3 *IDENTIFICATION MEASURES* – OVERVIEW

3.1 Overview of section

1. This section explains the *identification measures* required under Article 13 of the *Money Laundering Order*, and the framework under which a *supervised person* is required to apply a risk-based approach to the application of such measures.

2. This section should be read and understood in conjunction with the following sections:

- Section 4 of *this Handbook* – which explains the basis for finding out identity and obtaining evidence of identity;
- Section 5 of *this Handbook* – which considers the circumstances in which reliance might be placed on another party to have applied *reliance identification measures*;
- Section 6 of *this Handbook* – which explains the ongoing requirements to monitor relationships on an ongoing basis;
- Section 7 of *this Handbook* – which explains the application of *enhanced CDD measures* (including the case of a *customer* that is assessed as presenting a higher risk); and
- Section 8 of *this Handbook* – which explains the application of simplified *identification measures*.

3. Sound *identification measures* are vital because they:

- help to protect the *supervised person* and the integrity of the financial sector in which it operates by reducing the likelihood of the business becoming a vehicle for, or a victim of, *financial crime*, including *money laundering,* the *financing of terrorism,* and the *financing of proliferation*;
- assist law enforcement, by providing available information on *customers* or activities and transactions being investigated;
- constitute an essential part of sound risk management, e.g., by providing the basis for identifying, limiting and controlling risk;
- help to guard against identity fraud.

4. The inadequacy or absence of *identification measures* can expose a *supervised person* to serious *customer* and counterparty risks, as well as reputational, operational, legal, regulatory and concentration risks, any of which can result in significant financial cost to the business. Documents, data, or information held also assist the *MLRO* (or *Deputy MLRO*) and other employees to determine whether a *SAR* is appropriate.

5. A *customer* may be an individual (or group of individuals) or legal person. Section 4.2.1 of *this Handbook* deals with a *customer* who is an individual (or group of individuals), Section 4.3 of *this Handbook* deals with a *customer* (an individual or legal person) who is acting for a legal arrangement, and Section 4.5 of *this Handbook* deals with a *customer* who is a legal person.

6. The term *customer*, as used in *this Handbook*, is defined in the Glossary of *this Handbook*. As noted in the definition, *customers* can include a prospective *customer* (i.e., applicants for business).

3.2 Obligation to apply *identification* measures

Statutory requirements (paraphrased wording)

7. *Article 13(1) of the Money Laundering Order requires a relevant person to apply CDD measures. CDD measures comprise identification measures and 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 customer and verifying the authority of any person purporting so to act. See Article 3(2)(aa) of the Money Laundering Order;*
