handbook).

62. In addition to reporting on their financial statements, *auditor*s of such businesses are required to report to the *Commission* 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 8.8 of this Handbook). Therefore, *auditor*s of such businesses should not only be aware of the key provisions contained in the *Money Laundering Order* as they affect *auditor*s themselves, but also the requirements of the relevant *AML/CFT Handbook*, issued by the *Commission*, covering the business that they are auditing.

    › **Audits of other types of entity.** In general, *auditor*s 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* or the *financing of terrorism* is taking place.

---

[5] Serious crime is defined by the *Proceeds of Crime Law* as any criminal offence which is subject on conviction to a term of imprisonment of one year or more.

63. Whilst *auditor*s have no statutory responsibility to undertake work solely for the purpose of detecting *money laundering* and the *financing of terrorism*, they nevertheless need to take the possibility of *money laundering* and the *financing of terrorism* into account in the course of carrying out procedures relating to fraud and compliance with the *money laundering* legislation. An *auditor*'s wide access to documents and systems, and the need to understand the business, can make him ideally suited to spot such issues as they arise.

64. However, *auditor*s cannot be held responsible for the prevention of, and failure to detect, *money laundering* and *financing of terrorism* activities in the entities they audit. External *auditor*s performing financial statement audits within a short timescale are less likely than other professional accountants (such as forensic accountants and accountants in management positions) to encounter signs of possible *money laundering* and the *financing of terrorism*. Neither is it the *auditors*' responsibility to detect suspicious activity in connection with a compliance or operational audit of an *AML/CFT* programme or testing a suspicious activity reporting process.

1.5.4 Insolvency Practitioners

65. For the purpose of this Handbook, those in the business of undertaking *insolvency services* are referred to as '*insolvency practitioners*'.

1.5.5 Accountants undertaking Regulated Business

66. 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; and
- arranging loans.

67. Consequently, some accountancy firms are authorised and regulated by the *Commission* under the Financial Services (Jersey) Law 1998 and subject to one or more of the Investment Business, Trust Company Business and Funds Services Business Codes of Practice. Firms who are so regulated should refer to the separate *AML/CFT Handbook* when drawing up their *policies and procedures* for the prevention of and detection of *money laundering* and the *financing of terrorism* in respect of those regulated activities.

1.6 Risk Based Approach

Overview

68. The possibility of being used to assist with *money laundering* and the *financing of terrorism* poses many risks for the accountancy sector including:

- criminal and disciplinary sanctions for firms and for individuals;
- civil action against the firm as a whole and against individual members of senior management; and
- damage to reputation leading to loss of business.

69. These risks must be identified, assessed and mitigated in the same way as for all business risks faced by a firm.

70. To assist the overall objective to prevent *money laundering* and terrorist financing, the *Money Laundering Order* and this Handbook adopt a risk-based approach. Such an approach:

- recognises that the *money laundering* and the *financing of terrorism* threats to a firm vary across clients, countries and territories, services and delivery channels;
- allows a firm to differentiate between clients in a way that matches risk in a particular firm;
- while establishing minimum standards, allows a firm to apply its own approach to *systems and controls* and other arrangements in particular circumstances; and
- helps to produce a more cost effective system.

71. Nevertheless, it must be accepted that applying the risk-based approach will vary between firms and may not provide a level playing field.

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

73. Inter alia, Part 3 of the *AML/CFT Handbook* sets out in further detail the *Commission*'s expectations of a soundly reasoned risk based approach.

74. An effective and documented risk-based approach will enable a firm to justify its position on managing *money laundering* and terrorist risks to law enforcement, the courts, regulators and supervisory bodies.

Statutory Requirements

75. *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.*

1.7 Equivalence of Requirements in Other Countries and Territories

1.7.1 Equivalent business

76. Article 16 and Part 3A of the *Money Laundering Order* respectively permit reliance to be placed on an *obliged person* (a term that is defined in Article 1(1)) and exemptions from customer due diligence requirements to be applied to a client carrying on a *financial services business* that is overseen for *AML/CFT*[6] compliance in Jersey or carrying on business that is "**equivalent business**". Sections dealing with the acquisition of a business or block of clients and verification of identity concession also provide concessions from *AML/CFT Codes of Practice* on a similar basis.

77. Article 5 of the *Money Laundering Order* defines *equivalent business* as being overseas business that:

- if carried on in Jersey would be *financial services business*;

[6] AML/CFT means Anti-money Laundering / Countering the Financing of Terrorism

- › may only be carried on in the country or territory by a person registered or otherwise authorised under the law of that country or territory to carry on that business;
- › is subject to requirements to forestall and prevent *money laundering* and the *financing of terrorism* consistent with those in the *FATF* Recommendations in respect of that business; and
- › is supervised for compliance with those requirements by an overseas regulatory authority.

78. The condition requiring that the overseas 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, inter alia, where a person is located in an equivalent country or territory.

1.7.2 Equivalent Countries and Territories

79. With effect from 31 May 2021 the Commission no longer maintains a list of Equivalent Countries and Territories in Appendix B. Guidance to assist relevant persons to determine equivalence is set out in Section 1.7.3.

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

a. financial institutions and designated non-financial businesses and professions are required to take measures to forestall and prevent money laundering and the financing of terrorism that are consistent with those in the *FATF* Recommendations.

b. financial institutions and designated non-financial businesses and professions are supervised for compliance with those requirements by a regulatory or supervisory authority.

1.7.3 Determining Equivalence

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

82. In determining whether or not the requirements for measures to be taken in a country or territory are consistent with the *FATF* Recommendations, a *relevant 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* (including Gibraltar) or a member of the European Economic Area (***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 designated non-financial business or profession (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* and the *financing of terrorism*, such as those conducted by the *FATF*, *FATF* Style Regional Bodies, the International Monetary Fund (the ***IMF***) and the World Bank (and published remediation plans); and

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

83. Where a firm assesses whether a country or territory not listed by the *Commission* is an equivalent country or territory, it 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.

84. Hyperlinks to where additional information may be located are included below. 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.

- Financial Action Task Force ratings table: http://www.fatf-gafi.org/media/fatf/documents/4th-Round-Ratings.pdf
- Financial Action Task Force – High jurisdictions and other monitored jurisdictions: http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)
- Financial Action Task Force - Mutual Evaluation Reports: http://www.fatf-gafi.org/publications/mutualevaluations/?hf=10&b=0&s=desc(fatf_releasedate)
- *Financial Action Task Force*–style summary evaluations are published in FATF Annual Reports: www.fatf-gafi.org
- International Monetary Fund: www.imf.org
- The World Bank: www.worldbank.org
- MONEYVAL: www.coe.int/Moneyval
- The Offshore Group of Banking Supervisors (OGBS): www.ogbs.net
- The Caribbean Financial Action Task force (CFATF): www.cfatf.org
- The Asia/Pacific Group on Money laundering (APG): www.apgml.org
- The Intergovernmental Action Group against Money-Laundering in Africa (GIABA): www.giabasn.org
- The Middle East and North Africa Financial Action Task Force (MENAFATF): www.menafatf.org
- The Financial Action Task Force in South America: www.gafisud.org
- The Eastern and Southern Africa Anti-Money Laundering Group (EASSMLG): www.esaamlg.org
- The Eurasian Group (EAG): www.euroasiangroup.org

2 CORPORATE GOVERNANCE

Please Note:

- Regulatory requirements are set within this section as *AML/CFT Codes of Practice*.
- This section contains references to Jersey legislation which may be accessed through the JFSC website.
- Where terms appear in the Glossary this is highlighted by the use of italic text. The Glossary is available from the JFSC website.

2.1 Overview of Section

1. Corporate governance is the system by which enterprises are directed and controlled and their business risks managed. For those firms undertaking Schedule 2 business, *money laundering* and the *financing of terrorism* are risks that must be managed in the same way as other business risks.
2. On the basis that accountancy firms tend to be partnerships, rather than this Handbook referring to the responsibilities of "the Board" (as is the case in the *AML/CFT Handbook*) it refers to the responsibilities of the senior management of the firm. In the case of a sole trader, senior management will be the sole trader.
3. A sole practitioner will not necessarily be a sole trader[1].
4. Under the general heading of corporate governance, this Section therefore considers:
   - senior management responsibilities for the prevention and detection of *money laundering* and the *financing of terrorism*;
   - requirements for *systems and controls*, training and awareness; and
   - the appointment of a Money Laundering Compliance Officer (***MLCO***) and Money Laundering Reporting Officer (***MLRO***).
5. This Handbook describes the requirements for a firm's general framework of *systems and controls* to combat *money laundering* and the *financing of terrorism* as its "***systems and controls***". This Handbook refers to the way in which those *systems and controls* are to be implemented into the day-to-day operation of a firm as its "***policies and procedures***".

2.2 Measures to Prevent Money Laundering and the Financing of Terrorism

Statutory Requirements

6. *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.*

[1] "sole trader" is defined in Article 1(1) of the Money Laundering Order

7. *Article 37 of the Proceeds of Crime Law enables the Chief Minister to prescribe by Order the measures that must be taken by a relevant person. These measures are established in the Money Laundering Order.*

2.3 Senior Management Responsibilities

Overview

8. The key responsibilities of senior management, set out in further detail below, are to:
   - identify the firm's money laundering and the financing of terrorism risks;
   - ensure that its *systems and controls* are appropriately designed and implemented to manage those risks; and
   - ensure that sufficient resources are devoted to achieving these objectives.

9. Senior management is assisted in fulfilling these responsibilities by a *MLCO* and *MLRO*. Larger or more complex firms may also require dedicated risk or compliance functions to assist in the assessment and management of *money laundering* and the *financing of terrorism* risk.

Statutory Requirements

10. *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.*

11. *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 relevant services (**relevant employees**) aware of policies and procedures required under Article 11(1) of the Money Laundering Order and of Jersey's money laundering legislation. Article 11(10) of the Money Laundering Order requires a relevant person to provide relevant employees whose duties relate to the provision of relevant services 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 the financing of terrorism.*

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

13. *Articles 7 and 8 of the Money Laundering Order require that a relevant person appoints a MLCO and a MLRO.*

AML/CFT Codes of Practice

14. Senior management must conduct and record a business risk assessment. In particular, Senior management must consider, on an ongoing basis, its risk appetite, and the extent of its exposure to *money laundering* and the *financing of terrorism* risks "in the round" or as a whole by reference to its organisational structure, its clients, the countries and territories with which its clients are connected, its range of services, and how it delivers those services. The assessment must consider the cumulative effect of risks identified, which may exceed the sum of each individual risk element. Senior management's assessment must be kept up to date (see Section 2.3.1 below).

15. On the basis of its business risk assessment, Senior Management must establish a formal strategy to counter *money laundering* and the *financing of terrorism*. Where a Jersey firm forms part of a group operating outside the Island, that strategy may protect both its global reputation and its Jersey business.

16. Senior management must record the results of its business risk assessment and keep the assessment under review.

17. Taking into account the conclusions of the business risk assessment, senior management must: (i) organise and control the firm's affairs in a way that effectively mitigates the risks that it has identified, including areas that are complex; and (ii) be able to demonstrate the existence of adequate and effective *systems and controls* (including *policies and procedures*) to counter *money laundering* and the *financing of terrorism* (see Section 2.4).

18. Senior management must document its *systems and controls* (including *policies and procedures*) and clearly apportion responsibilities for countering *money laundering* and the *financing of terrorism*, and, in particular, responsibilities of the *MLCO* and *MLRO* (See Sections 2.5 and 2.6).

19. Senior management 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).

20. Senior management 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* and the *financing of terrorism*, and must take effective measures to address them (see Section 2.4.3).

21. Senior management must notify the *Commission* immediately in writing of any material failures to comply with the requirements of the *Money Laundering Order* or of this Handbook. Refer to Part 3 of the *AML/CFT Handbook* for further information.

2.3.1 Business Risk Assessment

AML/CFT Codes of Practice

1. A *firm* must maintain appropriate policies and procedures to enable it, when requested by the JFSC, to make available to that authority a copy of its business risk assessment.

Guidance Notes

22. Professional firms are likely to already have in place *policies and procedures* to minimise professional, client and legal risk. A firm may extend its existing risk management systems to address *AML/CFT* risks. The detail and sophistication of these systems will depend on the firm's size and the complexity of the business it undertakes. Ways of incorporating a firms' business risk assessment will be governed by the size of the firm and how regularly compliance staff and senior management are involved in day-to-day activities.

23. Senior management of a firm may demonstrate that it has considered its exposure to *money laundering* and the *financing of terrorism* risk by:

    - involving all members of senior management in determining the risks posed by *money laundering* and the *financing of terrorism* within those areas for which they have responsibility;
    - considering organisational factors that may increase the level of exposure to the risk of *money laundering* and the *financing of terrorism*, e.g. business volumes and 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 clients are and what they do;
- considering whether any additional risks are posed by the countries and territories with which the firm or its clients are connected. Factors such as high levels of organised crime, increased vulnerabilities to corruption and inadequate frameworks to prevent and detect *money laundering* and the *financing of terrorism* will impact the risk posed by relationships connected with such countries and territories;
- considering the risk that is involved in placing reliance on *obliged person*s to apply *reliance identification measures*;
- considering the characteristics of its service areas and assessing the associated vulnerabilities posed by each service area. For example:
    a. assessing how legal entities and structures might be used to mask the identities of the underlying beneficial owners; and
    b. considering how the firm establishes and delivers services to its clients. For example, risks are likely to be greater where relationships may be established remotely (non-face to face); and
- considering the accumulation of risk for more complex clients.

24. In developing a risk-based approach, firms need to ensure that it is readily comprehensible to senior management, other *relevant employees* and relevant third parties e.g. *auditor*s and the *Commission*.

25. In the case of a firm that is dynamic and growing, senior management may demonstrate that its business risk assessment is kept up to date where it is reviewed annually. In some other cases, this may be too often e.g. a firm with stable services or smaller well-established business. In all cases, senior management may demonstrate that its business risk assessment is kept up to date where it is reviewed when events (internal and external) occur that may materially change *money laundering* and the *financing of terrorism* risk.

2.3.1.1 Considering Client and Service Risks to the Business

Overview

26. The business risk assessment relating to clients and services will depend on the firm's size, type of clients and the practice area it engages in.

27. Firms 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 firm may be used to launder funds or assets through the firm or, alternatively, that the client or its counterparties may launder criminal funds or assets, but in a way that does not touch the accountancy firm.

Accountancy, Audit and Insolvency Service Risk

28. Those providing accountancy, auditing or *insolvency services* will primarily need to consider their business risk assessment in respect of the nature of their client base, the business sectors in which their clients operate and the geographical location of their clients. The standing of clients and adherence to sound corporate governance principles will also have an impact including those clients that have previously been prosecuted or fined for criminal or regulatory offences.

29. The business risk assessment should take account of the following risks:

    - setting up, winding up, or effecting recovery for high cash turnover businesses for clients 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* and the *financing of terrorism* attaching to the client and/or those who trade with or otherwise interact with clients.
    - 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).

30. Specialisation within a sector that undertakes higher risk activity from a *money laundering* and the *financing of terrorism* perspective will affect the business risk assessment. Examples of higher risk sectors and sensitive business areas for *money laundering* and the *financing of terrorism* purposes are:

    - financial services and 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; and
    - arms and armaments.

31. Firms 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.

Taxation Service Risk

32. Tax practitioners 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, 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 enhance the risks of the tax practitioner becoming concerned in an arrangement are:

- 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; and
- fraudulent evasion of Value Added Tax (***VAT***) by clients operating within the European Union including the possession and dealing in goods on which *VAT* has been evaded (e.g. Missing Trader Intra Community/Carousel fraud).

2.4 Adequate and Effective Systems and Controls

Overview

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

Statutory Requirements

34. *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.*

35. *Parts 3, 3A, 4 and 5 of the Money Laundering Order set out the measures that are to be applied in respect of customer due diligence, record keeping and reporting.*

36. *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.*

37. *Article 11(3) lists a number of policies and procedures that must be established and maintained.*

38. *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 whose duties relate to the provision of financial services 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.*

39. *Article 11(11) of the Money Laundering Order requires a relevant person to establish and maintain policies and procedures for: (i) monitoring compliance with, and testing the effectiveness of, its policies and procedures; and (ii) monitoring and testing the effectiveness of measures to promote awareness and training of relevant employees.*

40. *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 the financing of terrorism and matters that have an impact on that risk, such as the size and structure of the relevant person.*

41. *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)*

AML/CFT Codes of Practice

42. A firm must establish and maintain appropriate and consistent *systems and controls* to prevent and detect *money laundering* and the *financing of terrorism*, 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;
- report to the Joint Financial Crimes Unit (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 *Commission* and the *JFCU* on matters concerning vigilance, *systems and controls* (including *policies and procedures*);
- communicate *policies and procedures* to overseas branches and subsidiaries, and monitor compliance therewith; and
- monitor and review instances where exemptions are granted to *policies and procedures*, or where controls are overridden.

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

- client acceptance (and rejection), including approval levels for higher risk clients;

- the use of transaction limits and management approval for higher risk clients;
- 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; and
- taking action to comply with *Terrorist Sanctions Measures* and the *Directions Law*.

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

Guidance Notes

45. Whilst the *Money Laundering Order*, and consequently this Handbook, only brings within its scope the business activities of firms where they are carrying on Schedule 2 business, the primary *money laundering* legislation and the general offences and penalties cover all persons and all business activities within Jersey. Consequently, firms may wish to consider applying the *systems and controls* to counter *money laundering* and the *financing of terrorism* across the whole of their business activities, regardless of whether they are defined as Schedule 2 business.

2.4.1 Effectiveness of Systems and Controls

Guidance Notes

46. A firm may demonstrate that it checks that *systems and controls* (including *policies and procedures*) are adequate and operating effectively where senior management 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 *Commission* or *JFCU*, e.g. findings of supervisory and themed examinations and typologies;
    - changes made or proposed in respect of new legislation, *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law* or guidance;
    - resources available to comply with the *money laundering* legislation, the *Money Laundering Order* and *AML/CFT 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.
47. A firm may demonstrate that it checks that *systems and controls* (including *policies and procedures*) are operating effectively where senior management 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 the *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 clients that have been assessed by the firm as presenting a higher risk;
- the number of applications to establish business relationships or carry out one-off transactions 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 clients" that have still to be remediated under Section 4.7.2;
- details of failures by an *obliged person* or client 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 ongoing monitoring systems;
- the number of internal *SAR*s made to the *MLRO* (or *deputy MLRO*), the number of subsequent external *SAR*s submitted to the *JFCU*, and the timelines 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 awareness of *relevant employee*s 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.

48. The level of *systems and controls*, and the extent to which monitoring needs to take place will be affected by:
    - the firm'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 sells those services;
    - the type of business transactions it becomes involved in or advises on; and
    - its overall risk profile.

49. Issues which may 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;
    - *CDD* requirements to be met for standard and enhanced due diligence;
    - when outsourcing of *CDD* obligations or reliance on third parties will be permitted, and on what conditions;
    - how the firm will restrict work being conducted on a file where *CDD* has not been completed;
    - the circumstances in which delayed *CDD* is permitted;
    - when cash payments will be accepted;

- when payments, including payment of fees, will be accepted from, or made to, third parties; and
- the manner in which disclosures are to be made to the *MLRO*.

2.4.2 Testing of Compliance with Systems and Controls

Guidance Notes

50. A firm may demonstrate that it has tested compliance with *systems and controls* (including *policies and procedures*) where senior management 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.

51. A firm 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 paragraph 50 above, and in particular:

- the application of simplified and enhanced *CDD* measures;
- reliance placed on *obliged person*s 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 *Terrorist Sanctions Measures* and the *Directions Law*;
- 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

52. The implementation of *systems and controls* (including *policies and procedures*) for the prevention and detection of *money laundering* and the *financing of terrorism* does not obviate the need for a firm to address cultural barriers that can prevent effective control. Human factors, such as the inter-relationships between different employees, and between employees and clients, can result in the creation of damaging barriers.

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

Guidance Notes

54. A firm 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* and the *financing of terrorism* where senior management considers the prevalence of the following factors:

- an unwillingness on the part of fee earners or other employees to subject high value (and therefore important) clients to effective *CDD* measures for commercial reasons;
- pressure applied by senior management or fee earners outside Jersey upon employees in Jersey to transact without first conducting all relevant client due diligence;
- undue influence exerted by relatively large clients in order to circumvent *CDD* measures;

- excessive pressure applied on fee earners to meet aggressive revenue-based targets, or where employee or fee earner 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 client service;
- design of the client risk classification system in a way that avoids rating any client as presenting higher risk;
- the inability of employees to understand the commercial rationale for client relationships, resulting in a failure to identify non-commercial and therefore potential *money laundering* and the *financing of terrorism* activity;
- negative handling by senior management or fee earners 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 management 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 fee earners or other employees with certain clients resulting in unusual, complex, 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* are ignored; and
- non-attendance of senior management at training sessions on the basis of 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

55. In a case where a firm outsources a particular activity, it bears the ultimate responsibility for the duties undertaken in its name. This will include the requirement to ensure that the external party has in place satisfactory *systems and controls* (including *policies and procedures*), and to ensure that those *systems and controls* (including *policies and procedures*) are kept up to date to reflect changes in requirements.

56. Depending on the nature and size of a firm, the roles of *MLCO* and *MLRO* may require additional support and resources. Where a firm 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 the respective roles, and senior management will remain responsible for overall compliance with the *money laundering* legislation and the *Money Laundering Order* (and by extension, this Handbook).

AML/CFT Codes of Practice

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

58. A firm must assess possible *money laundering* or the *financing of terrorism* risk associated with outsourced functions, record its assessment, and monitor any risk on an on-going basis.

59. Where an outsourced activity is a financial services or Schedule 2 activity, a firm must ensure 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 firm must ensure that knowledge, suspicion, or reasonable grounds for knowledge or suspicion of *money laundering* or financing terrorism activity are reported by the third party to the firm's *MLRO* (or *deputy MLRO*).

2.5 The Money Laundering Compliance Officer (MLCO)

Overview

61. The Money Laundering Order requires a firm to appoint an individual as *MLCO*, and task that individual with the function of monitoring its compliance with legislation in Jersey relating to *money laundering* and the *financing of terrorism* and *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law*, and reporting thereon to senior management. The objective of this requirement is to require firms to clearly demonstrate the means by which they ensure compliance with the requirements of the same.

62. The *Money Laundering Order* also requires a firm to maintain adequate procedures for: (i) monitoring compliance with, and testing the effectiveness of, *policies and procedures*; and (ii) 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 firm shall have regard to the risk of *money laundering* and the *financing of terrorism* and matters that have an impact on risk, such as size and structure of the firm'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

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 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 Commission in writing within one month when a person is approved as, or ceases to be a MLCO. However, Article 10 provides that the Commission may grant exemptions from this notification requirement by way of notice.*

AML/CFT Codes of Practice

68. A firm must appoint a *MLCO* that:

- is employed by the firm;
- is based in Jersey;
- has sufficient experience and skills.

69. A firm must ensure that the *MLCO*:

- has appropriate independence, in particular from client-facing, business development and system and control development roles;
- reports regularly and directly to senior management and has a sufficient level of authority within the firm so that senior management 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; and
- is fully aware of both their and the firm's obligations under the *money laundering* legislation and the *Money Laundering Order* and *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law*.

70. 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 firm must take action to appoint an appropriate member of senior management to the position on a temporary basis.

71. If temporary circumstances arise where the firm has a limited or inexperienced compliance resource, it must ensure that this resource is supported as necessary.

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

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

Guidance Notes

73. A firm may demonstrate that its *MLCO* is monitoring whether enactments and *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law* are being complied with where he or she:

- regularly monitors and tests compliance with *systems and controls* (including *policies and procedures*) in place to prevent and detect *money laundering* and the *financing of terrorism* – supported as necessary by a compliance or internal audit function;
- reports periodically, as appropriate, to senior management on compliance with the firm's *systems and controls* (including *policies and procedures*) and issues that need to be brought to its attention; and
- responds promptly to requests for information made by the *Commission* and the *JFCU*.

2.6 The Money Laundering Reporting Officer (MLRO)

Overview

74. 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 firms, it may be appropriate to designate additional persons (***deputy MLROs***) to whom *SAR*s may be made.

Statutory Requirements

75. *Article 8 of the Money Laundering Order requires a firm 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.*

76. *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.*

77. *Article 8(4) of the Money Laundering Order requires a relevant person to notify the Commission in writing within one month when a person is appointed as, or ceases to be a MLRO. However, Article 10 provides that the Commission may grant exemptions from this notification requirement by way of notice.*

78. *Article 9 of the Money Laundering Order allows a relevant person to designate one or more persons (deputy MLROs), in addition to the MLRO, to whom internal SARs may be made.*

AML/CFT Codes of Practice

79. A firm must appoint a *MLRO* that:

- is employed by the firm;
- is based in Jersey; and
- has sufficient experience and skills.

80. A firm must ensure that the *MLRO*:

- has appropriate independence, in particular from client-facing and business development roles;
- has a sufficient level of authority within the firm;
- has sufficient resources, including sufficient time, and (if appropriate) is supported by *deputy MLRO*s;
- is able to raise issues directly with senior management;
- maintains a record of all enquiries received from law enforcement authorities and records relating to all internal and external suspicious activity reports;
- is fully aware of both *his* and the firm's obligations under the *money laundering* legislation, the *Money Laundering Order* and *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law*;
- ensures that relationships are managed effectively post disclosure to avoid tipping-off any third parties; and
- acts as the liaison point with the *Commission* and the *JFCU* and in any other third party enquiries in relation to *money laundering* or the *financing of terrorism*.

81. Where a firm has appointed one or more *deputy MLRO*s, it must ensure that the requirements set out above for the *MLRO* are also applied to any *deputy MLRO*s.

82. Where a firm has appointed one or more *deputy MLRO*s, it must ensure that the *MLRO*:

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

83. 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 firm must take action to appoint an appropriate member of senior management to the position on a temporary basis.

84. If temporary circumstances arise where a firm has a limited or inexperienced *money laundering* reporting resource, the firm must ensure that this resource is supported as necessary.

Guidance Notes

85. A firm may demonstrate that its *MLRO* (and any *deputy MLRO*) is receiving and considering *SAR*s in accordance with Article 21 of the *Money Laundering Order* where, inter alia, its *MLRO*:

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

86. A firm may demonstrate routine monitoring of the performance of any *deputy MLRO*s by requiring the *MLRO* to review:

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

2.7 Financial Groups

Overview

87. A Financial Group of which a firm is a member must maintain a group programme for the sharing of AML/CFT information. In addition, as explained in Section 1.4.3, where a company incorporated in Jersey carries on a *financial services business* through an overseas branch, it must comply with *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law* in respect of that business, irrespective of whether it also carries on *financial services business* in or from within Jersey.

Statutory Requirements

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

89. *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 risk;*
- *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); and*
- *the screening of employees*

90. *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 Codes of Practice

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

92. A person who:

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

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

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

3 IDENTIFICATION MEASURES: OVERVIEW

Please Note:

- Regulatory requirements are set within this section as *AML/CFT Codes of Practice*.
- This section contains references to Jersey legislation which may be accessed through the JFSC website.
- Where terms appear in the Glossary this is highlighted by the use of italic text. The Glossary is available from the JFSC website.

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 firm 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 *identification measures*; and
   - Section 7 - which explains the application of enhanced CDD measures (including the case of a client that is assessed as presenting a higher risk) and simplified *identification measures*.

3. Sound *identification measures* are vital because they:
   - help to protect the firm and the integrity of the professional and financial sector in which it operates by reducing the likelihood of the business becoming a vehicle for, or a victim of, financial crime;
   - assist law enforcement, by providing available information on applicants for business, clients 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; and
   - help to guard against identity fraud.

4. The inadequacy or absence of *identification measures* can subject a firm to serious client 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 business employees to determine whether a SAR is appropriate.

5. A client may be an individual (or group of individuals) or legal person. Section 4.3 deals with a client who is an individual (or group of individuals), Section 4.4 deals with a client (an individual or legal person) who is acting for a legal arrangement, and Section 4.5 deals with a client who is a legal person.

6. Throughout this Section, references to “client” include, where appropriate, a prospective client (an applicant for business). A “client” is a person with whom a business relationship has been formed or one-off transaction conducted.

3.2 Obligation to Apply Identification Measures

Statutory Requirements

7. *Article 13(1) of the Money Laundering Order requires a relevant person to apply CDD measures. CDD measures comprise identification measures and ongoing 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 client and verifying the authority of any person purporting so to act. See Article 3(2)(aa) of the Money Laundering Order.*
   - *Where the client is a legal person, understanding the ownership and control structure of that client and the provisions under which the client can enter into contracts, or other similarly legal binding arrangements, with third parties. See Article 3(2)(c)(ii) of the Money Laundering Order.*
   - *Where the client is a legal person, finding out the identity of individuals who are the beneficial owners or controllers of the client and obtaining evidence of the identity of those individuals. See Article 3(2)(c)(iii) of the Money Laundering Order.*
   - *Determining whether the client 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 client 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 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 client is acting for a third party, and where the client is a legal person, measures for obtaining evidence of identity for third parties, persons purporting to act on behalf of the client, and individuals who are the client'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; and*
- *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, the securities of which are listed on a regulated market.*

Ongoing monitoring

14. *Article 3(3) of the Money Laundering Order sets out what ongoing 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 client, including the client'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 clients. See Article 3(3)(b) of the Money Laundering Order.*

Policies and procedures

15. *Inter alia, 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; and*
- *the type of clients, business relationships, products and transactions with which the relevant person's business is concerned.*

16. Inter alia, 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 AML/CFT counter-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 organization that is subject to AML/CFT counter-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.

3.3 Risk Based Approach to Identification Measures

Overview

19. 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* and the *financing of terrorism* risk faced by a firm. While these stages must be incorporated into a firm's *policies and procedures*, they do not need to take place in the sequence outlined below, and will often occur simultaneously.

20. The risk assessment of a particular client will determine the extent of information that 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.

21. Section 2.3 of this Handbook requires senior management to conduct (and keep up to date) a business risk assessment, which considers the business' risk appetite, activities and structure and concludes on the business' exposure to *money laundering* and the *financing of terrorism* risk.

22. This business risk assessment will enable a firm to determine its initial approach to performing Stage 1 of the identification process set out below, depending on the type of client, or service involved. The remaining stages of the process require consideration as to whether the specific circumstances of the client will necessitate the application of further measures.

23. Part 3A of the *Money Laundering Order* sets out exemptions from client due diligence 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 relevant person who is exempt from applying third party identification requirements (see Article 17D).

24. The following are stages in the identification process:

Stage	Identification measure	Article(s)	Guidance
1.1	In the case of a client that is a legal person, a firm must understand the ownership and control structure of the client (and provisions under which the client can enter into contracts).	3(2)(c)(ii)	Section 3.3.1
1.2	A firm must find out the identity of: › the client; › any beneficial owners and controllers of the client; › any third party (or parties)[1] – including a legal arrangement - on whose behalf the client acts, whether directly or indirectly (and beneficial owners and controllers of the third party (or parties)); and › others listed in Article 3(2).	3(2)(a) to (c) 3(4)(a)	Section 4
1.3	A firm must obtain information on the purpose and intended nature of the business relationship or one-off transaction.	3(2)(d)	
1.4	A firm must obtain appropriate information for assessing the risk that a business relationship or one-off transaction will involve *money laundering* or the *financing of terrorism* risk. 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 firm 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* or the *financing of terrorism* risk (risk profile).	3(5)	Section 3.3.4
2.2	A firm must prepare and record a client business and risk profile.	3(3)(a)	Section 3.3.5
3	A firm 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

25. By virtue of ongoing monitoring, particularly in relation to higher risk categories of clients, under Article 3(3)(b) of the *Money Laundering Order*, a firm must keep documents, data and information obtained under Stages 1 and 3 up to date and relevant. See Section 3.4.

26. *Systems and controls* (including *policies and procedures*) will not detect and prevent all instances of *money laundering* or the *financing of terrorism*. A risk-based approach will, however, serve to balance the cost burden placed on a firm and on clients with the risk that

[1] For the avoidance of doubt, this will include any person who is a named beneficiary of a life assurance policy entered into by the client.

the firm may be used in *money laundering* or to finance terrorism by focusing resources on higher risk areas.

27. Care has to be exercised under a risk-based approach. Being identified as carrying a higher risk of *money laundering* or the *financing of terrorism* does not automatically mean that a client is a money launderer or is financing terrorism. Similarly, identifying a client as carrying a lower risk of *money laundering* or the *financing of terrorism* does not mean that the client is not a money launderer or financing terrorism.

AML/CFT Codes of Practice

28. A firm 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 Structures – Stage 1.1

Overview

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

30. Understanding ownership involves taking three separate steps: requesting information from the client (or a professional); validating that information; and checking that information held makes sense.

Guidance Notes

Step 1

31. A firm may demonstrate that it understands the ownership and control structure of a client that is a legal person where it applies one of the following *identification measures*:

- it requests the client to provide a statement of legal and beneficial ownership and control as part of its application to become a client. In the case of a legal person that is part of a group, this will include a group structure.
- to the extent that a client 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.

Step 2

32. A firm may demonstrate that it understands the legal ownership and control structure of a client that is a legal person where it takes into account information that is held: (i) by the client, e.g. recorded in its share register; (ii) by a lawyer, accountant or trust and company services provider; (iii) 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; or (iv) publicly, e.g. information that is held in a central register in the country of establishment.

33. A firm 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 client, e.g. in line with company law, *AML/CFT* 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* 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; or
- publicly available, e.g. in commercial databases and press reports.

Step 3

34. A firm may demonstrate that it understands the ownership and control structure of a client 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

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

All client types	
All client types	› Type, volume and value of activity expected (having regard for the Commission's Sound Business Practice Policy[2]). › *Source of funds*, e.g. nature and details of occupation or employment. › Details of any existing relationships with the firm.
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 *Commission*'s Sound Business Practice Policy and trading activities). › Geographical sphere of activities and assets. › Name of regulator, if applicable.

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

[2] https://www.jerseyfsc.org/industry/guidance-and-policy/sound-business-practice-policy/

3.3.2.1 Engagement Letters

Overview

37. It may be helpful to explain to the client the reason for requiring *CDD* information and for the client identification procedures. This can be achieved by including an additional paragraph in the engagement letter or in pre-engagement communications.

38. It may also be helpful to inform clients of the firm's reporting responsibilities under the primary legislation and the restrictions created by the 'tipping-off' rule on the firm's ability to discuss such matters with its clients.

39. Whether or not to advise the client of these issues is a decision to be taken by individual firms. However, if it is to be done it is important that the policy should apply consistently across the board for all clients. A decision only to do so once a suspicion had arisen could result in the firm committing a tipping-off offence (see Section 8.5 of this Handbook)

3.3.2.2 Specific Issues that Might be Covered When Drawing Up a Profile

Overview

40. The following list sets out suggested questions that might need to be answered to assist in developing the profile for a business or corporate client. Firms should amend the questions and focus to suit their own client base and services offered.

For entities/businesses

- What is its purpose in entering into any activity/transaction forming the basis of the proposed engagement or its purpose in seeking services where not related to a specific transaction?
- What are the entity's main trading and registered office addresses?
- What are its business activities or purposes and sector?
- Who controls and manages it (i.e. has executive power over the entity – this may be directors, shadow directors or others depending on the circumstances)?
- If the client is audited, were the accounts qualified and, if so, why?
- Are the persons purporting to represent the entity who they say they are?
- Who owns it i.e. ultimate beneficial owner(s) and the steps in between?
- What is its business model/intended business model (i.e. the mechanism by which a business intends to generate revenue and profits and serve its customers – in terms of broad principles)?
- What are the key sources of:
  - income (e.g. trading, investment etc); and
  - capital (e.g. public share offer, private investment etc)?
  - What is the historical and current (also forecast if readily available) scale of the entity's:
  - earnings (e.g. turnover and profits/losses); and
  - net assets?
- What are the entity's geographical connections (so that the firm is in a position to answer such questions as "why is it getting so much money from that location? and "why is it sending assets to that location?")?
- Has the entity been subject to insolvency proceedings, or is it in the course of being dissolved/struck off, or has it been dissolved/struck off?

For individuals

- What is their purpose in entering into any transaction forming the basis of the engagement or purpose in seeking services where not related to a specific transaction?
- What is their home address and, if applicable, different trading address?
- What is the scale and sources of the individual's capital (past and future)?
- What is the scale and sources of the individual's income (past and future)?
- What is the type and sector of the individual's business activities?
- What are the individual's geographical connections (so that the firm is in a position to answer such questions as "why is it getting so much money from that location? and "why is it sending assets to that location?")?
- Has the individual been subject to bankruptcy proceedings?
- Has the individual been disqualified as a director?

3.3.2.3 Insolvency Cases

Overview

41. In the context of insolvency work, the person or entity entering into the business relationship is considered to be the insolvent. An insolvency practitioner should risk assess, identify and verify the identity of the person or entity over which he is appointed. It is important for an officeholder to be sure about the identity of the person or entity over which he is taking appointment, given the urgency of the situation and the necessity not to delay when this might risk dissipation of assets and erosion of value.

3.3.2.4 Auditing Standards on Acceptance of Client Relationships

Overview

42. Auditing standards on quality control for audits state that acceptance of client relationships and specific audit engagements includes considering the integrity of the principal owners, key management and those charged with governance of the entity. This involves the auditor making appropriate enquiries and may involve discussions with third parties, the obtaining of written references and searches of relevant databases.

43. The extent of knowledge a firm will have regarding the integrity of a client will generally grow within the context of an ongoing relationship with that client. However, information at the start of a relationship may be obtained from a number of sources, for example:

    - the reasons for the proposed appointment of the firm and non-reappointment of the previous auditors;
    - communications with existing or previous providers of professional accountancy, banking and legal services to the client; and
    - background searches and relevant databases.

44. Whilst these procedures may provide some of the relevant client identification information, they will not be sufficient on their own to comply with the requirements of the *Money Laundering Order* and this Handbook.

3.3.3 Source of Funds – Stage 1.4

Overview

45. 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* and the *financing of terrorism* investigations. Understanding the *source of funds* and, in higher risk relationships, the client's *source of wealth* is also an important aspect of *CDD*.

46. ***Source of funds*** is the activity which generates the funds for a relationship e.g. a client's occupation or business activities. Information concerning the geographical sphere of the activities may also be relevant.

47. The *Money Laundering Order* and this Handbook stipulate record keeping requirements for transaction records which require information concerning the remittance of funds also 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 is the source of transfer and is not to be confused with *source of funds***.

48. ***Source of wealth*** is distinct from *source of funds*, and describes the activities which have generated the total net worth of a person both within and outside of a relationship, i.e. those activities which have generated a client's funds and property. Information concerning the geographical sphere of the activities that have generated a client's wealth may also be relevant.

49. In finding out *source of wealth* it will often not be necessary to determine the monetary value of an individual's net worth.

3.3.4 Assessment of Risk – Stage 2.1

Overview

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

51. In assessing client risk, the presence of one factor that might indicate higher risk will not automatically mean that a client is higher risk. Equally, the presence of one lower risk factor should not automatically lead to a determination that a client is lower risk.

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

53. Inconsistencies between information obtained, for example, between specific information concerning *source of funds* (or *source of wealth*), and the nature of expected activity may also assist in assessing risk.

Guidance Notes

54. A firm may demonstrate that it has assessed the risk that a business relationship or one-off transaction will involve *money laundering* or the *financing of terrorism* where it takes into account the factors set out below.

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

56. A firm may demonstrate that it has assessed the risk that a business relationship or one-off transaction will involve *money laundering* or the *financing of terrorism* where it takes into account the effect of a combination of a number of factors, e.g. the use of complex structures by a client who is a non-resident high-net worth individual in the course of wealth management, 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.

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

- The business of some firms, their products, and client 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 business' products are assessed to present, may be appropriate for most clients, with the focus being on those clients who fall outside the norm.
- Others may have a greater level of business, but large numbers of their clients 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 clients 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 clients may be considered to present a lower risk.

3.3.4.1 Factors to Consider

Service risk

58. Features that may be attractive to money launderers or those financing terrorism:

- Ability to make payments to, or receive from, external parties;
- Ability for clients to migrate from one service to another;
- Ability to hold boxes, parcels or sealed envelopes in safe custody for clients;
- Ability for clients to use "hold mail" facilities and "care of" addresses (other than temporary arrangements);
- Ability to place funds in client, nominee or other accounts, where funds are mingled with others' funds;
- Ability to place sealed parcels or sealed envelopes in safe custody;
- Ability to pool the funds of underlying clients within client accounts.

Delivery risk

59. Features that may be attractive to money launderers or those financing terrorism:

- Indirect relationship with the client – dealing through intermediaries or other third parties; and
- Non-face to face relationships – service delivered exclusively by post, telephone, internet etc. where there is no physical contact with the customer.

Client risk

60. Features that may be attractive to money launderers or those financing terrorism:

- Type of client. For example, an individual who has been entrusted with a prominent public function (or immediate family member or close associate of such an individual) may present a higher risk (as may a domestic politician);
- Nature and scope of business activities generating the funds/assets. For example, a client conducting "sensitive" activities (as defined by the *Commission* in its Sound Business Practice Policy) or conducting activities which are prohibited if carried on with certain countries; a client engaged in higher risk trading activities or engaged in a business which involves significant amounts of cash may indicate higher risk;
- Transparency of client. 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 Channel Islands Competition & Regulatory Authority may indicate lower risk. Clients 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 e.g. those with nominee directors or nominee shareholders or which have issued bearer shares;
- Reputation of client. For example, a well known, reputable person, with a long history in its industry, and with abundant independent and reliable information about it and its beneficial owners and controllers may indicate lower risk;
- Behaviour of client. For example, where there is no commercial rationale for the service that is being sought, or where undue levels of secrecy are requested by a client, or where a client 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, this may indicate higher risk;
- The regularity or duration of the relationship. For example, longstanding relationships involving frequent client contact that result in a high level of understanding of the client relationship may indicate lower risk;
- Type and complexity of relationship. For example, the use of overly complex or opaque structures with different layers of entities situated in two or more countries and cross border transactions involving counterparts in different parts of the world, the unexplained use of corporate structures and express trusts by clients, and the use of nominee and bearer shares may indicate higher risk;
- Value of client assets e.g. higher value;
- Value and frequency of cash or other "bearer" transactions (e.g. travellers' cheques and electronic money purses) e.g. higher value and/or frequency;
- Delegation of authority by the applicant or client. 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;
- In the case of an express trust, the nature of the relationship between the settlor(s) and beneficiaries with a vested right, 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; and

Client risk

› In the case of an express trust, the nature of classes of beneficiaries and classes within an expression of wishes. For example, a trust that is established for the benefit of the close family of the settlor may indicate a lower risk.

Country risk

61. Relevant connection to a country or territory that presents a higher risk of *money laundering* or the *financing of terrorism*, where the following types of countries or territories may be considered to present a higher risk:

› those that are generally considered to be un-cooperative in the fight against *money laundering* and the *financing of terrorism*;

› those with strategic deficiencies in the fight against ***money laundering*** **and the** ***financing of terrorism***, 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 United Nations (***UN***) or *EU* 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;

Country risk

- 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 .

62. Relevant connection to a country or territory that presents a lower risk of *money laundering* or the *financing of terrorism*, where the following factors may be considered to 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 and the Wassenaar Arrangement).
    - A favourable assessment by the Financial Stability Board concerning adherence to regulatory and supervisory standards on international **cooperation and information exchange**.
63. Familiarity of a firm 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 firm's own or group operations within that country.

3.3.4.2 External Data Sources

Overview

64. 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.
65. Information on the proliferation of nuclear and other weapons, and sanctions may be found on the *Commission*'s website.
66. Appendix D2 of the *AML/CFT Handbook* lists a number of countries and territories that are identified by reliable and independent external sources as presenting a higher risk. In assessing country risk for *AML/CFT* purposes, in addition to considering the particular features of a client, it will be relevant to take account of the number of occasions that a particular country or territory is listed for different reasons. Where a country or territory is identified as presenting a higher risk for different reasons by three, or four or more, separate external sources, it is more prominently highlighted in the appendix.

67. There are now also a number of providers of country risk "league tables" that rate countries according to risk (e.g. as lower, medium or higher risk), some of which 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.

68. External data sources may also assist in establishing customer specific risk. For example, electronic subscription databases list individuals entrusted with prominent public functions and a list of persons that are subject to financial sanctions may be accessed through the *Commission*'s website (UK Consolidated List).

3.3.5 Client Business Profile – Stage 2.2

Guidance Notes

69. A firm may demonstrate that it has prepared a client business profile where it enables it to.

- identify a pattern of expected transactions and activity within each business relationship; and
- recognise unusual transactions and activity, unusually large transactions or activity, and unusual patterns of transactions or activity.

70. For certain types of services, a firm may demonstrate that it has prepared a client business profile where it does so on the basis of generic attributes, so long as this enables it to recognise the transactions or activity referred to in paragraph 69 above. For more complex services, however, tailored activity profiles will be necessary.

3.4 On-Going Monitoring: Ensuring that Documents, Data and Information are up to Date and Remain Relevant

Overview

71. Article 3(3)(b) of the *Money Laundering Order* explains that ongoing 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.

72. Inter alia, where there is a change to information found out about the client, the client acts for a new third party, a new person purports to act for the client, or the client 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

73. A firm 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 client is requested to, and does provide, an assurance that he, she or it will update the information provided on a timely basis in the event of a subsequent change..

74. A firm 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" become apparent.

75. Trigger events e.g. when taking new instructions from a client, or meeting with a client, 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

76. Rather than establishing a business relationship directly with a client, a firm may establish that relationship through the transfer of a block of clients from another business. The transfer may be effected through legislation or with the agreement of the client.

Guidance Notes

77. A firm 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 *relevant person* or carrying on *equivalent business* as defined by Article 5 of the *Money Laundering Order* (refer to 1.7 of this Handbook); and
- the firm 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 and information for the business relationship to be acquired; and
- before, or at the time of the transfer, the firm obtains from the vendor all of the relevant documents, data or information (or copy thereof) held for each client acquired.

78. In a case where the vendor is not a *relevant person*, or is not carrying on *equivalent business* (refer to 1.7 of this Handbook), or where deficiencies in the vendor's *CDD policies and procedures* are identified (either at the time of transfer or subsequently), a firm 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 client and to remedy deficiencies which is agreed in advance with the *Commission*.

4 IDENTIFICATION MEASURES: FINDING OUT IDENTITY AND OBTAINING EVIDENCE

Please Note:

- Regulatory requirements are set within this section as *AML/CFT Codes of Practice*.
- This section contains references to Jersey legislation which may be accessed through the JFSC website.
- Where terms appear in the Glossary this is highlighted by the use of italic text. The Glossary is available from the JFSC website.

4.1 Overview of section

1. The purpose of this section of this 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 obtained that is reasonably capable of verifying that the person to be identified is who the person is said to be and satisfies a firm that it does establish that fact.
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* or the *financing of terrorism*, which is covered by stage 1.4 in Section 3.3. Nor does it address the enhanced measures that will be required in order to address the case of a client that is assessed as presenting a higher risk of *money laundering* or the *financing of terrorism*, which is covered in Section 7.
3. Guidance is also given on the timing of obtaining evidence of identity and, on 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); and in respect of "existing clients".
5. Inter alia, the requirement to find out identity and obtain evidence will apply when there is a:
   - change in identification information found out for a client e.g. following marriage or change of nationality;
   - change in beneficial ownership and control of a client; or
   - change in a third party (or parties) or beneficial ownership or control of a third party (or parties) on whose behalf a client acts.
6. A client may be an individual (or group of individuals), or legal person. Section 4.3 deals with a client who is an individual (or group of individuals), Section 4.4 deals with a client (an individual or legal person) who is acting for a legal arrangement, e.g. the trustee of an express trust, and Section 4.5 deals with a client who is a legal person.

7. Throughout this Section, references to a "client" include, where appropriate, a prospective client (an applicant for business). A client is a person with whom a business relationship has been formed or one-off transaction conducted.

4.2 Obligation to Find Out Identity and Obtain Evidence

Overview

8. Determining that a client is who they claim to be is a combination of being satisfied that:
   - a person exists - on the basis of information found out; and
   - the client is that person - by collecting from reliable and independent source documents, data or information, satisfactory confirmatory evidence of appropriate components of the client's identity.
9. Evidence of identity can take a number of forms. In respect of individuals, much weight is placed on identity documents and these are often the easiest way of providing evidence as to someone's identity. It is, however, possible to be satisfied as to a client's identity by obtaining other forms of confirmation, including independent data sources and, in appropriate circumstances, written assurances from *obliged person*s.
10. When obtaining evidence of identity, a firm will need to be prepared to accept a range of documents.

Statutory Requirements

11. *Requirements for identification measures are summarised in Section 3. Inter alia, identification measures must establish the persons who are concerned with a legal arrangement, and each beneficial owner and controller of a client who is a legal person.*
12. *Under Article 3(2)(b) of the Money Laundering Order a relevant person must determine whether a client is acting for a legal arrangement, Article 3(2)(a) requires the customer, e.g. the trustee of a trust or general partner of a limited partnership, to be identified.*
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) of the Money Laundering Order 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 client or where the client is more than one individual, such as a husband and wife.

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) of the *Money Laundering Order* to identify each person who falls within Article 3(7), and each individual who is that person's beneficial owner or controller;
- the beneficial owner or controller of a client, because of a requirement in Article 3(2)(c)(iii) of the *Money Laundering Order* to identify the individuals who are the client's beneficial owners or controllers;
- acting on behalf of a client (e.g. is acting according to a power of attorney, or who 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 client 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 firm may demonstrate that it has found out the identity of an individual who is a client under Article 3(2)(a) of the *Money Laundering Order* where it collects all of the following:

- Legal name, any former names (such as maiden name) and any other names used;
- Principal residential address;
- Date of birth;
- Place of birth;
- Nationality;
- Sex; and
- Government issued personal identification number or other government issued unique identifier.

19. However, in the case of a lower risk relationship, a firm may demonstrate that it has found out the identity of an individual who is a client under Article 3(2)(a) of the *Money Laundering Order* where it collects the following: legal name, any former names (such as maiden name) and any other names used; principal residential address; and date of birth.

4.3.2 Obtaining Evidence of Identity

Overview

20. Evidence of identity may come from a number of sources, including:

- Original documents
- Certified copies of documents (see Section 4.3.3)
- External data sources (see Section 4.3.4)
- E-ID (see Part 4, Section 4.2)

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, for example passports and national identity cards; others are issued on request, without any such checks being carried out. A firm should recognise that some documents are more easily forged than others. Similarly, some smart phone or tablet applications may not

sufficiently mitigate the risks inherent in using such technology and a firm will need to ensure that its *CDD systems and controls* include measures specifically designed to do so.

22. Additionally, documents incorporating photographic confirmation of client identity provide a higher level of assurance that an individual is the person who he or she claims to be.

23. Where a firm is not familiar with the form of the evidence obtained to verify identity, appropriate measures may be necessary to satisfy itself 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*.

AML/CFT 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 the employees of the firm), and must be translated into English at the request of the *JFCU* or the *Commission*.

Guidance Notes

26. A firm 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 the individual is 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;

› Sex; and

› Passport or national identity number.

27. However, in the case of a lower risk relationship with a client who is resident in Jersey, a firm 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 the individual is said to be where that evidence covers: legal name and other names used; and principal residential address (or, as an alternative, date of birth) using at least one source of evidence (see paragraph 28).

28. A firm 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 the individual is 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 (eg. States and parish authorities); • A letter of introduction confirming residential address from: (i) a *relevant person* that is regulated by the *Commission*; (ii) a person carrying on a *financial services business* which is regulated and operates in a well-regulated country or territory; or (iii) 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 client who is resident in Jersey, a firm 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 the individual is said to be where that evidence is a: (i) Jersey driving licence; or (ii) birth certificate, in conjunction with a bank statement, or a utility bill, or document issued by a government source, or a letter of introduction from a *relevant person* that is regulated by the *Commission*.

30. A firm 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 the individual is said to be where the data or information comes from an independent data source or (in the case of a residential address) personal visit to that address.

31. Where an individual's residential address changes, a firm 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 the individual is said to be where the data or information is collected through on-going correspondence with that customer at the changed address.

32. A firm 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; and

    › recent independent assessments of its regulatory environment, such as those conducted and published by the *IMF*.

4.3.3 Insolvency Cases

Overview

33. It is not always possible or necessary to obtain identification evidence direct from individuals or individual shareholders or directors in an appointment in respect of a company as their co-operation may not be forthcoming.

Guidance Note

34. 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.

4.3.4 Suitable Certification

Overview

35. "Suitable certification" is a process where, rather than requesting a person to present evidence of identity directly to a firm, the person is called on to present himself, herself or itself to a trusted external party along with original documentation that supports that person's identity (and which is current) specifically for the purpose of entering into a relationship or one-off transaction with a firm. The effect of this is to create an environment in which *identification measures* are applied through a trusted external party and where the client (or other person) is seen on a face-to-face basis.

36. "Suitable certification" is not to be confused with a case where a firm 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 firm in respect of record-keeping and access to records - where Section 5 is relevant.

37. Nor should provisions in 4.4.5 and 4.5.7 for copy documentation to be provided by a regulated trust and company services provider be confused with "suitable certification".

38. For certification to be effective, a person will need to personally present an original document to an acceptable suitable certifier and that certifier will need to be subject to professional rules (or equivalent) providing for the integrity of the certifier's conduct.

39. Acceptable persons to certify evidence of identity 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;
- 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); and
- a director, officer, or manager of (i) a person carrying on a *financial services business* which is regulated and operates in a well-regulated country or territory; or (ii) 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.

40. In determining whether a country or territory is well-regulated, a firm 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 by the *IMF*.

41. Best efforts should be exercised to secure an adequate quality copy of photographic evidence of identity that is certified.

42. 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.

Guidance Notes

43. A firm 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 the person is said to be when it:

    › obtains a true copy, signed and dated by the suitable certifier ("wet" signature), of a document that is accompanied by confirmation on the matter set out in paragraph 44 and adequate information set out in paragraph 46 so that he may be contacted in the event of a query; and

    › takes additional steps in line with paragraph 47 to validate the credentials of the suitable certifier, where that person is connected to a higher risk country or territory or based in a different country or territory to that of the individual, or there is reason to believe that certification may not be effective (see paragraphs 38 and 39).

44. The matter to be confirmed is 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.

45. In a case where the document to be certified relates to a legal arrangement or legal person, then paragraphs 43 and 44 of this section apply, except that the documents to be certified will be those that provide evidence of identity of that arrangement or person.

46. An adequate level of information to be provided by a certifier will include *his* or her name, position or capacity, *his* or her address and a telephone number or email address at which he or she can be contacted.

47. The additional steps to be taken to validate the credentials of the certifier may include considering factors such as: the stature and track record of the certifier; previous experience of accepting certifications from certifiers in that profession or country or territory; the adequacy of the framework to counter *money laundering* and the *financing of terrorism* in place in the country or territory in which the certifier is located; and the extent to which the framework applies to the certifier.

4.3.5 Obtaining Evidence of Identity - Independent Data Sources

Overview

48. Independent data sources can provide a wide range of confirmatory material on a client, and are becoming increasingly accessible, for example, through improved availability of public information (registers of electors and telephone directories – to the extent permitted by data protection legislation) and the emergence of commercially available data sources such as those provided by data services providers, e.g. credit reference agencies and business information service providers.

49. Where a firm 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

50. A firm 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 firm uses positive data or information source(s) that can be called upon to link a client to both current and historical data and information; and
- processes allow the firm to capture and record the data or information.

51. A firm may demonstrate that it is satisfied that data or information supplied by the 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 European Economic Area (the ***EEA***) or 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:
    a. accesses: (i) a range of positive data or information sources that can be called upon to link a client to both current and historical data and information; (ii) negative data and information sources such as databases relating to fraud and deceased persons; and (iii) a wide range of alert data sources; or
    b. otherwise ensures that its source(s) are sufficiently extensive, reliable and accurate; and
- processes allow the firm to capture and record the data information.

4.3.6 Guarding Against the Exclusion of Jersey Residents

Overview

52. On occasions, an individual may be unable to provide evidence of identity using the sources of evidence 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 Codes of Practice

53. A firm must determine that there is a valid reason for a client being unable to provide more usual sources of evidence of identity, and must document that reason.

Guidance Notes

54. 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 *accountancy services*, a firm 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 the person is said to be where that evidence is: (i) the minor's birth certificate; and (ii) letter from the parent or guardian confirming their status (i.e. I am the parent of [name of minor]; or guardian of [name of minor]) and the residential address of the minor.

55. In the case of a lower risk individual who is resident in a Jersey nursing home or residential home and has a valid reason for being unable to produce more usual evidence of identity, and would otherwise be excluded from accessing *accountancy services*, a firm 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 the person is said to be where that evidence is a letter from a Jersey nursing home or residential home for the elderly, which a firm is satisfied that it can place reliance on, confirming the identity of the resident.

56. 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 *accountancy services*, a firm 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 the person is said to be where that evidence is:

- A letter from a Jersey employer, which a firm 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 *his* or her 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 client and the head of household, together with evidence that the head of household resides at the address.
- A letter from a principal of a university or college, which a firm 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.

57. Confirmatory letters should be written on appropriately headed notepaper.

4.3.7 Residential Address: Overseas Residents

Overview

58. On occasions, an individual resident abroad may be unable to provide evidence of *his* principal residential address using the sources set out at Section 4.3.2 of this Handbook. Examples of such individuals 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 private address may not be obtained through a personal visit.

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

AML/CFT Codes of Practice

60. A firm must determine that there is a valid reason for a client being unable to provide more usual sources of evidence of an address, and must document that reason.

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

Guidance Notes

62. Where an individual has a valid reason for being unable to produce more usual evidence for a residential address, a firm 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 the person is said to be where it receives written confirmation from an individual satisfying the criteria for a suitable certifier that he or she has visited the individual at that address.

63. Where an individual has a valid reason for being unable to produce more usual evidence for a residential address, a firm 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 firm may demonstrate that it has obtained evidence that is reasonably capable of verifying that a person to be identified is who the person is said to be where it obtains evidence that the individual may normally be met or contacted at that address.

64. A "locator" address - 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

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

66. 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.

67. There is 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 and trusts established for wealth management purposes. Trusts may also be established as a *collective investment scheme* – known as a unit trust.

68. 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 firm on behalf of the legal arrangement and who will be considered to be the client(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).

69. In forming a business relationship or carrying out a one-off transaction with a trustee or general partner, a firm will be dependent on information provided by the trustee or general partner (a regulated trust and company services provider 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 (see Section 3.3 of this Handbook), the risk factors set out in Section 3.3.4.1 and Section 7.14.1 of this Handbook 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 firm (see Section 6 of this Handbook) may provide additional comfort that relevant and up to date identification and relationship information on identity has been found out.

70. 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).

71. The following provisions apply to situations where a trustee of an express trust or general partner of a limited partnership is the **client** of a firm.

72. The following 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 client, because of a requirement in Article 3(2)(c)(iii) of the *Money Laundering Order* to identify the individuals who are the client's beneficial owners or controllers; or

    › a third party on whose behalf a client 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.

73. Where the trustee or general partner is a *relevant person carrying on regulated business* (defined in Article 1 of the *Money Laundering Order*) 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.

74. The measures that must be applied by a firm where a third party is a trust need not include a settlor of a trust who is deceased.

75. 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 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.

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

77. Notwithstanding the requirement to find out and obtain evidence in relation to the trustee, the trust and those individuals listed in Article 3(7) of the *Money Laundering Order*, a firm 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

78. A firm 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).

79. A firm 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 initial 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. This information may be provided by the trustee.

80. A firm 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.

81. A firm 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.

82. A firm may demonstrate that it has found out the identity of persons having a beneficial interest in a unit trust 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.

83. A firm may demonstrate that it has found out the identity of 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, who has been identified as presenting higher risk. This information may be provided by the trustee.

84. A firm may demonstrate that it has found out the identity of any other individual 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

85. In any case where a settlor, protector, beneficiary or object of a power, or other person referred to in paragraphs 79 to 84 (the **person**) of a trust which is a third party is not an individual, a firm 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:

- 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** over the person **through other means.**
- Where no individual is otherwise identified under this section, individuals who exercise **control** of the person **through positions held** (who have and exercise strategic decision-taking powers or have and exercise executive control through senior management positions).

86. For lower risk relationships, a general threshold of 25% is considered to indicate a material controlling ownership interest in capital. However, 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 Codes of Practice

87. All key documents (or parts thereof) obtained as evidence of identity must be understandable (i.e. in a language understood by the employees of the firm), and must be translated into English at the request of the *JFCU* or the *Commission*.

88. A firm must obtain evidence that any person purporting to act as the trustee of a trust which is a third party has authority so to act.

Guidance Notes

89. A firm 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 is what it is said to be where the evidence covers the following components of identity: name and date of establishment of the express trust, appointment of the trustee and 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

90. A firm 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 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).

91. A firm 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.

92. 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 firm 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 and intimate family relationships, historical or contractual associations or as a result of default on certain payments.

93. Where no person is otherwise identified under this section, a firm 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** (who have and exercise strategic decision-taking 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.

94. In any case where a partner or other person referred to in paragraphs 91 to 93 is not an individual, a firm 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:

- 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.**
- 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** (who have and exercise strategic decision-taking powers or have and exercise executive control through senior management positions).

95. 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.

96. 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. Whilst this principle may also apply to other relationships, 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 Codes of Practice

97. All key documents (or parts thereof) obtained as evidence of identity must be understandable (i.e. in a language understood by the employees of the business), and must be translated into English at the request of the *JFCU* or the *Commission*.

98. A firm must obtain evidence that any person purporting to act as general partner of a partnership which is a third party has authority so to act.

Guidance Notes

99. A firm 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 who the partnership is said to be where the evidence covers all of the following components of identity:

- Name of partnership.
- Date and country of registration/establishment.
- Official identification number.
- Registered office/business address.
- Principal place of business/operations (if different).

100. However, in the case of a lower risk relationship, a firm 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 who the

partnership is said to be where the evidence covers the following components of identity: name of partnership; date and country of registration/establishment; and official identification number.

101. A firm 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 who the partnership 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 clients):

› 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.

102. A firm 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 who the partnership is said to be where the data or information comes from an independent data source 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.

103. Where a partner holds this role by virtue of *his* employment by (or position in) a business that is a regulated Jersey trust and company services provider, a firm 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; and

› 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

104. Where information is provided by a trust and company service provider that is regulated by the *Commission*, the Guernsey Financial Services Commission or the Isle of Man Financial Services Authority ("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 66), a firm may demonstrate that it has taken reasonable measures to obtain evidence of identity of that person under Article 13 of the *Money Laundering Order* where it obtains a copy of a document that is listed in paragraph 27 from the regulated trust and company services provider, along with confirmation on certain matters.

105. The matters to be confirmed are that:

› the regulated trust and company services provider has seen the original document that it has copied to the firm, or the document that has been copied to the firm was provided to the regulated trust and company services provider by a suitable certifier;

› the regulated trust and company services provider is satisfied that the original document seen, or document provided to it by a suitable certifier, provides evidence that the individual is who he or she is said to be; and

› the document provided to the firm is a true copy of a document that is held by the regulated trust and company services provider.

106. This will be different to a case where a firm 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 party (whatever those measures might have involved), where evidence of identity may be held by the obliged party, and where the obliged party has a continuing responsibility to the firm in respect of record-keeping and access to records – Section 5 is relevant.

107. 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 client risk under Article 13, or assessment of risk under Article 16 of the *Money Laundering Order*.

108. 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.

4.5 Obligation to Find Out Identity and Obtain Evidence: Legal Persons

Overview

109. Jersey law recognises a number of distinct forms of legal person, in particular: the company; the foundation; the limited liability partnership; the separate limited partnership; and the incorporated limited partnership.

110. Companies are established under the Companies (Jersey) Law 1991 (the ***Companies Law***). Foundations are established under the Foundations (Jersey) Law 2009. Limited liability partnerships are established under the Limited Liability Partnerships (Jersey) Law 1997. Separate Limited Partnerships are established under the Separate Limited Partnerships (Jersey) Law 2011. Incorporated Limited Partnerships are established under the Incorporated Limited Partnerships (Jersey) Law 2011.

111. The following provisions apply to situations where a legal person is the **client**.

112. 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 client, because of a requirement in Article 3(2)(c)(iii) of the *Money Laundering Order* to identify the individuals who are the client's beneficial owners or controllers;
- Acting on behalf of a client (e.g. is acting according to a power of attorney, or has signing authority over an account); or
- A third party on whose behalf a client 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.

113. The *Companies Law* allows for the incorporation of cell companies: incorporated cell companies (***ICCs***) and protected cell companies (***PCCs***).

114. Each of these types of cell companies may establish one or more cells.

115. 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.

116. Where a firm 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 client 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.

117. 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 firm establishes a business relationship or enters into a one-off transaction with a cell of an *ICC*, the cell (a company) will be taken to be the client.

118. In a case where the ownership structure of a legal person to be identified (A) includes other legal persons, the beneficial owners and controllers of A will include those individuals **ultimately** holding a material controlling ownership interest in A. See paragraph 132.

119. The *identification measures* to be applied to a company are set out in Sections 4.5.1 and 4.5.2. The identification measures to be applied to a foundation are set out in Sections 4.5.3 and 4.5.4. The identification measures to be applied to a partnership are set out in Sections 4.5.5 and 4.5.6.

120. For the purposes 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 firm or otherwise own property; an anstalt; an incorporated and unincorporated association, club, society, charity, church body, or institute; a mutual or friendly society; a co-operative; and a provident society.

121. Where information relating to a legal person is not available from a public source, a firm will be dependent on the information that is provided by the legal person acting for the legal arrangement. When determining the risk assessment for a legal person (see Section 3.3 of this Handbook), the risk factors set out in Section 3.3.4.1 of this Handbook will be relevant. The risk factors set out in Section 7.14.1 of this Handbook will also be relevant in determining whether it is appropriate to use information on a legal person provided through a trust and company (or other) services provider. In addition, the monitoring measures maintained by a firm (see Section 6 of this Handbook) may provide additional comfort that relevant and up to date information on identity has been found out.

122. Where a director of a company holds this role by virtue of *his* employment by (or position in) a regulated Jersey trust company business, 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.

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

124. 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 firm. For example, it may not be appropriate to request evidence directly from a person in whose favour discretion may be exercised.

125. Where a firm 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

126. A firm may demonstrate that it has found out the identity of a company which is a client 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 of incorporation/registration.
    - Official identification number.
    - Registered office address.
    - Mailing address (if different).
    - Principal place of business/operations (if different).
    - Names of all persons having a senior management position[1].
127. A firm may demonstrate that it has found out the identity of a person who is the client'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.
128. To the extent that there is doubt as to whether the persons exercising c**ontrol through ownership** are beneficial owners, or where no person exerts control through ownership, a firm may demonstrate that it has found out the identity of a person who is the client'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 and intimate family relationships, historical or contractual associations or as a result of default on certain payments.
129. Where no person is otherwise identified under this section, a firm may demonstrate that it has found out the identity of a person who is the client'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** (who have and exercise strategic decision-taking powers or have and exercise executive control through senior management positions, e.g. directors[2]).
130. This information may be provided by the company.
131. In any case where a person identified under paragraphs 127 to 129 is not an individual, a firm 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:

---

[1] Individuals having a senior management position means those who have and exercise strategic decision-taking powers or who have and exercise executive control.

[2] This information may be provided by the company. In the case of other bodies, anstalts, associations, clubs, societies, charities, church bodies, institutes, mutual or friendly societies, co-operatives and provident societies, senior individuals will often include members of the governing body or committee plus executives

- 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.**
- 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.**
- Where no individual is otherwise identified under this section, individuals who exercise control of the company **through positions held** (who have and exercise strategic decision-taking powers or have and exercise executive control through senior management positions).

132. In the case of a lower risk relationship, person/s having 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.

133. For lower risk relationships, a general threshold of 25% is considered to indicate material controlling ownership interest in the capital of a company. Whilst this principle may also apply to other relationships, 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.

4.5.2 Obtaining Evidence of Identity – Legal Person that is a Company

AML/CFT Codes of Practice

134. All key documents (or parts thereof) obtained as evidence of identity must be understandable (i.e. in a language understood by the employees of the firm), and must be translated into English at the request of the *JFCU* or the *Commission*.

Guidance Notes

135. A firm 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 client to be identified is who the company is said to be where the evidence covers all of following components of identity:

- Name of company.
- Date and country of incorporation.
- Official identification number.
- Registered office address.
- Principal place of business/operations (where different to registered office).

136. However, in the case of a lower risk relationship, a firm 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 client to be identified is who the company is said to be where the evidence covers the following components of identity: name of company; date and country of incorporation/registration; and official identification number.

137. A firm 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 client to be identified is who the company 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 clients):

- Certificate of incorporation (or other appropriate certificate of registration or licensing) 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.

138. A firm 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 client is who the company is said to be where the data or information comes from an independent data source 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.

139. Where a person/s having a senior management position holds this role by virtue of *his* employment by (or position in) a business that is a regulated Jersey trust and company services provider, a firm 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; and
- 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

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

- Name of foundation.
- Date and country of incorporation.
- Official identification number.
- Business address. In the case of a foundation incorporated under the Foundations (Jersey) Law 2009, this will be the business address of the qualified member of the council.
- Mailing address (if different).
- Principal place of business/operations (if different).
- Name of all council members and, if any decision requires the approval of any other person, the name of that person.

141. A firm 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. This information may be provided by the foundation.
- the guardian (who takes such steps as are reasonable to ensure that the council of the foundation carries out its functions). This information may be provided by the foundation.
- the council members and, if any decision requires the approval of any other person, that person. This information may be provided by the foundation.

- any beneficiary entitled to a benefit under the foundation in accordance with the charter or the regulations of the foundation. This information may be provided by 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. This information may be provided by the foundation.
- Any other person exercising ultimate effective control over the foundation. This information may be provided by the foundation.

142. In any case where a founder, guardian, beneficiary or other person listed in paragraph 141 (the **person**) is not an individual, a firm 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 over the person through other means.**
- Where no individual is otherwise identified under this section, individuals who **exercise control** of the person **through positions held** (who are responsible for strategic decision-taking or exercising executive control through senior management positions).

143. 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 firm may find out the identity of council members who have and exercise authority to operate a business relationship or one-off transaction.

144. For lower risk relationships, a general threshold of 25% is considered to indicate a material controlling ownership interest in capital. Whilst this principle may also apply to other relationships, 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.

4.5.4 Obtaining Evidence of Identity – Legal Person that is a Foundation

AML/CFT Codes of Practice

145. All key documents (or parts thereof) obtained as evidence of identity must be understandable (i.e. in a language understood by the employees of the firm), and must be translated into English at the request of the *JFCU* or the *Commission*.

Guidance Notes

146. A firm 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 client is who the foundation is said to be where the evidence covers all of the following components of identity:

- Name of foundation.
- Date and country of incorporation.
- Official identification number.
- Business address.

- Principal place of business/operations (if different).

147. However, in the case of a lower risk relationship, a firm 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 client to be identified is who the foundation is said to be where the evidence covers the following components of identity: name of foundation, date and country of incorporation, and official identification number.

148. A firm 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 the foundation 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 further evidence (one source for lower risk customers):

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

149. A firm 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 client is who the foundation is said to be where the data or information comes from an independent data source 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 *Commission*'s website (for the business address of the qualified member of the council).

150. Where a council member who is an individual holds this role by virtue of their employment by (or position in) a business that is a regulated Jersey trust and company services provider, a firm 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 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

151. A firm may demonstrate that it has found out the identity of a partnership which is a client 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 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).

152. A firm may demonstrate that it has found out the identity of a person who is the client'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.

153. 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 firm may demonstrate that it has found out the identity of a person who is the client'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 and intimate family relationships, historical or contractual associations or as a result of default on certain payments.

154. Where no person is otherwise identified under this section, a firm may demonstrate that it has found out the identity of a person who is the client'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** (who have and exercise strategic decision-taking powers or have and exercise executive control through senior management positions, e.g. general partner or limited partner that participates in management).

155. This information may be provided by the partnership.

156. In any case where a partner or other person referred to in paragraphs 152 to 154 is not an individual, a firm 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** of the partnership **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** (who have and exercise strategic decision-taking powers or have and exercise executive control through senior management positions).

157. 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.

158. For lower risk relationships, a general threshold of 25% is considered to indicate a material controlling ownership interest in the capital of a partnership. Whilst this principle may also apply to other relationships, 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.

4.5.6 Obtaining Evidence of Identity – Legal Person that is a Partnership

AML/CFT Codes of Practice

159. All key documents (or parts thereof) obtained as evidence of identity must be understandable (i.e. in a language understood by the employees of the firm), and must be translated into English at the request of the *JFCU* or the *Commission*.

Guidance Notes

160. A firm 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 client to

be identified is who the partnership is said to be where the evidence covers all of the following components of identity:

- Name of partnership.
- Date and country of incorporation/registration/establishment.
- Official identification number.
- Registered office/business address.
- Principal place of business/operations (if different).

161. However, in the case of a lower risk relationship, a firm 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 client to be identified is who the partnership is said to be where the evidence covers the following components of identity: name of partnership, date and country of incorporation/registration, and official identification number.

162. A firm 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 client to be identified is who the partnership 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 clients):

- 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.

163. A firm 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 partnership which is a client is who the partnership is said to be where the data or information comes from an independent data source 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.

164. Where a partner holds this role by virtue of their employment by (or position in) a business that is a regulated Jersey trust and company services provider, a firm 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; and
- 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

165. Where information is provided by a trust and company services provider that is regulated by the *Commission*, the Guernsey Financial Services Commission or the Isle of Man Financial Services Authority ("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 116), a firm may demonstrate that it has taken reasonable measures to obtain evidence for that person under Article 13 of the *Money Laundering Order* where it obtains a

copy of a document that is listed in paragraph 27 from the regulated services provider, along with confirmation on certain matters.

166. The matters to be confirmed are that:

- the regulated trust and company services provider has seen the original document that it has copied to the firm, or the document that has been copied to the firm was provided to the regulated services provider by a suitable certifier;
- the regulated trust and company services provider is satisfied that the original document seen, or document provided to it by a suitable certifier, provides evidence that the individual is who he or she is said to be; and
- the document provided to the firm is a true copy of a document that is held by the regulated trust and company services provider.

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

168. 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 client risk under Article 13, or assessment of risk under Article 16 of the *Money Laundering Order*.

169. 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.

4.6 Obligation to Find out Identity and Obtain Evidence: Authorised Agent of Client

Statutory Requirements

170. *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.*

AML/CFT Codes of Practice

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

172. In the case of a legal arrangement that is a trust, a firm must obtain evidence that any person purporting to act as the trustee has authority so to act.

173. In the case of a legal arrangement that is a limited partnership, a firm must obtain evidence that any person purporting to act as general partner has authority so to act.

Guidance Notes

174. A firm may demonstrate that it has taken reasonable measures to obtain satisfactory 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.

175. In the case of a lower risk relationship, a firm 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 client.

4.7 Timing of identification measures

Statutory Requirements

Initial

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

177. *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:*

178. *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.*

179. *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.*

180. *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 financing terrorism is effectively managed; and*
- *evidence of identity is obtained as soon as reasonably practicable.*

181. *Under Articles 11(3)(fa) and 11(3) (fb) of the Money Laundering Order, policies and procedures must be in place to: assess the risk of money laundering or the financing of terrorism and to manage the risks in relation to the conditions under which a client may utilise a business relationship with the relevant person before the identification of the client has been completed; as referred to in Article 13(4); and 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

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

183. *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

184. *Article 13(2) of the Money Laundering Order says 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.

185. *Article 13(3) of the Money Laundering Order says that "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; and*
- *any time when a relevant person suspects money laundering or the financing of terrorism (unless agreed otherwise with the JFCU).*

186. *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 Commission.*

187. *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

188. *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 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; and*
- *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

189. Article 13(4) of the *Money Laundering Order* allows, in certain circumstances, a firm a reasonable timeframe to undertake the necessary enquiries for obtaining evidence of identity after the initial establishment of a 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, then subject to Section 4.8.1 of this Handbook, a firm must terminate the relationship (See Section 4.8 of this Handbook).

190. A relationship is considered to be established as soon as a firm undertakes to act on instructions as to the operation of that relationship, for example, by receiving and accepting signed terms of business from the client.

191. Where the provision of Schedule 2 business is urgent, this 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.

AML/CFT Codes of Practice

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

- it highlights to its clients its obligation to terminate the relationship at any time on the basis that evidence of identity is not obtained; and

› money laundering and the *financing of terrorism* risk is effectively managed.

193. In any event, a firm must not pay away funds to an external party (or to another account in the name of the client), other than to invest or deposit the funds on behalf of the client, until such time as evidence of identity has been obtained.

Guidance Notes

194. A firm may demonstrate that it has highlighted to a client the obligation to terminate a relationship where terms of business, which govern its relationships with its client:
(i) encompass the termination of relationships when evidence of identity is not obtained; and
(ii) clearly state that termination may lead to a client suffering losses – where, e.g. funds have been invested in a collective investment fund where a forced redemption is necessary.

195. A firm may demonstrate that *money laundering* and the *financing of terrorism* risk is effectively managed where:

› *policies and procedures* establish timeframes for obtaining evidence of identity;

› the establishment of any 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 in respect of the relationship.

196. A firm may demonstrate that periodic reporting is in line with Article 11(3)(fa) of the *Money Laundering Order* where it highlights to senior management:

› the number of clients 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; and

› in any case where the delay is for more than a particular period of time, the name of the client, the reason for the delay, the extent to which evidence of identity has not been obtained, the risk rating given to that client, and action that is to be taken to obtain evidence or terminate the relationship (and by when).

197. Guidance as to appropriate steps to take where a firm 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

198. In the course of a business relationship between a firm and a client that is a trustee, a firm 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 or the *financing of terrorism* occurring as a result of obtaining evidence after entitlement is conferred.

199. In the course of a business relationship between a firm and a client that is a trustee, a firm 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

200. In the case of a business relationship between a firm and a client that is a foundation, a firm 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; 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 conferring entitlement.

201. In the course of a business relationship between a firm and a client that is a foundation, a firm 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 Clients"

Overview

202. *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.

203. For the purposes of the *Money Laundering Order*, an existing client means a business relationship established before the *Money Laundering Order* came into force for accountants on 1 May 2008 and which continues.

204. For the avoidance of doubt, the *identification measures* (finding out identity and obtaining evidence) to be applied to existing clients 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 client on the basis that a relationship will have been established on, or before, 30 April 2008.

205. Except with the agreement of the *Commission*, the effect of Article 13(3A) of the *Money Laundering Order* is to require the identity of a client to have been found out by 31 December 2014. There is no similar deadline for obtaining evidence of identity.

206. 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).

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

208. A firm may meet its obligation to apply *identification measures* by placing reliance on an *obliged person*. See Section 5.

AML/CFT Codes of Practice

209. A firm must review its "existing client" base in order to determine a risk assessment for each client that has still to be remediated.

Guidance Notes

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

- As soon as is practicable after the date that a firm has assessed a client to present a higher *money laundering* or the *financing of terrorism* risk; and
- 31 December 2014 (or later date agreed with the *Commission*).

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

- The date when a transaction of significance takes place;
- The date when a firm's client documentation standards change substantially; and
- 31 December 2014 (or later date agreed with the *Commission*).

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

213. A firm 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 client built up through the historical conduct of the relationship, etc.

4.8 Failure to Complete Identification Measures

Overview

214. Where *identification measures* cannot be completed, a firm must not establish a business relationship or carry out a one-off transaction. In the case of an established client, the relationship must be terminated.

215. 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 client, 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.

216. Wherever possible, a firm should return assets or funds directly to the client.

217. In a case where the client requests that assets or funds be transferred to an external party, a firm 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*.

218. Where contact has been lost with a client 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.

Statutory Requirements

219. *If a relevant person is unable to apply identification measures before the establishment of a relationship or before carrying out a one-off transaction (except for circumstances provided for 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.

220. *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) of the Money Laundering Order, to terminate the relationship.*

221. *Article 14 of the Money Laundering Order requires a relevant person to terminate a business relationship or a one-off transaction where it cannot apply on-going identification measures.*

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

223. *Article 14(11) of the Money Laundering Order provides that a business relationship or one-off transaction may proceed or continue where a suspicious activity report has been made and the relevant person is acting with the consent of a designated police or customs officer.*

Guidance Notes

224. Wherever possible when terminating a relationship where client money or other assets have been received, a firm should return the assets directly to the client, for example by returning money to the account from which it was received.

225. Where the client requests that money or other assets be transferred to third parties, or to a different account in the client's name, the firm should assess whether this provides grounds for suspicion of *money laundering* or *financing of terrorism*.

226. If procedures are not completed before entering into a business relationship, firms and their clients may suffer considerable cost and inconvenience in having to terminate a relationship if identification and verification procedures either cannot be completed, or where the results are unsatisfactory. Terms and conditions should clearly state that termination may lead to an applicant suffering losses if *CDD* procedures cannot be satisfactorily completed.

4.8.1 Ascertaining Legal Position

Overview

227. 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 client or performing the task of defending or representing their client in legal proceedings (including advice on instigating or avoiding proceedings).

228. 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

229. *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 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

230. *CDD* information will still need to be collected within a reasonable timescale in order to comply with Article 13 of the *Money Laundering Order*.

231. Firms are advised 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*.

5 IDENTIFICATION MEASURES: RELIANCE ON OBLIGED PERSONS

Please Note:

- Regulatory requirements are set within this section as *AML/CFT Codes of Practice*.
- This section contains references to Jersey legislation which may be accessed through the JFSC website.
- Where terms appear in the Glossary this is highlighted by the use of italic text. The Glossary is available from the JFSC website.

5.1 Overview of section

1. In some strictly limited cases, a firm may meet its obligation to comply with Article 13(1)(a) or (c)(ii), Article 15(1)(a), (b), (d), (e) or (g) or Article 15A of the *Money Laundering Order* and *AML/CFT 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 client and to obtain evidence of identity.

2. In order to consider what reliance might be placed on an *obliged person*, a firm will first need to determine what elements of identity must be found out and what evidence of identity is to be obtained for its client. It will do so in accordance with Article 3 of the *Money Laundering Order* and *AML/CFT Codes of Practice* set in Sections 3, 4 and 7, and will take into account its risk assessment for the client. Once it has determined what *identification measures* it is to apply, a firm can then consider whether those measures have already been applied by an *obliged person*.

3. Where an *obliged person* has met its client, who is resident in the same country 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 firm in a case where the firm is resident in a different country to the *obliged person* and client, and where it has not met its client. Even in a case where the firm and *obliged person* have met a client and are resident in the same country, the measures taken by the *obliged person* may still differ to those to be applied by the firm 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 firm 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 firm to find out more information on identity and obtain evidence for that aspect of identity itself.

5. However, it is not necessary that the *obliged person* will have found out identity or obtained evidence of identity exactly in line with *policies and procedures* applied by the firm, since guidance in Section 4 provides 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 firm is permitted to place reliance on the *obliged person* to have found out the identity and to have obtained evidence of the identity of: (i) the firm's client; (ii) any beneficial owner or controller of that client; (iii) any third party for which that client is acting; (iv) any beneficial owner or controller of a third party for whom that client is acting; and/or (v) any person purporting to act on behalf of that client.

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. Further, Article 16 of the *Money Laundering Order* cannot be applied in any case where a firm suspects *money laundering* or the *financing of terrorism*, in any case where a firm 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 where the *obliged person* has a relevant connection to a country or territory that is subject to a *FATF* call to apply enhanced *CDD* measures (see Section 7.5).

9. Whilst the information on identity found out by the *obliged person* must be provided to the firm immediately before establishing a business relationship or carrying out a one-off transaction, a firm is not also required to immediately obtain evidence of identity. Evidence of identity may be held by an *obliged person*, so long as the firm 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*.

10. Inter alia, an *obliged person* may be:

    › Another accountancy firm that is a *relevant person* carrying on Schedule 2 business.

    › A trust and company services provider.

11. A firm will remain responsible for the satisfactory performance of all elements of ***reliance identification measures***. Under Article 16 of the *Money Laundering Order,* in this section *"reliance identification measures"* means -

    › the identification measures specified in Article 3(2)(a), (aa), (b) or (c) of the Money Laundering Order; or

    › if the obliged person is not in Jersey, similar identification measures that the obliged person applies that satisfy Recommendation 10 of the FATF recommendations.

12. However, where the measures taken by a firm are reasonable, it will have a defence should the obliged person fail to have performed satisfactory measures.

13. 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 client will have a direct relationship with a firm but not with the delegate carrying on the outsourced activity. Although the delegate may have substantial contact with the client, the client is a client of the firm but not of the delegate. The delegate will be carrying on the outsourced activity for the firm according to the terms of a contract with the firm. An example of a typical outsourcing arrangement is where a trustee of a collective investment fund outsources the management of the fund to an external party.

14. Where information on identity found out or evidence of that identity is passed by an *obliged person* to a firm 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.

15. A client may be an individual (or group of individuals) or legal person. Section 4.3 deals with a client who is an individual (or group of individuals), Section 4.4 deals with a client (an individual or legal person) who is acting for a legal arrangement, and Section 4.5 deals with a client who is a legal person.

16. Throughout this section, references to "client" (or "customer") include, where appropriate, a prospective client or customer (an applicant for business). A client is a person with whom a business relationship has been formed or one-off transaction conducted.

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; or
- a person purporting to act on behalf of that customer.

Statutory Requirements

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 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 Commission discharges supervisory functions that is overseen for AML/CFT compliance in Jersey; or*
- *A person who carries on equivalent business (refer to Section 1.7).*

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; and*
- *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; and*
- *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: (i) 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; and (ii) 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 he has obtained during the course of applying reliance identification measures in respect of a person; and*
- *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 a customer 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; or*

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 Codes of Practice

34. To the extent that reliance is placed on an *obliged person*, a firm 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 firm (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 firm 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, such as that published in Appendix C; and

› explains what evidence of identity it has obtained.

37. An assurance that addresses the matters listed in paragraph 37 above will be considered to be reasonably capable of being regarded as reliable under Article 16(6)(a) of the *Money Laundering Order*.

38. Where, as a result of Article 16(6)(b) of the *Money Laundering Order*, a firm 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

39. A firm 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 entity must be able to show why this constitutes provision without delay based on the nature of its client base. In order to demonstrate the reasons for the delay the *relevant person* is expected to provide detail of the reasons as to what led to the delay, how many days evidence remained outstanding, how many times a delay has occurred previously across the *firm's* practice, as well as the decision-makers' considerations.

5.1.1 Assessment of Risk

Overview

40. The risk factors that are set out in this section will also be relevant to a client risk assessment that is conducted under Section 3.3.4.1 in the cases highlighted at Sections 4.4 (paragraph 70) and 4.5 (paragraph 122).

Statutory Requirements

41. *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.*

42. *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.*

43. *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.*

44. *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 Codes of Practice

45. 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*: (i) has not applied the necessary *reliance identification measures*; (ii) does not provide adequate, accurate and current information; (iii) does not keep evidence of identity for as long as is necessary; or (iv) will not provide that evidence without delay when requested to do so, a firm 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

46. Immediately before relying upon an *obliged person*, a firm may demonstrate that it has had regard for the higher risk of *money laundering* and the *financing of terrorism*, and the risk that an *obliged person* will fail to provide the firm 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 or territory in which the obliged person is based. Factors to consider include those found at section 3.3.4.1;
- the adequacy of the framework to combat *money laundering* and the *financing of terrorism* in place in the country or 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* and the *financing of terrorism* to which the *obliged person* is subject;
- the adequacy of *identification measures* applied by the *obliged person* to combat *money laundering* and the *financing of terrorism*.

47. A firm 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* and the *financing of terrorism* 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.

6 ON-GOING MONITORING: SCRUTINY OF TRANSACTIONS & ACTIVITY

Please Note:

- Regulatory requirements are set within this section as *AML/CFT Codes of Practice*.
- This section contains references to Jersey legislation which may be accessed through the JFSC website.
- Where terms appear in the Glossary this is highlighted by the use of italic text. The Glossary is available from the JFSC website.

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 firm will still need to consider reporting provisions summarised in Section 8, e.g. where there is suspicion that payment for the service is made out of the proceeds of criminal conduct.
3. This section explains the measures required to demonstrate compliance with the requirement to scrutinise transactions and also sets a requirement to scrutinise client activity.
4. The requirement to keep documents, data and information up to date and relevant is discussed at Section 3.4 of this Handbook.

6.2 Obligation to Perform On-going Monitoring

Statutory Requirements

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(1) of the Money Laundering Order requires a relevant person to establish and 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(1), "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 firm **monitors** all client transactions and activity in order to **recognise notable transactions or activity,** i.e. those that:

› are inconsistent with the firm's knowledge of the client;

› are complex or unusually large;

› form part of an unusual pattern; or

› present a higher risk of money laundering or the financing of terrorism.

11. Secondly, such notable transactions and activity are then **examined** by an appropriate person, including the background and purpose of such transactions and activity.

12. In addition to the scrutiny of transactions, as required by the *Money Laundering Order*, *AML/CFT Codes of Practice* set in this section require a firm to also scrutinise client activity (though this will already be the effect of *policies and procedures* required by Article 11(3)(a)(iii) of the *Money Laundering Order*).

13. A firm must therefore, as a part of its **scrutiny** of transactions and activity, establish appropriate procedures to **monitor** all of its clients' transactions and activity and to **recognise** and **examine** notable transactions or activity.

14. Sections 3 and 4 of this Handbook address the capturing of sufficient information about a client that will allow a firm to prepare and record a client business and risk profile which will provide a basis for recognising notable transactions or activity, which may indicate *money laundering* or the *financing of terrorism*. Additional or more frequent monitoring is required for relationships that have been designated as carrying a higher risk of *money laundering* or the *financing of terrorism*.

15. **Unusual transactions or activity, unusually large transactions or activity, and unusual patterns of transactions or activity** may be recognised where transactions or activity are inconsistent with the expected pattern of transactions or expected activity for a particular client, or with the normal business activities for the type of service that is being delivered.

16. For many clients of accountancy and tax firms (and in all cases for insolvency firms), a complete profile and appropriate risk assessment may only become evident whilst acting for the client, making the updating of documents, data or information and monitoring of client activity and transactions key to obtaining a complete understanding of client relationships. The more a firm knows about its clients and develops an understanding of the instructions, the better placed it will be to assess risks.

17. **Higher risk transactions or activity** may be recognised by developing a set of "red flags" or indicators which may indicate *money laundering* or the *financing of terrorism*, based on a firm's understanding of its business, its products and its clients (i.e. the outcome of its business risk assessment – Section 2.3.1).

18. **Complex transactions or activity** may be recognised by developing a set of indicators, based on a firm's understanding of its business, its products and its customers (i.e. the outcome of its business risk assessment – Section 2.3.1).

19. External data sources and media reports will also assist with the identification of notable transactions and activity.

20. Where notable transactions or activity are **recognised**, such transactions or activity 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 recognised. 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 client business and risk profile, but on occasions this examination will involve requesting additional information from a client.

21. Notable transactions or activity may indicate *money laundering* or the *financing of terrorism* 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.

22. Scrutiny may involve both **real time** and **post event** monitoring and may involve manual or automated procedures. However, for most accountancy and tax firms, it is unlikely that automated transaction or activity monitoring procedures will be relevant. Monitoring is likely to be most effective when undertaken on a case-by-case basis by fee earners, administration and accounts staff which may be expected to highlight notable transactions or activity.

23. The examination of notable transactions or activity may be conducted either by fee earners or some other independent reviewer. In any case, the examiner must have access to all client records.

24. The results of an examination should be recorded and action taken as appropriate. Refer to Section 10 of this Handbook for record-keeping requirements in relation to the examination of some notable transactions and activity.

25. In order to recognise *money laundering* and the *financing of terrorism*, employees will need to have a good level of awareness of both and to have received training. Awareness raising and training are covered in Section 8 of this Handbook.

26. Where on-going monitoring indicates possible *money laundering* or the *financing of terrorism* activity an internal SAR must 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 Codes of Practice

27. 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 firm's knowledge of the client, including the client's business and risk profile.

28. A firm 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 firm to regard it as particularly likely to be related to *money laundering* or the *financing of terrorism*.

29. As part of its examination of the above transactions, a firm must examine, as far as possible, their background and purpose and set forth its findings in writing. A firm must have *policies and procedures* in place to address any specific risks associated with client relationships established where the client is not physically present for identification purposes (i.e. non-face to face).

Guidance Notes

30. A firm 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 accountancy business and services;
- whether it is possible to establish appropriate standardised parameters for automated monitoring; and
- the monitoring procedures that already exist to satisfy other business needs.

31. A firm may demonstrate that *CDD policies and procedures* are appropriate where the following are used to **recognise** notable transactions or activity:

- **client 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 firm's client base – based on its business risk assessment (refer to Section 2.3.1 of this Handbook), information published from time to time by the *Commission* 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 or activity** – based on its business risk assessment (refer to Section 2.3.1 of this Handbook), information published from time to time by the *Commission* or the *JFCU*, e.g. findings of supervisory and themed examinations and typologies, and information published by reliable and independent third parties.

32. A firm may demonstrate that *CDD policies and procedures* are appropriate if **examination** of notable transactions or activity includes:

- reference to the client'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.

33. A firm may demonstrate that *CDD* and reporting *policies and procedures* are effective if **post-examination** of notable transactions or activity it:

- revises, as necessary, its client's business and risk profile;
- adjusts, as necessary, its monitoring system e.g. refines monitoring parameters, enhances controls for more vulnerable services; 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

6.2.2 Monitoring and Recognition of Business Relationships – Person Connected with an Enhanced Risk State or Sanctioned Country or Organization

Overview

34. The risk that a business relationship is tainted by funds that are the proceeds of criminal conduct or are used to finance terrorism is increased where the business relationship is with a person 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* or the *financing of terrorism*, such measures being imposed by one or more countries or sanctioned by the *EU* or the *UN* – a **sanctioned country or territory**.

35. Similarly, the risk that a business relationship is tainted by funds that are the proceeds of criminal conduct or are used to finance terrorism is increased where the business relationship or transaction is with a person connected with an organization subject to such measures or who is themselves subject to such measures - a **sanctioned country or territory**.

36. As part of its on-going monitoring procedures, a firm will establish appropriate procedures to **monitor** all client transactions and activity in order to **recognise** whether any business relationships are with such a person.

37. 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.

38. There is not a Statutory Requirement to **examine**, or have *policies and procedures* in place to examine, business relationships with a **sanctioned person, organization, country or territory** once they are recognised. This is because provisions in financial sanctions legislation must be followed. Inter alia, such provisions may prohibit certain activities or require the property of listed persons to be frozen. Further guidance[1] is published on the *Commission*'s website.

AML/CFT Codes of Practice

39. On-going monitoring must involve **examining** transactions and activity recognised as being with a person connected with an enhanced risk state.

40. A firm 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.

41. As part of its examination of the above transactions, a firm must examine, as far as possible, their background and purpose and set forth its findings in writing.

[1] https://www.jerseyfsc.org/industry/international-co-operation/sanctions/

Guidance Notes

42. A firm 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);
- whether it is practicable to monitor transactions or activity in real time (i.e. before client instructions are put into effect); and
- whether it is possible to establish appropriate standardised parameters for automated monitoring.

43. A firm 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 -** Client business and risk profile in line with Section 3.3.5 of this Handbook.
- **Enhanced risk states** - Appendix D1 of the *AML/CFT Handbook*.
- **Sanctioned countries** - Appendix D2 of the *AML/CFT Handbook* (Source 6 only).

44. A firm 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 client'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.

45. A firm 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 client's business and risk profile;
- adjusts, as necessary, its monitoring system e.g. refines monitoring parameters, enhances controls for more vulnerable services; 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.

6.3 Automated Monitoring Methods

Overview

46. Automated monitoring methods may be effective in recognising notable transactions and activity, and business relationships and transactions with persons connected to enhanced risk states and sanctioned countries and territories.

47. **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 client's business and risk profile.

48. Large or more complex firms may also use automated monitoring methods to facilitate the monitoring of significant volumes of transactions, or - in an e-commerce environment - where the opportunity for human scrutiny of individual transactions is limited.

49. What constitutes unusual behaviour by a client is often defined by the system. It will be important that the system selected has an appropriate definition of 'unusual' and one that is in line with the nature of business conducted by the firm.

50. Where an automated monitoring method (group or otherwise) is used, a firm 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).

51. Use of automated monitoring methods does not remove the need for a firm to otherwise remain vigilant. Factors such as staff intuition, direct contact with a client, and the ability, through experience, to recognise transactions and activity that do not seem to make sense, cannot be automated.

52. 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 clients may be particularly effective. However, where a firm 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 firm:

- Understands which business relationships and transaction types are screened.
- Understands the system's capacity for "fuzzy matching" (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.
- Records the basis for "discounting" alerts (e.g. false positives) to provide an audit trail.

53. 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"

54. Further information on screening practices may be found in a report published by the *Commission* in August 2014[2].

[2] http://www.jerseyfsc.org/pdf/Banking-AML-&-Sanctions-Summary-Findings-2014.pdf

6.4 Money Laundering Warning Signs for the Accountancy Sector

Overview

55. Article 13 of the *Money Laundering Order* requires firms to conduct ongoing monitoring of business relationships and take steps to be aware of transactions with heightened *money laundering* risks. The *Proceeds of Crime Law* requires firms to report suspicious transactions and activity (see Section 8 of this Handbook).

56. This Section highlights a number of warning signs for accountants generally and for those working in specific business areas to help firms decide where there are reasons for concern or the basis for a reportable suspicion.

57. Because money launderers 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 client's risk profile, or give cause for concern.

6.4.1 Secretive Clients

58. Whilst face to face contact with clients is not always possible, an excessively obstructive or secretive client may be a cause for concern. Consideration should be given as to whether clients who demand strict confidentiality relating to their financial and business affairs are evading tax or seeking to mask the true beneficial ownership of their assets.

6.4.2 Unusual Instructions

59. Instructions that are unusual in themselves, or that are unusual for the firm or the client 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, 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; and
- excessive use of off-balance sheet transactions or activity.

6.4.2.1 Instructions Outside the Firm's Area of Expertise

60. Taking on work which is outside the firm's normal range of expertise can present additional risks because a money launderer might be using the firm to avoid answering too many questions. An inexperienced accountant might be influenced into taking steps which a more experienced accountant would not contemplate. Accountants should be wary of highly paid niche areas of work in which the firm has no background, but in which the client claims to be an expert.

61. If the client is based outside Jersey, firms should satisfy themselves that there is a genuine legitimate reason why they have been instructed. For example, have the firm's services been recommended by another client or is the matter based near your firm? Making these types of enquiries makes good business sense as well as being a sensible *AML/CFT* check.

6.4.2.2 Changing Instructions

62. Instructions that change unexpectedly might be suspicious, especially if there seems to be no logical reason for the changes.

63. The following situations could give rise to cause for concern:

- a client deposits funds into a firm's client account, but then ends the transaction for no apparent reason;
- a client advises that funds are coming from one source and at the last minute the source changes; and
- a client unexpectedly requests that money received into a firm's client account be sent back to its source, to the client or to a third party.

6.4.3 Use of Client Accounts

64. Client accounts should only be used to hold client money for legitimate transactions for clients, or for another proper legal purpose. Putting criminal money through a professional firm's client account can clean it, whether the money is sent back to the client, 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

65. If funding is from a source other than a client, firms may need to make further enquiries, especially if the client has not advised what they intend to do with the funds before depositing them into the firm's account. If it is decided to accept funds from a third party, perhaps because time is short, firms should ask how and why the third party is helping with the funding.

66. Enquiries do not need to be made into every source of funding from other parties. However, firms must always be alert to warning signs and in some cases will need to seek more information.

6.4.4 Accountancy and Audit Services

6.4.4.1 Intent

67. 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*.

68. If an individual or firm knows or believes that a client is acting in error, the client may be approached and the situation and legal risks explained to them. However, once the criminality of the conduct is explained to the client, 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 firm, clients should be referred to an appropriate specialist or legal adviser.

69. If there are reasonable grounds to suspect that a client knew or suspected that their actions were criminal, a report must be made. Even if the client does not have the relevant intent, but the firm is aware that there is criminal property, consideration needs to be given to whether a report has to be made to *JFCU*.

6.4.4.2 Holding of Funds

70. Firms who choose to hold funds as a stakeholder or escrow agent in commercial transactions 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.

71. 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 General Warning Signs

72. Any of the following general warning signs should prompt additional questions or investigation by those offering accountancy and *audit services*:

- use of many different firms of *auditor*s and advisers for connected companies and businesses;
- the client has a history of changing bookkeepers or accountants yearly; and
- 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.

6.4.4.4 Factors Arising from Action by the Entity or its Directors

73. Where an entity is actively involved in *money laundering*, the signs are likely to be similar to those where there is a risk of fraud, and 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.

6.4.4.5 Where the Client May Be Unknowingly a Party to Money Laundering

74. There may be occasions where the client has been duped by its own customers or clients into providing assistance or a vehicle for laundering criminal funds. Warning signs may be:

- unusual transactions without an explanation or a pattern of trading with one customer that is different from the norm;
- request for settlement of sales in cash;
- a client setting up a transaction that appears to be of no commercial advantage or logic;

- a client requesting special arrangements for vague purposes;
- unusual transactions with companies registered overseas;
- 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

75. 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 low risk of *money laundering* for those working in this area.

76. When winding up an estate, there is no blanket requirement that firms should be satisfied about the history of all of the funds which make up the estate under administration. However, firms 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, firms 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 territory, firms may need to make further checks about the source of those funds.

77. Firms 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.

78. Firms should bear in mind that an estate may include criminal property. An extreme example would be where the firm knows or suspects that the deceased person was accused or convicted of acquisitive criminal conduct during their lifetime.

79. If firms 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.

80. 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. Firms should remain alert to warning signs, for example if the deceased or their business interests are based in a higher risk jurisdiction.

81. If the deceased person is from another jurisdiction and a lawyer is dealing with the matter in the home country, firms may find it helpful to ask that person 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

82. While the majority of charities are used for legitimate reasons, they can be used as *money laundering* or the *financing of terrorism* vehicles.

83. Firms acting for charities should consider its purpose and the organisations it is 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, firms should be alert to unusual circumstances, including large sums of money.

6.4.7 Taxation Services

84. There are a number of tax offences which can give rise to the proceeds of crime and the need to submit a *SAR* to the *JFCU*. A tax practitioner 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.

85. There will however, be no question of criminality where the client has adopted in good faith, honestly and without mis-statement, a technical position with which the revenue authority disagrees.

86. The main areas where offences may arise in 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

87. It is not uncommon for tax practitioners to become aware of errors or omissions, in current or past years, from clients' 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 practitioner 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 practitioner may form a suspicion that the original irregularity was criminal in nature and this will then become a reportable suspicion.

6.4.7.2 Unwillingness or Refusal to Disclose to the Tax Authorities

88. Where a client indicates that they are unwilling, or refuse, to disclose the matter to the tax authorities in order to avoid paying the tax due, the client appears to have formed a criminal intent and therefore the reporting obligation arises. The tax practitioner 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 clients for whom the tax practitioner has declined to act.

6.4.7.3 Adjusting Subsequent Returns

89. 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.

6.4.7.4 Intention to Underpay

90. A client 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 practitioner can and should apply their professional body's normal ethical guidance to persuade the client to comply with the legislation. Should the client's intention in this regard still remain in doubt, the tax practitioner 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 once there are proceeds of crime.

6.4.7.5 Offences Applicable to Value Added Tax

91. A business client who is resident in the UK or another *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 guidance for the tax practitioner produced as an appendix to the *AML/CFT* guidance released by the UK Consultative Committee of Accountancy Bodies.

6.4.8 Business Recovery or Receiverships

92. *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 has invested criminal funds.

6.4.8.1 Observation of Unlawful Conduct Resulting in Advice

93. 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.

94. Examples of unlawful behaviour which may be observed, and may well result in advice to a client 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, firms 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 client 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

Please Note:

- Regulatory requirements are set within this section as *AML/CFT Codes of Practice*.
- This section contains references to Jersey legislation which may be accessed through the JFSC website.
- Where terms appear in the Glossary this is highlighted by the use of italic text. The Glossary is available from the JFSC website.

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 customer due diligence 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 firm determines that a client presents a higher risk of *money laundering* or the *financing of terrorism*, Articles 15, 15A and 15B of the *Money Laundering Order* also require enhanced *CDD* measures to be applied in the following specified scenarios:

Scenario	Section
Client, or some other person, is not physically present for identification purposes	7.4
Client has a "relevant connection" to an "enhanced risk state"	7.5
Client, or some other prescribed person, is a *PEP*	7.6
Client is a non-resident	7.7
Client is provided with private banking services	7.8
Client is a personal asset holding vehicle	7.9
Client is a company with nominee shareholders or issues bearer shares	7.10

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 clients (for instance identification of beneficial owner(s) and understanding the nature and purpose of the relationship) and significantly reduce the risk that criminals may hide behind "shell" companies or that the basis for the relationship is not considered or understood. 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 Sections 4 and 6 of this Handbook and must address the particular risk presented. This section provides some (non-exhaustive) examples for each category of client.

5. A client may be an individual (or group of individuals) or legal person. Section 4.3 deals with a client who is an individual (or group of individuals), Section 4.4 deals with a client (an

individual or legal person) who is acting for a legal arrangement, and Section 4.5 deals with a client who is a legal person.

6. Throughout this section, references to "client" include, where appropriate, a prospective client (an applicant for business). A client is a person with whom a business relationship has been formed or one-off transaction conducted.

7.2 Requirement to apply enhanced CDD measures

Statutory Requirements

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 client; (ii) a beneficial owner or controller of a client; (iii) a third party for whom a client 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 client, 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 or insufficiently applies the FATF Recommendations.*

9. *Article 15(1) of the Money Laundering Order requires a firm to apply enhanced CDD measures on a risk-sensitive basis in the following circumstances:*

- *if a customer has, or proposes to have, a business relationship or proposes to carry out a one-off transaction with the firm and the firm 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;*
- *if a customer has not been physically present for identification purposes;*
- *if the firm 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;*
- *if the customer of the firm is a company with nominee shareholders or that issues shares in bearer form;*
- *if the customer of the firm is –*
  - *a legal person established by an individual for the purpose of holding assets for investment purposes; or*
  - *a person acting on behalf of a legal arrangement established for an individual for the purpose of holding assets for investment;*
- *if the firm provides or proposes to provide a customer with private banking services;*
- *Any situation which by its nature can present a higher risk of money laundering.*

7.3 Higher risk client

Overview

10. Section 3.3 explains the risk based approach to *identification measures*. It explains that a firm must, on the basis of information collected, assess the risk that a business relationship or one-off transaction will involve *money laundering* or the *financing of terrorism*.

11. Enhanced CDD measures must be applied where a firm's assessment is that there is a higher risk of *money laundering* or the *financing of terrorism* (i.e. a situation which by its nature can present a higher risk of *money laundering* or the *financing of terrorism*).

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 firm may demonstrate that it has applied enhanced *identification measures* to an individual who is a higher risk client under Article 15(1)(b) of the *Money Laundering Order* where it obtains evidence that verifies a:

    › former name (such as maiden name); or

    › passport or national identity card number.

14. A firm may demonstrate that it has applied enhanced *identification measures* to a higher risk client 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 client's *source of wealth*.

    › where a firm 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 client's *source of wealth*.

    › where a firm 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 client has a connection about the *source of funds* involved and/ or client's *source of wealth*.

    › obtaining reliable information directly from the client 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 client has the relevant connection about the *source of funds* involved and/or client'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 client'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 client'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 relevant connection is established during the course of an existing relationship, a firm 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 client, a firm 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 client, e.g. a passport, subsequently expires, a firm 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).

17. A firm may demonstrate that it has applied enhanced on-going monitoring to a higher risk client 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 Client not physically present for identification measures

Overview

18. Frequently, relationships will be established where there is no face to face contact with the client to be identified or its beneficial owners or controllers, for example:

- relationships established by individuals through the post, by telephone or via the internet where external data sources are used to obtain evidence of identity; and
- 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 client, but where documentary evidence is to be provided at a time when the client is not present.

20. Such circumstances may increase the risk of *money laundering* or the *financing of terrorism* as it may be easier for criminals to conceal their true identity when there is no face to face contact with the firm. They may also increase the risk of impersonation or identity fraud being used to establish a 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, where the certifier has met the person at the time the documents are certified.

Statutory requirements

22. *Under Article 15(1)(b) of the Money Laundering Order, if a customer has not been physically present for identification purposes, a firm must apply enhanced CDD measures on a risk-sensitive basis.*

AML/CFT Code of Practice

23. A firm 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 client, 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 firm may demonstrate that it has applied enhanced *identification measures*: (i) under Article 15(1)(b) of the *Money Laundering Order*; and (ii) under the *AML/CFT Code of Practice* set in paragraph 23 above, where it finds out further information on a person (A), obtains an additional form of evidence of identity for A, or carries out some other additional measure in respect of 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 firm is part of a group, confirmation from another part of that group that A has been met (face to face).
- Confirmation from a *relevant person* that carries on a *regulated business* or a person who carries on an *equivalent business* that A has been met (face to face).
- Confirmation from a firm that carries on trust company business or a person who carries on an *equivalent business* that 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 firm's risk assessment for A, including:
  - requiring payment of funds to be drawn on an account in the client's name at a bank that is a *regulated person* or carries on an *equivalent business* (refer to Section 1.7 of this Handbook);
  - telephone contact with the client prior to establishing a relationship on a home or business number which has been verified, or a "welcome call" to the client before transactions are permitted, using the call to verify additional components of identity found out;
  - internet sign-on following verification measures where the client 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 Client with a 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* and the *financing of terrorism* risks and/or have in place insufficient *AML/CFT* 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". A person with a connection to these countries or territories presents a higher risk of being involved in *money laundering* or the *financing of terrorism* 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*, countries or territories in relation to which the *FATF* has called for the application of enhanced *CDD* measures are those listed in Appendix D1.

7.5.1 Application of enhanced CDD measures to a client with a relevant connection

Statutory Requirements

29. *Under Article 15(1)(c) of the Money Laundering Order, if the firm 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 firm must apply enhanced CDD measures on a risk-sensitive basis.*

For the purpose of 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; and

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 Code of Practice

30. The enhanced *CDD* measures applied to a client 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 senior management; and
- where there is a relevant connection because a client's *source of funds* is, or derives, from: (i) assets held in the state by the client or by any person on behalf of the client; or (ii) income arising in the state, taking reasonable measures to find out the *source of wealth* of the client.

Guidance Notes

31. A firm may demonstrate that it has taken reasonable measures to find out the *source of wealth* at the time that a relationship is established or one-off transaction carried out, where measures taken are commensurate with risk and include one or more of the measures listed in paragraph 14 above.

32. Where a relevant connection is established during the course of an existing relationship, a firm 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.

33. A firm 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 client, e.g. a passport, subsequently expires, a firm 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 of 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 Client who is a Politically Exposed Person (PEP)

Overview

34. Corruption by some high profile individuals, generally referred to as *PEP*s, inevitably involves 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.

35. 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 businesses and jurisdictions concerned, in addition to the possibility of criminal charges.

36. Indications that a client 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.

37. 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.

38. 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 firm 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.
- 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*.

39. There is no "one-size fits all" approach to applying enhanced *CDD* measures for *PEP*s.

40. The nature and scope of a firm's activities will generally determine whether the existence of *PEP*s in its client base is a practical issue for the business.

7.6.1 Determining whether a client is a Politically Exposed Person (*PEP*)

Statutory requirements

41. *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; and*
- *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; and*
- *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 his or her 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.*

42. *Under Article 15A(4) for the purpose of deciding whether a person is a close associate of a person, a firm need only have regard to information which is in that person's possession or is publicly known.*

7.6.2 Enhanced CDD measures in relation to *PEP*s

Statutory requirements

43. *Article 15A of the Money Laundering Order applies to a firm:*

a) 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

b) 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

c) 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 firm

ii) a third party for whom the customer of the firm is acting,

iii) a beneficial owner or controller of a third party described in clause (ii),

iv) a person acting or purporting to act on behalf of the customer of the firm.

44. *A firm to whom this Article applies must apply enhanced customer due diligence measures on a risk-sensitive basis including –*

- *unless the firm 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 firm;*
- *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.*

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 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 Code of Practice

45. Policies and procedures maintained in line with Article 11 of the *Money Laundering Order* must recognise that clients may subsequently acquire *PEP* status.

Guidance Notes – foreign *PEP*s

46. Where the existence of *PEP*s is considered to be a practical issue, a firm may demonstrate that it has appropriate *policies and procedures* for determining whether a client or prescribed person is a *PEP* where it:

- assesses those countries and territories with which clients are connected, which pose the highest risk of corruption. See Section 3.3.4.1.
- finds out who are the current and former holders of prominent public functions within those higher risk countries and territories and determines, as far as is reasonably practicable, whether or not clients have any connections with such individuals (including through immediate family or close associates). In determining who are the current and former holders of prominent public functions, it may have regard to information already held by the firm and to external information sources such as the *UN*, the European Parliament, the UK Foreign and Commonwealth Office, the Group of States Against Corruption, and other external data sources.
- exercises vigilance where clients are involved in business sectors that are vulnerable to corruption such as, but not limited to, oil or arms sales.

47. Where a firm runs the details of all its clients and prescribed persons through an external data source to determine whether any is a *PEP*, it should nevertheless assess those countries and territories which pose the highest risk of corruption and exercise particular vigilance where clients are involved in business sectors that are vulnerable to corruption such as, but not limited to, oil or arms sales.

48. In a case where a *PEP* is a director (or equivalent) of a client, or person acting, or purporting to act for a client, and where no property of that *PEP* is handled in the particular business relationship or one-off transaction, a firm 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* role and reason why the *PEP* has such a role.

49. Similarly, where a *PEP* is a trustee or a general partner that is a client, 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 firm 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 *PEP*s

50. In determining whether someone is a domestic *PEP*, a firm should consider the criterion set out at Article 15A(3) – 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.

51. In the context of Jersey, this will include (but is not limited to) the following:

- Lieutenant-Governor
- Ministers (but not necessarily deputy Ministers)
- Chief Executive of the States of Jersey
- Director-Generals of the States of Jersey
- Attorney-General
- Solicitor-General
- Commissioners of the Jersey Financial Services Commission
- Director General of the Jersey Financial Services Commission
- Registrar of Companies
- Information Commissioner
- Comptroller and Auditor-General
- Bailiff
- Deputy Bailiff
- Judicial Greffier
- Comptroller of Revenue
- HM Receiver General
- Senior Executives of State Owned Body Corporates (or similar)

52. Note that this will also include immediate family members and close associates of individuals listed above.

Higher Risk Domestic *PEP*s

53. Mandatory enhanced measures are only required in relation to higher risk relationships or transactions with domestic *PEP*s, as set out in Article 15A(1)(b).

54. Individuals entrusted with a prominent public function in Jersey may be considered to pose a low risk, unless a firm 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.

55. 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 firm 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 client

Overview

56. Clients 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 firm in that country or territory will typically have legitimate reasons for doing so. Some clients will, however, pose a risk of *money laundering* or the *financing of terrorism* 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

57. *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 firm and the firm 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 firm must apply enhanced CDD measures on a risk-sensitive basis.*

Guidance Notes

58. A firm 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 client is looking to establish a business relationship or carry out a one-off transaction other than in their home country or territory;
- the use of external data sources to collect information on the client and the particular country risk in order to build a client business and risk profile similar to that available for a resident client.

7.8 Client provided with private banking services

Overview

59. Private banking is generally understood to be the provision of banking and investment services to high net worth clients in a closely managed relationship. It often involves complex, bespoke arrangements and high value transactions across multiple countries and territories. Such clients may therefore present a higher risk of *money laundering* or the *financing of terrorism*.

60. For the avoidance of doubt, a trustee who may from time to time facilitate such banking or investment 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

61. *Under Article 15(1)(f) of the Money Laundering Order if the firm provides or proposes to provide a customer with private banking services, a firm must apply enhanced CDD on a risk sensitive basis.*

62. *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

63. A firm may demonstrate that it has applied enhanced *CDD* measures under Article 15(1)(f) of the *Money Laundering Order*, 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 Client that is a personal asset holding vehicle

Overview

64. 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.

Statutory Requirements

65. *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 client;

- the personal asset holding vehicle is the third party for whom a trustee or general partner (the client) is acting.

Guidance Notes

66. A firm 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:

- determining the purpose and rationale for making use of such a vehicle, and being satisfied that the client's use of such an investment vehicle has a genuine and legitimate purpose.
- taking reasonable measures to find out the *source of funds* and *source of wealth*.

7.10 Client that is a company with nominee shareholders or issues bearer shares

Overview

67. 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.

68. Notwithstanding this, 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.

69. Where one or more of the following circumstances apply, the client should not be considered to be a client that issues bearer shares for the purpose of Article 15(1)(d) 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 firm, the client or trusted external party along with an undertaking from that trusted external party or client to inform the firm of any transfer or change in ownership.

Statutory Requirements

70. *Under Article 15(1)(d) of the Money Laundering Order, if a customer of a firm is a company with nominee shareholders or that issues shares in bearer form, a firm must apply enhanced CDD measures on a risk-sensitive basis.*

Guidance Notes

71. A firm 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.

72. In the case of clients who are companies with nominee shareholders, additional measures may include:

- determining and being satisfied with the reasons why the client is making use of nominees; and

- 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.

73. In the case of clients 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 client has issued bearer shares or retains the ability to do so;
- ensuring that any new or continued relationship or any one-off transaction is approved by the senior management of the firm; and
- 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 Enhanced CDD measures - transitional arrangements

Overview

74. Where amendments to the *Money Laundering Order* introduce new *CDD* requirements applicable to client relationships and one-off transactions, these requirements do not apply retrospectively and no remediation project is required.

75. However, Article 13(1)(c)(ii) of the *Money Laundering Order* requires a firm to apply *identification measures* where the firm has doubts about the veracity or adequacy of documents, data or information previously obtained.

76. 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 the *AML/CFT Handbook*) a firm becomes aware that documents, data or information previously obtained do not satisfy the additional *CDD* requirements set out in the *Money Laundering (Amendment No.10) (Jersey) Order 2019*, the firm will need to apply enhanced *CDD* measures to that customer at that time, in line with the requirement in Article 13(1)(c)(ii) of the *Money Laundering Order*.

7.12 Exemptions from CDD requirements

Overview

77. 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 -17D and 18.

78. Article 17A provides circumstances in which exemptions under this Part do not apply, namely where:

a) the firm *suspects money laundering;*

b) the firm considers that there is a higher risk of *money laundering*;

c) the relevant customer is resident in a country that is not compliant with the *FATF* Recommendations; or

d) the relevant customer is a person in respect of whom Article 15(1)(c) applies.

79. In addition to the above a firm is not exempt under Articles 17B - 17D from applying third party identification requirements if the relevant customer is a person in respect of whom Article 15B(1) applies with regards 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. For the purpose of Part 3A , **relevant customer** means a customer of a firm that the firm knows or reasonably believes is –

a) a firm in respect of whose *financial services business* the *Commission* discharges supervisory functions, or a person carrying on *equivalent business*; or

b) a person wholly owned by a firm specified in sub-paragraph (a) (the "parent"), 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,

iii) the person's activity is ancillary to the business in respect of which the *Commission* discharges supervisory functions, or to *equivalent business* carried on by the parent, and

iv) in relation to that activity, the person maintains the same *policies and procedures* as the parent;

c) **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).

d) **non-public fund** means a scheme falling within the definition of "collective investment fund" in Article 3 of the Collective Investment Funds (Jersey) Law 1984, except that the offer of units in the scheme or arrangement is not an offer to the public within the meaning of that Article.

7.13 Exemption from applying third party identification requirements in relation to relevant customers acting in certain regulated, investment or fund services business

Statutory Requirements

81. *Under Article 17B(1) of the Money Laundering Order, a firm 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", or equivalent business; or*

› *that is an investment business or fund services business registered under the Financial Services (Jersey) Law 1998, or equivalent business.*

82. *Under Article 17B(2) of the Money Laundering Order, a firm 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 Code of Practice

83. A firm must be able to demonstrate that the conditions required by the *Money Laundering Order* are met.

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

84. *Under Article 17C(1) of the Money Laundering Order a firm 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 Law, or equivalent business;

c) carries on trust company business and is registered to carry on such business under the Financial Services (Jersey) Law 19987, or equivalent business, but only if the firm 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 Law, or

iii) an accountant carrying on a business described in paragraph 2 of Part B of Schedule 2 to the Law; or

d) is an independent legal professional carrying on a business described in paragraph 1 of Part B of Schedule 2 to the Law and is registered to carry on such business under the Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008, but only if the firm is carrying on deposit-taking business.

85. *Under Article 17C(2), a firm who 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 firm, without delay and in writing, with the information obtained from applying the identification measures, if so requested by the firm,

iii) will keep the evidence obtained during the course of applying the identification measures, and

iv) will provide the firm with that evidence without delay, if requested to do so by the firm.

86. *Under Article 17C(3) 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 firm in relation to a business relationship or transaction.*

87. *Article 17C(4) provides that a relevant person (including a person who was formerly a relevant person) who has given an assurance to another person under paragraph (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 paragraph (2)(b)(i) (see paragraph 97 above).*

Guidance Notes

88. In relation to the exemption set out at Article 17C(1)(a) or (b) of the *Money Laundering Order*, a firm may be satisfied that there is little risk of *money laundering* or the *financing of terrorism* 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.

89. A firm may demonstrate that it has found out the identity of a significant third party where:

› for lower risk relationships, it has found out the identity of each third party whose financial interest is over a general threshold of 25%.

90. For the purposes of Article 17C(9A) of the *Money Laundering Order*, a firm may demonstrate that it has found out the identity of a third party where:

› For third parties who are natural persons - it finds out the name, address and date of birth of the third party.

› For third parties who are legal persons or legal arrangements – it finds out the name, date and country of incorporation (or equivalent) and registered office address (or equivalent) of the third party.

91. In relation to the exemption set out at Article 17C(1)(c)(iii) of the *Money Laundering Order*, a firm may demonstrate that by reason of the nature of the relationship with the client that there is little risk of *money laundering* or the *financing of terrorism* occurring where the service provided to a trust company business client 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.

92. A firm 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.

93. For example, the provision of generic information on Jersey accounting or tax requirements, to a person carrying on trust company business, that requires no more than an explanation of a Jersey accounting or tax requirement and which attracts a nominal fee, may be illustrative of a service which presents little opportunity for *money laundering* to occur. Whereas, by contrast, the provision of detailed and complex tax structuring services that requires detailed information of the person or arrangement in question to be collected and which attracts more than a nominal fee, may not.

7.14.1 Assessment of risk

Overview

94. The risk factors that are set out in this section will also be relevant to a client 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

95. *Immediately before applying the exemptions set out in Part 3A, Article 17B(2) and 17D(2) of the Money Laundering Order, a firm is required to conduct an assessment as to whether it is appropriate to do so, having regard to the customer's business and the higher risk of money laundering and the financing of terrorism, should the 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.*

96. *Article 17B(2) and 17D(2) require a firm to prepare a written record of the reason why it is appropriate to apply CDD exemptions.*

97. *Article 17D(3) of the Money Laundering Order also provides 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, and in conducting such tests, consider whether the relevant customer may be prevented, by application of a law, from providing that information or evidence.

98. *As a result of conducting tests, if the relevant person is unable to establish that the relevant customer complies with the above requirements under Article 17D (3)(b), (c) or (d), the relevant person must immediately apply the identification measures specified in Article 13(1)(a) and 13(1)(c)(ii).*

AML/CFT Code of Practice

99. In a case where, for a particular business relationship, testing under Article 17D(3) of the *Money Laundering Order* highlights that a client 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 firm must review the basis upon which it has applied CDD exemptions to other relationships with that particular client (if any) in order to determine whether it is still appropriate to apply those measures.

Guidance Notes

100. Immediately before applying the exemption under this Part, a firm may demonstrate that it has had regard to a client's business where it considers the following factors:

- the general risk appetite of its client;

- the geographic location of its client's customer base;
- the general nature of the client's customer base, e.g. whether institutional or private client;
- the nature of the services that the client provides to its customers;
- the extent to which its client carries on business with its own customers on a non-face to face basis or customers are otherwise subject to enhanced *CDD* measures; and
- the extent to which customers of its client may be *PEP*s or present a higher risk of *money laundering* or the *financing of terrorism*, and the *source of funds* of such *PEP*s.

101. Immediately before applying the exemption under this Part, a firm may demonstrate that it has had regard for the higher risk of *money laundering* and the *financing of terrorism* should its client 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 its client.
- The adequacy of the framework to combat *money laundering* and the *financing of terrorism* (including for the avoidance of doubt, financial sanctions) in place in the country or territory in which its client is based and the period of time that the framework has been in place.
- The adequacy of the supervisory regime to combat *money laundering* and the *financing of terrorism* to which its client is subject.
- The adequacy of *identification measures* applied by its client to combat *money laundering* and the *financing of terrorism*.
- The extent to which the client itself relies on obliged parties (however described) to identify its customers and to hold evidence of identity, and whether such obliged parties are *relevant person*s or carry on an *equivalent business*.

102. A firm may demonstrate that it has considered the adequacy of *identification measures* applied by its client where it takes one or more of the following steps:

- Reviews previous experience (if any) with the client.
- Makes specific enquiries, e.g. through use of a questionnaire or series of questions.
- Reviews relevant *policies and procedures*.
- Where the client 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 client's *policies and procedures* to combat *money laundering* and the *financing of terrorism*, whether through onsite visits, or through requesting specific *CDD* information and/or copy documentation to be provided.

7.15 Further exemptions from applying identification requirements

Overview

103. Article 18 of the *Money Laundering Order* provides specified circumstances where exemptions from applying identification requirements may be used.

Statutory Requirements

Case 1. Insurance business

104. *Under Article 18(1), 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.

Case 2. Pension, superannuation, employee benefit, share option or similar scheme

105. *Under Article 18(2), 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.

Case 3. Regulated person and those carrying on equivalent business

106. *Under Article 18(3), 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,

iii) the person's activity is ancillary to the regulated business or equivalent business carried on by the parent,

iv) in relation to that activity, the person maintains the same policies and procedures as the parent.

Case 4. Public authority or body corporate with listed securities

107. *Under Article 18(4), 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 (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 the securities of which are listed on an IOSCO-compliant market or on a regulated market (within the meaning of Article 2(5)); or

c) a person wholly owned by a person mentioned in sub-paragraph (b).

Case 5. Person authorised to act on behalf of a customer

108. *Under Article 18(5), 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.

AML/CFT Code of Practice

109. For each case described in Article 18 of the *Money Laundering Order*, a firm must obtain information on the purpose and intended nature of the business relationship or one-off transaction.

110. A firm must obtain and retain documentation establishing that the client is entitled to benefit from an exemption in Article 18 of the *Money Laundering Order*.

7.15.1 Pension, superannuation, employee benefit, share option or similar schemes

Overview

111. Where a firm 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*.

112. However, the exemption cannot be applied if a firm considers that there is a higher risk of *money laundering* or the *financing of terrorism*.

Guidance Note

113. A firm may demonstrate that it considers whether there is a higher risk of *money laundering* or the *financing of terrorism* when, inter alia, it considers the reputation of the sponsoring employer and adequacy of controls in place over membership.

7.15.2 Jersey Public Authority

Overview

114. Where a client is a public authority 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 authority, on the beneficial owners and controllers of the authority, or those purporting to act on behalf of the authority.

115. However, the obligation to apply *identification measures* to any third party for which the authority may be acting and obligation to verify the authority of persons acting on behalf of the authority continue.

116. 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; or

› A parish authority.

7.15.3 Body corporate with listed securities

Overview

117. Where a client is a body corporate the securities of which are listed on a market that conforms to international standards set by *IOSCO* or on a regulated market (defined in Article 2(5) of the *Money Laundering Order*), then, in line with Article 18(4)(b) of the *Money Laundering Order*, there is no requirement to apply *identification measures* on that body corporate (or any wholly owned subsidiary), on the beneficial owners and controllers of the body (or any wholly owned subsidiary), or those purporting to act on behalf of the body corporate (or any wholly owned subsidiary).

118. However, the obligation to apply *identification measures* to any third party for which the body corporate (or wholly owned subsidiary) may be acting and obligation to verify the authority of persons acting on behalf of the body corporate (or wholly owned subsidiary) continue.

119. 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.

120. Whilst there is not a list of countries and territories that "fully implement" or "broadly implement" *IOSCO* Principles 16 and 17, reference may be made to *IMF* compliance assessments at: http://www.imf.org/external/NP/fsap/fsap.aspx.

121. Guidance published by the UK's Joint Money Laundering Steering Group addresses what may be considered to be a regulated market.

7.15.4 Regulated person and those carrying on equivalent business

Overview

122. Where a client is: (i) a *regulated person* (defined in Article 1(1) of the *Money Laundering Order*); (ii) a person who carries on *equivalent business* to any category of *regulated business*; or (iii) wholly owned by a person listed in (i) or (ii) 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 client, the beneficial owners and controllers of the client, or those purporting to act on behalf of the client. Nor is there a requirement to verify the authority of any person purporting to act for the client.

123. However, these provisions do not also provide an exemption in respect of any third party (or parties) for whom the client is acting, or for the beneficial owners and controllers of such a third party (or parties).

7.15.5 Person authorised to act on behalf of a client

Guidance Notes

124. Where a person authorised to act on behalf of a client holds this role by virtue of *his* employment by (or position in) a business that is a *regulated person* (or equivalent), a firm may demonstrate that this exception applies where it obtains:

› the full name of the individual; and

› an assurance from the employer that the individual is an officer or employee.

7.16 Simplified identification measures - obtaining evidence of identity for very low risk products/services

Overview

125. Where funds involved in a relationship:

› have been received from a bank that is a *regulated person* or carries on *equivalent business* to deposit-taking (refer to Section 1.7); and

› have come from an account in the sole or joint name of the client 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 the person is said to be where the product or service requested by the client is considered to present a very low *money laundering* or the *financing of terrorism* risk. This will be the case where funds may only be received from, and paid to, an account in the client's name, i.e. a product or service where funds may not be paid in by, or paid out to, external parties.

126. In the event that any of the conditions set below are breached, evidence of identity for the client must be obtained at that time in accordance with Sections 4 and 7 of the *AML/CFT Handbook*.

AML/CFT Codes of Practice

127. This concession must not be applied where a firm suspects *money laundering* or the *financing of terrorism*, in any situation which by its nature can present a higher risk of *money laundering* or the *financing of terrorism*, where the client has a relevant connection to a country or territory that is subject to a *FATF* call to apply countermeasures, or where the client is resident in a country or territory that is not compliant with the *FATF* Recommendations.

128. To benefit from this 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 (refer to Section 1.7), where the account can be confirmed as belonging to the client;

› 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 client, where he or she is 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 (refer to Section 1.7), where the account can be confirmed as belonging to the client, or on the death of the client 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.

129. A firm 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 (refer to Section 1.7), and, where a request for a withdrawal or transfer to another bank account is received, confirmation that this account is also in the client's name and held at a bank that is a *regulated person* or carries on an *equivalent business* to deposit-taking (refer to Section 1.7).

130. If a firm has reason to suspect the motive behind a particular transaction or believes that the business is being structured to avoid standard *identification measures*, it must not use this concession.

8 REPORTING MONEY LAUNDERING AND THE FINANCING OF TERRORISM

Please Note:

- Regulatory requirements are set within this section as *AML/CFT Codes of Practice*.
- This section contains references to Jersey legislation which may be accessed through the JFSC website.
- Where terms appear in the Glossary this is highlighted by the use of italic text. The Glossary is available from the JFSC website.

8.1 Overview of Section

1. Under the *Proceeds of Crime Law* and *Terrorism Law* where any person conducting *financial services business* in or from within Jersey forms a knowledge, suspicion, or has reasonable grounds to suspect *money laundering* or the *financing of terrorism* activity relating to business that is conducted in Jersey, then it must report its knowledge or suspicion to the *JFCU*.
2. Under the *Money Laundering Order*, an accountancy firm undertaking Schedule 2 business must have procedures in place for reporting knowledge or suspicion of money laundering or financing terrorism activity to the *JFCU*.
3. This Section outlines the statutory provisions concerning reporting that apply to: (i) an employee of a *relevant person*; and (ii) a *relevant person*, in the course of carrying on any trade profession or business (including Schedule 2 business). It also sets *AML/CFT 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
   - *MLRO*s (and *deputy MLRO*s) 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 application of tipping off provisions.
5. An important precondition for making a report 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 report may also be based on information from other sources, including law enforcement agencies, other government bodies, the media, or the client.
7. Whilst this Section describes reports made to the *JFCU* under the *Proceeds of Crime Law* and *Terrorism Law* as *SAR*s, 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. Additional information on reporting is contained within Part 2 of the *AML/CFT Handbook*.

8.2 Reporting Knowledge or Suspicion

Overview

9. Legislation deals with reporting by a firm and employee in the course of carrying on a *financial services business* (distinct from other 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 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 that property is 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**. Take the situation of a firm that knows or suspects, or has reasonable grounds for knowing or suspecting, that property constitutes or represents the proceeds of criminal conduct, and which 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 under Article 32 of the *Proceeds of Crime Law* – the effect being that it does not commit a *money laundering* offence under Article 30 (and perhaps also Article 31) of that law.

11. There is also a reporting requirement (Article 34A) and protection for reporting (Article 32) in a case where information or a matter comes to a firm's attention other than in the course of carrying on a *financial services business* (i.e. **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 reporting procedures. Such procedures must provide for securing 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.

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 relationship or one-off transaction (a series of linked transactions).

8.2.1 Requirement to Disclose of Knowledge or Suspicion within a Firm

Overview

15. In the course of carrying on a *financial services business*, employees of a firm must 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 *financing of terrorism*; or

- Property constitutes or represents the proceeds of criminal conduct; or
- Property is, or may be, terrorist property.

16. What may constitute reasonable grounds for knowledge or suspicion will be determined from facts or circumstances from which an honest and reasonable person working in a firm would have inferred knowledge or formed a suspicion (the so called "objective test"[1]).

17. Something which appears unusual is not necessarily suspicious and will likely form the basis for examination. This may, in turn, require judgement to be exercised as to whether something is suspicious.

18. A firm's *MLRO* (or *deputy MLRO*) must consider all internal *SAR*s as soon as practicable.

19. A firm's *MLRO* (or *deputy MLRO*) must make an external *SAR* as soon as is practicable if he or she knows, suspects or has reasonable grounds for knowing or suspecting, that:

- Another person is engaged in *money laundering* or the *financing of terrorism*; or
- Property constitutes or represents the proceeds of criminal conduct; or
- Property is, or may be, terrorist property.

20. 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 information or matter reported.

21. Under the *Proceeds of Crime Law*, the requirement to report applies in relation to the proceeds of criminal conduct which 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.

22. Under the *Terrorism Law*, the requirement to report applies in relation to property which is intended to be used 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.

23. Other than in the course of carrying on a *financial services business* (i.e. any other trade, profession or business carried on by a firm), employees of a firm must also 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 other matter on which knowledge or suspicion is based comes to them in the course of their employment. This will be so 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.

24. 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 *financial services business*. This means that such matters, in the absence of a specific Jersey connection, are not required to be reported.

Statutory Requirements

25. *Under Article 34D(4) of the Proceeds of Crime Law, a relevant person and employee of that relevant person are required to make a report where two conditions are fulfilled.*

26. *The first is that they know, suspect or have reasonable grounds for suspecting that:*

[1] See Part 2 of the AML/CFT Handbook.

- *Another person is engaged in money laundering or the financing of terrorism; or*
- *Any property constitutes or represents the proceeds of criminal conduct.*

27. *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****.*

28. *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.*

29. *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).*

30. *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 he or she has 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.*

31. *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.*

32. *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, he or she must report to a designated police officer or designated customs officer as soon as is practicable using the approved form. Inter alia, delivery of the approved form must comply with the requirements (including those in respect of delivery) indicated on the approved form.*

33. *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.*

34. *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.*

35. *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.

36. *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.*

37. *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.*

38. *"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 outside Jersey, would have constituted such an offence if occurring in Jersey.*

39. *Articles 19 to 22 of the Terrorism Law contain similar reporting requirements in respect of the financing of terrorism.*

40. *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.*

41. *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.*

42. *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.***

43. *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 an entity which commits, prepares or instigates an act of terrorism or facilitates the commission, preparation or instigation of an act of terrorism.*

44. *The meaning of "terrorism" is defined in Article 2 of the Terrorism Law and the meaning of "terrorist entity" is defined in Article 4*.

8.2.2 Protective Report

Overview

45. In the course of carrying on its business, employees of a firm 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;
- Property is terrorist property; or
- They are providing a service for the purposes of terrorism or for the support of a terrorist entity.

46. This will be so **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.

47. A firm's *MLRO* (or *deputy MLRO*) must consider all internal *SAR*s as soon as practicable.

48. Under the *Proceeds of Crime Law*, a firm's *MLRO* (or *deputy MLRO*) will make an external *SAR* before the firm does a particular act, or as soon as reasonably practicable after the person has done the act in order to be protected.

49. Under the Terrorism Law, a firm's *MLRO* (or *deputy MLRO*) will make an external *SAR* before the firm does a particular act or as soon as reasonably practicable after the person becomes involved in the transaction or arrangement.

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 certain conditions are fulfilled) where it makes such a protective report.

51. Under the *Proceeds of Crime Law*, protection for reporting applies in relation to the proceeds of criminal conduct which 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 to be used 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.

53. In this section, for the purpose of Article 21 of the *Money Laundering Order*, "approved form" means the form approved by the Minister, which could be changed from time to time.

Statutory Requirements

54. *Where a relevant person and employee of a relevant person suspect or believe that any property constitutes or represents the proceeds of criminal conduct and make 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.*

55. *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.*

56. *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.*

57. *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, he or she must report to a designated police officer or designated customs officer as soon as is practicable using the approved form. Inter alia, delivery of the form must comply with the requirements (including those in respect of delivery) indicated on the form.*

58. *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.*

59. *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.*

60. *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.*

61. *"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 outside Jersey, would have constituted such an offence if occurring in Jersey.*

62. *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.*

63. *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

64. The three mental elements of knowledge, suspicion, and reasonable grounds for suspicion, which are relevant to statutory offences are not terms of art and are not defined within the statutes. However, case law has provided some guidance on how they should be interpreted.

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. The term 'suspects' is one which the court has historically avoided defining; however, because of its importance in English criminal law, some general guidance has been given. In the case of *Da Silva* [1996] EWCA Crim 1654, Longmore LJ stated:

'It seems to us that the essential element in the word "suspect" and its affiliates, in this context, is that the defendant must think that that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice.'

67. 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.

68. The test for whether a person holds a suspicion is an objective one. 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* is taking place for there to be a suspicion.

69. The meaning of suspicion detailed above was also confirmed by the Court of Appeal in the case of K v NatWest [2006] EWCA Civ 1039.

70. If someone has not yet formed a suspicion, but they have cause for concern, a firm may choose to ask the client or others more questions. This choice depends on what is already known, and how easy it is to make enquiries.

71. If there is a belief that a client is innocent, but there are suspicions that another party to a transaction is engaged in *money laundering*, a firm may need to consider referring the client for specialist advice regarding the risk that they may be a party to one of the principal offences.

72. Sections 2.3.1.1 and 3.3.4 of this Handbook contain a number of standard warning signs which may give cause for concern. However, whether someone has a suspicion is a matter for their own judgement.

8.2.3.3 Reasonable Grounds to Suspect: The Objective Test of Knowledge or Suspicion

73. Article 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, using, concealing etc with criminal or terrorist property where there are reasonable grounds to know or suspect that property represents the proceeds of crime or terrorist property.

74. 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, if they had reasonable grounds for knowing or suspecting that it was. In other words, were there factual circumstances from which an honest and reasonable person, engaged in a similar business, should have inferred knowledge or formed the suspicion that another was engaged in *money laundering*, or there was knowledge of circumstances which would put an honest and reasonable person on enquiry.

75. It is important that accountants, *auditors* and tax advisers do not turn a blind eye to information that comes to their attention. Reasonable enquiries should be made, such as a professional with their qualifications, experience and expertise might be expected to make in such a situation within the normal scope of their assignment or client relationship. A reasonable conclusion should then be drawn, such as may be expected of a person of their standing.

76. Accountants, *auditors* and tax advisers should exercise a healthy level of professional scepticism, and if unsure of the action that should be taken, consult with the *MLRO* or otherwise in accordance with their firm's procedures. If in doubt, such individuals should err on the side of caution and make a report to their *MLRO*.

8.2.4 Auditors' Further Enquiries

Overview

77. Once an *auditor* suspects a possible breach of legislation, further enquiries will need to be made to assess the implications of this for the audit of the financial statements. Auditing standards on legislation requires that when the *auditor* becomes aware of information concerning a possible instance of non-compliance, the *auditor* should obtain an understanding of the nature of the act and the circumstances in which it has occurred. Sufficient other information must be obtained to evaluate the possible effect on the financial statements.

78. *Money laundering* legislation does not require the *auditor* to undertake any additional enquiries to determine further the details of the predicate criminal offence. To minimise any risk of tipping-off, it is important that any further enquiries represent only steps that the *auditor* would have performed as part of the normal audit work and that the *MLRO* is consulted before any further enquiry is performed. If the *auditor* is genuinely uncertain as to whether or not there are grounds to make a disclosure, they may wish to seek advice from the *MLRO*.

79. 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 in itself an offence, it is possible that in some circumstances, a report may need to be made.

80. Where the *auditor* makes a report to the *MLRO* and the *MLRO* decides 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*.

81. The *auditor* will need to consider whether continuing to act for the company 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 itself, in particular, the offence of becoming involved in an arrangement. In those circumstances the *auditor* may want to consider whether to resign, but should firstly contact the firm's *MLRO*, both to report the suspicion and to 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* for such an action to be taken.

82. Partners and employees in audit firms will need to follow their firm's internal reporting procedures when considering whether to include documentation relating to *money laundering* reporting in the audit working papers.

8.3 Procedures for Reporting

Overview

83. Reporting procedures provide the interface between *CDD* measures carried out by a firm and the work of the *JFCU*'s intelligence wing. Like all *policies and procedures*, they should be drafted in a way that can be readily understood by employees, should be tailored to the firm's risk assessment, and applied in every case where functions are outsourced (in line with Section 2.4.4 of this Handbook).

Statutory Requirements

84. *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 a 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 a deputy MLRO) to have access to all other information which may be of assistance in considering the report; and*
- *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.*

85. *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 a report, 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 Codes of Practice

86. In addition to the reporting procedures that must be maintained under Article 21 of the *Money Laundering Order*, a firm must maintain procedures that:

- highlight that reporting requirements extend to business relationships and one-off transactions that are declined (i.e. where no business relationship is established or transaction carried out);
- highlight that internal *SAR*s are to be made regardless of the amount involved in a transaction or relationship and regardless of whether, amongst other things, it is thought to involve tax matters;
- highlight the importance attached to making an internal *SAR* as soon as practicable;
- require internal *SAR*s to be acknowledged by the *MLRO* (or a *deputy MLRO*) as soon as is practicable;
- require the *MLRO* (or *deputy MLRO*) to record all internal *SAR*s in a register (including details of the date of the internal *SAR*, identity of the individual making the internal *SAR*, and information to allow supporting documentation to be retrieved on a timely basis).

87. A firm must not allow internal *SAR*s 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, they must emphasise that the decision on reporting remains with that employee.

88. A firm must establish and maintain arrangements for disciplining any employee who fails, without reasonable excuse, to make an internal *SAR* where he or she has knowledge, suspicion or reasonable grounds for knowledge or suspicion, or does not do so as soon as is practicable.

Guidance Notes

89. A firm 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 failure to do so as soon as is practicable.

90. A firm may demonstrate that employees make internal *SAR*s as soon as practicable where the *MLRO* (or *deputy MLRO*) periodically considers (by business area if appropriate):

- The period of time 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 *SAR*s, and concludes that both are consistent with the firm's business risk assessment.

8.3.2 External SARs

Overview

91. 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 client. 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 client that a report to the *JFCU* may be being considered (though this may not yet be tipping off).

92. When considering an internal *SAR*, the *MLRO* (or *deputy MLRO*), taking account of the risk posed by the transaction or activity being addressed, will need to strike the 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 in searching a number of unlinked systems and records that might hold relevant information.

AML/CFT Codes of Practice

93. In addition to reporting procedures that must be maintained under Article 21 of the *Money Laundering Order*, a firm 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 not to make such a report, which must be retained with the internal *SAR*.
- Require the *MLRO* (or *deputy MLRO*) to record all external *SAR*s in a register (including the date of the report and information to allow supporting documentation to be retrieved on a timely basis).
- Require the *MLRO* (or *deputy MLRO*) to inform the *JFCU* where relevant information is subsequently discovered.

Guidance Notes

94. A firm may demonstrate that an internal *SAR* is considered in light of all other relevant information when it considers:

- 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 matters or relationships. Connectivity can arise through commercial connections, e.g. linked transactions or common referrals, or through individuals, e.g. third parties, beneficial owners and controllers or account signatories.
- The risk that assets will dissipate.

95. A firm may demonstrate that the *MLRO* (or *deputy MLRO*) reports as soon as practicable where senior management considers:

- The typical period of time taken by the *MLRO* (or *deputy MLRO*) to process an internal *SAR* (being the period between the date of the internal *SAR* and date of the external *SAR* (or decision taken not to report)).
- The number of internal *SAR*s not processed within a period of time set by senior management, together with an explanation.

8.4 JFCU Consent

Overview

96. Protective reports before or after doing an act are not equal options which a firm can choose between.

- A report should be made **before doing an act** where a client instruction is received prior to an activity or transaction taking place, or arrangements being put in place. However, when an activity or transaction which gives rise to concern has already been actioned and where a delay would lead to a breach of a contractual obligation, the *MLRO* (or *deputy MLRO*) may need to let the activity or 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.

97. The receipt of a protective report concerning an act (transaction or activity) that has already occurred in an established business relationship (the continuation of which is considered to be another future act) will be acknowledged by the *JFCU*, and in the absence of any instruction to the contrary from the *JFCU*, a firm will generally be provided with consent to maintain the client relationship (the future act) under normal commercial circumstances (referred to as consent to operate normally). However, receipt of such consent from the *JFCU* in these circumstances does not indicate that the knowledge or suspicion is with or without foundation, and other future acts (transactions or activity) should continue to be monitored and reported, as appropriate.

98. In the vast majority of cases in which an external *SAR* is made, consent to continue an activity, process a transaction, or continue a business relationship is provided by the *JFCU* within seven working days of receipt of a report (indeed, the *JFCU* responds within two working days in the majority of cases). However, it should be noted that the *JFCU* is not obligated to provide consent within a particular time frame, or at all.

99. Consent may be delayed where information is required by the *JFCU* from an overseas financial intelligence unit. Consent may also be withheld where the report lacks sufficient detail to allow the *JFCU* to form a view on consent.

100. While waiting for the *JFCU* to provide consent to proceed with an activity or transaction (where it is necessary for consent to be provided), or in the event that the *JFCU* notifies a firm that consent will not be given, a firm should be aware of the risk of committing a tipping off offence where it fails to act on a client's instruction.

101. Where a firm does not wish to act upon a client's instruction, this may lead to civil proceedings being instituted by the client for breach of contract. It may be necessary in circumstances where a client has instigated civil proceedings for a firm to seek the directions of the court.

102. A firm may reduce the potential threat of civil proceedings by ensuring that clients' terms of business specifically:

- Allowing an instruction to be delayed or deferred, pending investigation.
- Exclude breaches in circumstances where following a client instruction may lead to the firm committing an offence.

8.5 Tipping-off

Overview

103. Except where otherwise provided, where a person knows or suspects that a *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*.

104. Except where 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 that is, or is about to be, conducted into *money laundering* or the *financing of terrorism*, a person will commit a tipping off offence where it:

- Discloses to another person any information relating to the investigation; or
- Interferes with material which is likely to be relevant to such an investigation.

105. Inter alia, the effect of this is that a firm or employee of a firm:

- Cannot, at the time, tell a client 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 client 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 client that a transaction or activity was delayed because an internal or external *SAR* had been made.
- Cannot tell the client that law enforcement is conducting an investigation.

106. However, a tipping off offence is not committed when a firm discloses: that an internal *SAR* has been made; that it will make, or has made, an external *SAR*; information relating to such *SAR*s; or information relating to a criminal investigation to its:

- **Lawyer** - in order to obtain legal advice or for the purpose of legal proceedings (except where the disclosure is made with a view to furthering a criminal purpose); 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 firm's financial statements (except where the disclosure is made with a view to furthering a criminal purpose).

107. Nor is a tipping off offence committed when a **lawyer** discusses that disclosure with its client 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 the disclosure with its client**.

108. In addition, a tipping off offence will not be committed where a disclosure is permitted under the Proceeds of Crime and Terrorism (Tipping Off – Exceptions) (Jersey) Regulations 2014 (the "***Tipping Off Regulations***") – a **protected disclosure**. So long as a disclosure meets conditions that are set in the *Tipping Off Regulations*, a disclosure will be a protected disclosure where it is:

- 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 *relevant person* (but not an *equivalent business*); or
- Made to the *Commission*.

109. Except where a disclosure 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*.

110. Whereas 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).

111. In a case where a firm:

- Is the client of a financial institution or designated non-financial business or profession (A) that is not a *relevant 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 other than where such a disclosure is made with the permission of the *JFCU*.

112. Care should 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.

113. In this section, a 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*).

Statutory Requirements

114. *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.*

115. *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 a money laundering or the financing of terrorism investigation - except if the disclosure is a **protected disclosure** under the Tipping Off Regulations.*

116. *It is a defence under Article 35(5) of both the Proceeds of Crime Law and Terrorism Law for a person charged with an offence to prove that they had a reasonable excuse for the disclosure or interference.*

117. *However, 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

118. *A person who is guilty of an offence under Article 35 is liable to imprisonment for a term not exceeding 5 years or a fine, or to both.*

119. *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.*

120. *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).*

121. *Regulation 3 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.*

122. *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.*

123. *Regulation 4 permits a relevant person and 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.*

124. *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.*

125. *Regulation 5 permits a relevant person and 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.*

126. *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).*

127. *Regulation 6 permits a relevant person and 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 Commission.*

128. *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 Code of Practice

129. In addition to reporting procedures that must be maintained under Article 21 of the *Money Laundering Order*, a firm must maintain procedures that remind employees making internal *SAR*s of the risk of committing a tipping off offence.

8.5.1 CDD Measures

Overview

130. 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 firm 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.

131. Where a firm suspects *money laundering* or the *financing of terrorism*, the application of *identification measures* could unintentionally lead to the client being tipped off, where the process is managed without due care.

132. In circumstances where an external *SAR* has been made, and where there is a requirement to conduct *identification measures*, the risk of tipping off a client (and its advisers) may be minimised 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 firm is concerned that applying *identification measures* will lead to the client being tipped off.

133. Where a firm reasonably believes that the application of *identification measures* could lead to the client 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.

134. Reasonable enquiries of a client conducted in a tactful manner regarding the background to a transaction or activity that is inconsistent with the usual pattern of transactions of activity is prudent practice, forms an integral part of *CDD* measures, and should not give rise to the tipping off offence.

8.5.2 Terminating a Relationship

Overview

135. The giving of consent by the *JFCU* following an external *SAR* is not intended to override normal commercial judgement, and a firm is not committed to continuing a business relationship with a client if such action would place the firm at commercial risk.

136. 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 firm must be free to make such judgements. However, in certain circumstances, a firm should consider liaising with the *JFCU* to consider whether it is likely that termination would alert the client or affect an investigation in any way. If there is continuing suspicion and there are funds which need to be returned to the client, a firm should seek advice from the *JFCU*.

8.6 Disclosure to Group Companies and Networks

Overview

137. Whereas the focus of the *Money Laundering Order* is on the role that a particular *relevant person* has in preventing and detecting *money laundering* and the *financing of terrorism*, where a firm is part of a group or larger network, it is important that it should be able to play its part in the prevention and detection of *money laundering* and the *financing of terrorism* at group or network level.

138. Accordingly, it is important that there should be no legal impediment to providing certain information to a group company or network.

139. Where a firm also wishes to disclose information to another *relevant 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 client to do so in certain circumstances.

Statutory Requirements

140. *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.*

141. *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 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 on Banking Supervision;*
- *the Objectives and Principles of Securities Regulation issued by IOSCO; or*
- *the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.*

8.7 The Auditor's Responsibility for Monitoring Compliance

Overview

142. 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. *Money laundering* legislation does not require the *auditor* to extend the scope of the audit save as set out in Section 8.8 of this Handbook but the normal audit work could 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 relating directly to the preparation of the financial statements;
- legislation which provides a legal framework within which the entity conducts its business;
- other legislation.

143. Auditing standards relating to legislation require the *auditor* to obtain sufficient appropriate audit evidence about compliance with legislation that has an effect on the determination of material amounts and disclosures in the financial statements. This may cause the *auditor* to be suspicious that, for example, fraud or tax offences have taken place, which may be criminal offences resulting in the acquisition of criminal property.

144. Auditing standards on legislation also require the *auditor* to perform procedures to help identify possible or actual instances of non-compliance with legislation which provides a legal framework within which the entity conducts its business and which are central to the entity's ability to conduct its business and hence to its financial statements. These procedures consist of:

- obtaining a general understanding of the legal and regulatory framework applicable to the entity and the industry and of the procedures followed to ensure compliance with that framework;
- inspecting correspondence with the relevant licensing or regulatory authorities;
- enquiring of those charged with governance as to whether they are on notice of any such possible instances of non-compliance with laws or regulations; and
- obtaining written representation that those charged with governance have disclosed to the *auditor* all known actual or possible 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.

145. 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*.

146. Legislation relating to *money laundering* will be central to an entity's business if the client falls within the definition of a '*financial services business*'. When auditing the financial statements of such businesses, the *auditor* must review the steps taken by the entity to comply with the *Money Laundering Order* and the *Commission*'s Regulatory Requirements, assess their effectiveness and obtain management representations concerning compliance with them. If the client's systems are thought to be ineffective, the *auditor* must consider whether there is a responsibility to report a matter of 'material significance' to the regulator and the possible impact of regulatory action (see also Section 8.8 of this Handbook).

147. The *auditor* will need to give consideration to whether any contingent liabilities might arise in this area. For example, there may be criminal fines for non-compliance with the *money laundering* legislation and/or the *Money Laundering Order*. In certain circumstances civil claims may arise or confiscation proceedings may give rise to contingent liabilities. The *auditor* will need to remain alert to the fact that discussions with the client on such matters may give rise to a risk of 'tipping-off' (see Section 8.5 of this Handbook).

148. In some situations, the audit client 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. Whether an act constitutes non-compliance with the *money laundering* legislation may involve consideration of matters which do not lie within the competence and experience of individuals trained in the audit of financial information. Provided that the *auditor* considers that the advice has been obtained from a suitably qualified and independent lawyer and that the lawyer was made aware of all relevant circumstances known to the *auditor*, the *auditor* may rely on such advice, provided the *auditor* has complied with auditing standards on using the work of an expert.

8.8 Reporting to Regulators

Overview

149. Reporting to the *JFCU* does not relieve the *auditor* from other statutory duties, examples of statutory reporting responsibilities include:

- **Audits of entities in the financial sector:** the *auditor* has a statutory duty to report matters of 'material significance' to the *Commission* which come to the *auditor's* attention in the course of audit work.
- **Audits of entities in the public sector**: *auditor*s of some public sector entities may be required to report on the entity's compliance with requirements to ensure the regularity and propriety of financial transactions. Activity connected with *money laundering* may be a breach of those requirements.
- **Audits of other types of entity**: *auditor*s of some other entities are also required to report matters of 'material significance' to regulators (for example, charities and occupational pension schemes).

8.9 Balancing Professional Work and Post-Reporting Requirements

Overview

150. Continuation of work post-reporting may require discussion with the client's senior management of matters relating to the suspicions that were formed. Care must be taken to select appropriate, and non-complicit, members of senior management for such discussions, always bearing 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 investigate a matter, unless this is within the scope of the professional work commissioned.

151. In more complex circumstances, consultation with law enforcement may be necessary before enquiries are continued, but in most cases a common sense approach will resolve the issue. It should be noted that neither the *JFCU* nor other law enforcement agencies may give consent to tipping-off, but discussions with them will still be valuable.

152. Firms may wish to consult the *MLRO* or other suitable specialist (for example a lawyer) regularly if there are tipping-off concerns. In particular, it is important that before any document referring to the subject matter of a report is released to a third part, the *MLRO* is consulted and, where necessary, law enforcement. Some typical examples of documents released to third parties are shown below as an aide memoire:

- public audit or other attest reports;
- public record reports to regulators;
- confidentiality reports to regulators;
- statements on the resignation as *auditor*s;
- professional clearance/etiquette letters; or
- communications to clients of intention to resign.

153. There is no legal mechanism for obtaining clearance from *JFCU* for the contents of such statements or other documents relating to resignation. However, firms may well wish in cases of complexity to discuss the matter with the *JFCU* in order to understand their perspective and document such discussion.

154. *MLRO*s may on occasion need advice to assist them in formulating their instructions to the firm. 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.

8.9.1 The Auditor's Report on Financial Statements

Overview

155. Where it is suspected that *money laundering* has occurred, the *auditor* will need to apply the concept of materiality when considering whether the *auditor's* report on the 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.

156. If it is known that *money laundering* has occurred and that directors or members of senior management of the company were knowingly involved, the *auditor* will need to consider whether the *auditor's* report is likely to include a qualified opinion on the financial statements. Any disclosure in the *auditor's* report is subject to the tipping-off requirements. It might be necessary for the *auditor*, through the *MLRO*, to discuss with the relevant law enforcement agency whether disclosure in the report on the financial statements, either through a qualified opinion or referring to fundamental uncertainty, could constitute a tipping-off offence. If so, the *auditor*, through the *MLRO*, will need to agree an acceptable form of words with the *JFCU*.

157. Whilst an attempt may be made to seek the views of the *JFCU* or the relevant law enforcement agency, it must be borne in mind that law enforcement may not be willing or able to agree on a form of words to use in communicating with the client. In such circumstances, the *auditor* is advised to consider whether it would be appropriate to seek legal advice, although appropriate consent cannot be given to tipping-off, it is unlikely that the *auditor* who uses a form of words agreed with the relevant law enforcement agency will commit a tipping-off offence.

158. Timing may be a crucial factor. Any delay in issuing the audit report pending the outcome of an investigation is likely to be impracticable and could in itself lead to issues of tipping-off. The *auditor* must also consider the potential dangers of tipping-off by not issuing the audit report as expected.

159. If an audit report has to be issued, and agreement with the relevant law enforcement agency cannot be reached, firms may need to seek legal advice before issuing a qualified audit report. As a last resort, it may be necessary to make an application to the court in respect of the content of the qualified audit report.

160. If a firm, having filed a *SAR*, wishes to terminate a relationship and is concerned that, in doing so, it may prejudice an investigation, it should seek advice from the *JFCU*. This is to avoid the danger of tipping-off. However, the *JFCU* cannot instruct a firm to continue a relationship that it wishes to terminate.

161. Firms may wish to resign if it is believed that the client or an employee is engaged in *money laundering* or any other illegal act, particularly where a normal relationship of trust can no longer be maintained. Where the *auditor* intends to cease to hold office, there may be a conflict between the requirements for the *auditor* to bring certain matter to the attention of members or creditors and the risk of tipping-off. In such circumstances the *auditor* should seek the advice of the *JFCU* and the appropriate investigating agency to agree 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.

162. The offence 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 the suspicions of *money laundering*, to do so would run the risk of tipping-off. Expressing such concerns orally rather than in writing does not alleviate the issue. However, in certain circumstances it may be necessary to communicate the underlying circumstances which gave rise to the disclosure. When doing so, advice should be taken from the *MLRO* who may need to seek an opinion from the *JFCU*.

8.10 Investigation and the Use of Court Orders

Overview

163. Following the receipt of a disclosure 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.

164. 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 *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.

165. During the course of an investigation, a firm 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 firm should consider what, if any, property may be utilised subject to having obtained the appropriate consent from the *JFCU*.

166. 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 legitimately obtained assets. A firm 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 commonplace 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.

167. Property may also be forfeited in Jersey utilising civil proceedings under the *Terrorism Law*.

168. From time to time, with a view to obtaining additional intelligence, the *JFCU* will issue general liaison notices to all *relevant person*s, or to a particular category of business. The *JFCU* will ensure that the requests contained within such notices are proportionate and reasonable in the circumstances. Firms are requested to respond with any relevant information as soon as is reasonably practicable.

8.10.1 Feedback from the JFCU

Overview

169. Because a significant proportion of *SAR*s 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 feedback on individual disclosures. However, on a regular basis, the *JFCU* will provide statistics, trends and advice to enhance the quality of disclosures, or issue periodic newsletters. In addition, the States of Jersey Police Annual Report contains some information on disclosures, prosecutions and confiscations.

9 SCREENING, AWARENESS AND TRAINING OF EMPLOYEES

Please Note:

- Regulatory requirements are set within this section as *AML/CFT Codes of Practice*.
- This section contains references to Jersey legislation which may be accessed through the JFSC website.
- Where terms appear in the Glossary this is highlighted by the use of italic text. The Glossary is available from the JFSC website.

9.1 Overview of the Section

1. One of the most important controls over the prevention and detection of *money laundering* and the *financing of terrorism* is to have appropriately screened employees who are: (i) alert to *money laundering* and the *financing of terrorism* risks; and (ii) well trained in the recognition of notable transactions or activity, which may indicate *money laundering* or the *financing of terrorism* activity (Section 6).
2. The effective application of even the best designed *systems and controls* (including *policies and procedures*) can be quickly compromised if employees lack competence or probity, are unaware of, or fail to apply, *systems and controls* (including *policies and procedures*), and are not adequately trained.
3. It is essential that a firm takes action to make sure that fee earners and other employees are:
   - competent and have probity;
   - aware of *policies and procedures* and their obligations under the *money laundering* legislation and the *Money Laundering Order* and *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law*; and
   - trained in the recognition of notable transactions or activities (which may indicate *money laundering* or the *financing of terrorism*) or transactions and activity with enhanced risk states and/ or sanctioned countries (Section 6).
4. In particular, fee earners and those other employees who handle or are responsible for the handling of client transactions will provide the firm with its strongest defence, or its weakest link.
5. The term "employee" is to be understood to include fee earners and other officers of the firm 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 firm under an outsourcing agreement.
6. A firm should also encourage its fee earners and other employees to "think risk" as they carry out their duties within the legal and regulatory framework governing *money laundering* and the *financing of terrorism*.

9.2 Screening of employees

Statutory Requirements

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 Code of Practice

8. A firm 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:

   › Fee earners and other employees handling or responsible for the handling of business relationships or one-off transactions;

   › Employees directly supporting fee earners, or who handle or are responsible for the handling of business relationships or one-off transactions, e.g. accounts and administration staff;

   › The *MLRO* (and any *deputy MLRO*) and *MLCO*; and

   › Senior management.

Guidance Notes

9. A firm 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.

   › 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[1] (or absence of such convictions).

9.3 Obligations to Promote Awareness and to Train

Overview

10. The *Money Laundering Order*'s requirements concerning both awareness training and training apply to employees whose duties relate to the provision of *financial services business* (hereafter referred to as '***relevant employees***'), and not to all employees of a firm. However, primary *money laundering* and the *financing of terrorism* offences established in the *Proceeds of Crime Law*, *Terrorism Law* and other legislation are wider in scope, and so all employees will need to have a basic understanding of *money laundering* and the *financing of terrorism*, and an awareness of internal reporting procedures and the identity of the *MLRO* (and, if applicable, *deputy MLRO*).

11. *Relevant employee*s will include fee earners, accounts and administration staff.

Statutory Requirements

12. *Article 11(9) to (11) of the Money Laundering Order requires 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 or the financing of terrorism; and*

[1] Enquiries into an individual's criminal past must be subject to the Rehabilitation of Offenders (Jersey) Law 2001, which prevents a *relevant 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.

- *the enactments in Jersey relating to money laundering and the financing of terrorism and any relevant AML/CFT 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; and*
  - *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; and

- *establish and maintain procedures that monitor and test the effectiveness of the financial services business' policies and procedures, employees' awareness and the training provided to employees.*

AML/CFT Codes of Practice

13. A firm must:

    - provide employees who are not *relevant employee*s with a written explanation of the firm's and employee's obligations and potential criminal liability under the *money laundering* legislation, including the implications of failing to make an internal *SAR*; and
    - require such employees to acknowledge that they understand the firm's written explanation and procedures for making internal *SAR*s.

14. In the case of a sole practitioner who is a sole trader, that person must be aware of the enactments in Jersey relating to *money laundering* and the *financing of terrorism* and *AML/CFT Codes of Practice*.

15. In the case of a sole practitioner who is a sole trader, that person must be able to recognise and handle: (i) transactions carried out by or on behalf of a person who is or appears to be engaged in *money laundering* or the *financing of terrorism*; and (ii) other conduct that indicates a person is or appears to be engaged in *money laundering* or the *financing of terrorism*.

Guidance Notes

16. A firm may demonstrate that it has satisfied awareness raising and training obligations that apply to *relevant employee*s where it includes:

    - fee earners and other employees handling or responsible for the handling of business relationships or one-off transactions;
    - employees directly supporting fee earners, or who handle or are responsible for the handling of business relationships or one-off transactions, e.g. accounts and administration staff;
    - the *MLRO* (and any *deputy MLRO*) and *MLCO*; and
    - senior management.

17. In the case of a sole practitioner who is a sole trader, that person may demonstrate that they are aware of relevant enactments (under paragraph 15) and able to recognise and handle transactions and other conduct (under paragraph 15) where they have received formal training or through self-study.

9.4 Awareness of Relevant Employees

Overview

18. With the passage of time between training initiatives, the level of employee awareness of the risk of *money laundering* and the *financing of terrorism* decreases. The utilisation of techniques to maintain a high level of awareness can greatly enhance the effectiveness of a firm's defences against *money laundering* and the *financing of terrorism*.

Guidance Notes

19. A firm may demonstrate that it has appropriate awareness measures in place to make *relevant employee*s 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 firm may be abused, in order to provide context for the application of *policies and procedures*.
- provides ready access to its *policies and procedures*.

20. A firm may demonstrate that it takes appropriate measures to make *relevant employee*s aware of enactments in Jersey relating to *money laundering* and the *financing of terrorism* where it:

- provides *relevant employee*s with a written explanation of the firm's and employee's obligations and potential criminal liability under the *money laundering* legislation, including the implications of failing to make an internal *SAR*.
- provides *relevant employee*s 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 it is practicable.
- requires such employees to acknowledge that they understand the firm's written explanations and procedures for making internal *SAR*s.
- 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 *Commission* 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.

21. A firm may demonstrate that it takes appropriate measures to make *relevant employee*s who are officers (e.g. directors or equivalent) aware of enactments in Jersey relating to *money laundering* and the *financing of terrorism*, where it also explains how officers may be held personally liable for an offence committed by the firm.

9.4.1 Monitoring and Testing Effectiveness

Guidance Notes

22. A firm 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 takes appropriate action where awareness is insufficient.
- statutory obligations, and takes appropriate action where awareness is insufficient.

9.4.2 Technological Developments

AML/CFT Code of Practice

23. Where a firm has identified a risk that may arise in relation to new services, business practices and technology, including where developed at group level or by outside developers (in Jersey and elsewhere), a firm must take steps to ensure that those involved in their development have a basic awareness of *money laundering* and the *financing of terrorism* and of current *money laundering* techniques, methods and trends.

Guidance Notes

24. A firm may demonstrate that developers have a basic awareness of *money laundering* and the *financing of terrorism* and of current *money laundering* 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 services, business practices and technology may be abused.

    › circulates any relevant material, e.g. material that is published by the *Commission* or *JFCU*, *FATF*, or *EU*.

    › circulates relevant media reports.

25. A firm may demonstrate that developers have a basic awareness of *money laundering* and the *financing of terrorism* and of current *money laundering* techniques, methods and trends where it obtains assurances that similar measures to those set out in paragraph 24 are taken by group or outside developers.

9.5 Training of Employees

Overview

26. The guiding principle for all anti-*money laundering* and the *financing of terrorism* 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 firm against the threat of *money laundering* and the *financing of terrorism*.

27. There is a tendency, in particular on the part of more junior employees, non-client facing employees, and support employees to mistakenly believe that the role that they play is less crucial than, or secondary to, that of more senior colleagues or customer facing colleagues. Such an attitude can lead to failures to report important information because of mistaken assumptions that the information will have already been identified and dealt with by other colleagues.

AML/CFT Codes of Practice

28. A firm must provide employees with adequate training at appropriate frequencies.

29. Such training must:

    › be tailored to the firm and 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* and the *financing of terrorism*; and

    › cover key aspects of legislation to prevent and detect *money laundering* and the *financing of terrorism*.

9.5.1 All Relevant Employees

Guidance Notes

30. A firm may demonstrate the provision of adequate training to *relevant employee*s where it addresses:

- the *money laundering* legislation, the *Money Laundering Order* and *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law*;
- vulnerabilities of products and services offered by the firm (based on the firm's business risk assessment), and subsequent *money laundering* and the *financing of terrorism* risk;
- *policies and procedures*, and employees' responsibilities;
- application of risk based *CDD policies and procedures*;
- recognition and examination of notable activity and transactions, such as activity outside of expected patterns, unusual settlements, abnormal payment or delivery instructions and changes in the patterns of business relationships;
- *money laundering* and the *financing of terrorism* developments, including techniques, methods, trends and typologies (having regard for reports published by the insular authorities, *FATF* and *FSRB*s); and
- 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 Senior management

Guidance Notes

31. A firm may demonstrate the provision of adequate training to senior management where (in addition to training for *relevant employee*s) it addresses:

- conducting and recording a business risk assessment;
- establishing a formal strategy to counter *money laundering* and the *financing of terrorism*;
- assessing the effectiveness of, and compliance with, *systems and controls* (including *policies and procedures*).

9.5.3 The MLCO

Guidance Notes

32. A firm may demonstrate the provision of adequate training to the *MLCO* where (in addition to training for *relevant employee*s) it addresses the monitoring and testing of compliance with *systems and controls* (including *policies and procedures*) to counter *money laundering* and the *financing of terrorism*.

9.5.4 The MLRO and Deputy MLROs

Guidance Notes

33. A firm may demonstrate the provision of adequate training to the *MLRO* (and, if applicable, *deputy MLRO*s) where (in addition to training for *relevant employee*s) it addresses:

- the handling and validation of internal *SAR*s;
- liaising with the *Commission*, *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 firm may demonstrate the provision of adequate training to employees who are not *relevant employee*s where it addresses:

    › the threat of *money laundering* and the *financing of terrorism*; and

    › procedures for making internal *SAR*s.

9.5.6 Timing and Frequency of Training

Guidance Notes

35. A firm 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 employee*s on the basis of risk, with more frequent training where appropriate.

9.5.7 Monitoring the Effectiveness of Screening, Awareness and of 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 this Handbook.

37. Such monitoring and testing should also be considered in the context of senior management's periodic check that *systems and controls* (including *policies and procedures*) are operating effectively, as set out at Section 2.4.1 of this Handbook.

10 RECORD KEEPING

Please Note:

- Regulatory requirements are set within this section as *AML/CFT Code of Practice*.
- This section contains references to Jersey legislation which may be accessed through the JFSC website.
- Where terms appear in the Glossary this is highlighted by the use of italic text. The Glossary is available from the JFSC website.

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 Codes of Practice* and provides guidance on keeping records. More general obligations on firms 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* and the *financing of terrorism* and confiscation of criminal property may not be possible. Likewise, if the funds used to finance terrorist activity cannot be traced back through the financial system, then the sources and the destination of terrorist financing will not be identified.

3. Record-keeping is also essential to facilitate effective supervision, allowing the *Commission* to supervise compliance by firms with statutory requirements and *AML/CFT* Codes *of Practice*. Records provide evidence of the work that a firm has undertaken to comply with statutory requirements and *AML/CFT* Codes *of Practice*. Records also provide a necessary context for the opinion that may be prepared on the truth and fairness of a firm's financial statements by its external *auditor*.

4. Records may be kept:
   - by way of original documents;
   - by way of photocopies 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 client's identity, a firm must keep a copy, or references to the evidence of the client's identity obtained during the application of *CDD* measures. In circumstances (such as where evidence is obtained at a client's home and photocopying facilities are not available) where it would not be possible to take a copy of the evidence of identity, a record will be made of the type of document and its number, date and place of issue, so that, if necessary, the document may be obtained from its source of issue.

6. In addition, a firm 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; and business correspondence and the results of any analysis undertaken.

Statutory Requirements

7. *Article 19(2) of the Money Laundering Order requires a relevant person to make and retain the following records:*

   › *copies of evidence of identity or information that enables a copy of such evidence to be obtained; and*

   › *all supporting documents, data and information in respect of a business relationship or one-off transaction which is the subject of client due diligence measures, including the results of analysis undertaken in relation to the business relationship or any transaction.*

8. *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.*

9. *Article A19 of the Money Laundering Order defines 'relevant person' for the purpose of the record retention requirements as including a person who was formerly a relevant person.*

10. *Article 20(1) and (2) of the Money Laundering Order requires 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 that is more than five years.*

Guidance Notes

12. A firm 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 with or for a client in the course of carrying on a *financial services business* must be recorded. Transactions records in support of such transactions, in whatever form they are used, e.g. credit/debit slips, cheques, will also be kept.

Statutory Requirements

14. *Article 19(2)(b) of the Money Laundering Order requires a financial services business 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 were completed.*

17. *Article 20(5) of the Money Laundering Order allows for the Commission to require a relevant person to keep records of transactions for a period that is more than five years.*

AML/CFT Codes of Practice

18. A record must be kept of the following for every transaction/activity carried out with or for a client in the course of a business relationship or one-off transaction:

- name and address of the client;
- if a monetary transaction, the kind of currency and the amount;
- if the transaction involves a client's account, the number, name or other identifier for the account;
- date of the transaction;
- details of the counterparty, including account details;
- nature of the transaction; and
- details of the transaction.

19. Client transaction records must provide a clear and complete transaction history of incoming and outgoing funds or assets.

Guidance Notes

20. A firm may demonstrate that it has kept details of a transaction where it records:

- valuation(s) and price(s);
- the form (e.g. cash, cheque, electronic transfer) in which funds are transferred;
- memoranda of instruction(s) and authority(ies);
- memoranda of purchase and sale; and
- custody of title documentation.

21. A firm may demonstrate that it has a clear and complete transaction history where it records all transactions undertaken on behalf of a client within that client's records.

10.4 Other Record Keeping Requirements

10.4.1 Corporate Governance

AML/CFT Codes of Practice

22. A firm must keep for a period of five years after the end of the calendar year in which it is superseded the business risk assessment that it must conduct and record under Section 2.3 of this Handbook.

23. A firm must keep for at least five years after the end of the calendar year in which they are superseded, adequate and orderly records of its *systems and controls* (including *policies and procedures*) that it must document under Section 2.3 of this Handbook that are maintained by a *financial services business* to prevent and detect money laundering and the *financing of terrorism*.

24. A firm must keep for a period of five years after the end of the calendar year in which a matter is considered, adequate and orderly records showing how 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 this Handbook, including reports presented by the *MLCO* on compliance matters and the *MLRO* on reporting.

25. A firm must keep for a period of five years after the end of the calendar year in which a matter is considered, 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 this Handbook.

26. A firm must keep for a period of five years after the end of the calendar year in which a person ceases to be a *MLCO* or *MLRO* (or *deputy MLRO*), adequate and orderly records to demonstrate that officer's experience and skills, independence, access to resources, and technical awareness, in line with Sections 2.5 and 2.6 of this Handbook.

27. A firm must keep for a period of five years after the end of the calendar year in which a measure is applied, adequate and orderly records to demonstrate that in line with Section 2.3 of this Handbook:

    › measures that are at least equivalent to *AML/CFT* Codes *of Practice* are applied to *financial services business* carried on by a firm through overseas branches; and

    › subsidiaries are required to apply measures that are at least equivalent to *AML/CFT* Codes *of Practice*.

10.4.2 Identification Measures

AML/CFT Codes of Practice

28. Where a firm is required to apply an identification measure through an *AML/CFT Code of Practice* set in Sections 4, 5 and 7 of this Handbook, an adequate and orderly record of that measure must be kept in line with record-keeping requirements in Part 4 of the *Money Laundering Order*.

29. A firm must keep for a period of five years after the end of the calendar year in which it is superseded, its risk assessment for each client that has still to be remediated in line with Section 4.7.3 of this Handbook.

10.4.3 On-going monitoring

AML/CFT Codes of Practice

30. A firm may demonstrate that it has kept details of the results of analysis undertaken in relation to the 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 firm's knowledge of the client (unusual transactions or activity);

    › Are complex or unusually large;

    › Form part of an unusual pattern; and

    › Present a higher risk of *money laundering* or the *financing of terrorism*,

    for a period of five years from the end of the calendar year in which the examination is undertaken.

31. A firm may demonstrate that it has kept details of the results of analysis undertaken in relation to the 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 connected

with 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 Codes of Practice

32. A firm must keep registers of internal and external *SAR*s, maintained in line with procedures required under Sections 8.3.1 and 8.3.2 of this Handbook.

33. In line with procedures required under Sections 8.3.1 and 8.3.2 of this Handbook, a firm must keep, 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, adequate and orderly records containing:

- a copy of the form used to make any internal *SAR* for that client and supporting documentation;
- enquiries made in relation to that internal *SAR* and 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*;
- relevant information passed to the *JFCU* after making the external *SAR.*

10.4.5 Screening, Awareness and Training of Employees

AML/CFT Codes of Practice

34. A firm must keep adequate and orderly records of training provided on the prevention and detection of *money laundering* and the *financing of terrorism* for five years after the end of the calendar year in which training was provided, including:

- the dates on which training was provided;
- the nature of the training provided;
- names of employees who received the training;
- 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 to and Retrieval of Records

Overview

35. The *Money Laundering Order* does not specify where records should be kept, but the overriding objective is for firms to be able to access and retrieve relevant information without undue delay.

AML/CFT Codes of Practice

36. A firm must keep documents, data or information obtained under *identification measures* in a way that facilitates on-going monitoring of each business relationship.

37. For all other purposes, the records kept by a firm must be readily accessible and retrievable by it. 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 Jersey or outside Jersey), or such longer period as agreed with the *Commission*. Other records must be accessible and retrievable within 10 working days (whether kept in Jersey or outside Jersey), or such longer period as agreed with the *Commission*.

38. A firm must periodically review the condition of paper and electronic records and consider the adequacy of its record-keeping arrangements.

39. A firm must periodically test procedures relating to access to, and retrieval of, its records.

40. Records must be maintained in a format that can be read. Where records are kept other than in legible form, they must be maintained so as to be readable at a computer terminal in Jersey - so that they may be produced in legible form.

10.5.1 External Record Keeping

Overview

41. Where records are kept by another person (group or otherwise) or kept outside Jersey, such as under outsourcing or storage arrangements, or where reliance is placed *obliged persons*, this will present additional factors for a *financial services business* to consider.

42. Whatever the particular circumstances, a firm remains responsible for compliance with all record-keeping requirements.

43. Where an *obliged person* ceases to trade or have a relationship with a client for whom it has provided an assurance to a firm, particular care needs to be taken to check that assurance continues to have effect, or that evidence of identity is obtained from the *obliged person*. Section 5 deals with placing reliance on *obliged person*s.

AML/CFT Codes of Practice

44. A firm must not: (i) allow another person (group or otherwise) to keep records; or (ii) keep records outside Jersey, where access and retrieval of records (by that person, the *Commission* and/or law enforcement) is likely to be impeded by confidentiality or data protection restrictions.

10.5.2 Reorganisation or Termination

Overview

45. Record-keeping requirements are unaffected where a firm 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 clients to another person.

AML/CFT Codes of Practice

46. A firm that undergoes mergers, continuance, take-overs, or internal reorganisations, must ensure that records remain readily accessible and retrievable for the required period, including when rationalising computer systems and storage arrangements.

47. Record-keeping arrangements must be agreed with the *Commission* where a firm terminates its activities, or transfers a block of clients to another person.

10.6 Disclosure of Records

Overview

48. The *FATF* Recommendations identify a number of cases where a financial institution or designated non-financial business or profession (e.g. accountancy firm) 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.

49. Accordingly, it is important that where the respondent institution or party relied on is a *relevant person* in Jersey, there should be no legal impediment to providing the data and information requested.

Statutory Requirements

50. *Article 16(3)(d) states that, where a relevant person (A) has given an assurance under Article 16 of the Money Laundering Order (or under a provision that applies outside Jersey that is equivalent to Article 16) to another relevant person (B), A must make available to B, at B's request, evidence of identity that A has obtained under Article 3 of the Money Laundering Order. A commits an offence under the Proceeds of Crime Law where it fails do so.*

51. *Article 17C(4) states that, where a relevant person (A) has given an assurance under Article 17C(2)(b) of the Money Laundering Order (or under a provision that applies outside Jersey that is equivalent to Article 17C) to another person (B), A may make available to B, at B's request, information and evidence of identity that A has obtained under Article 3 of the Money Laundering Order. However, A is not required by law to do so.*

52. *Article 19(7) 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.*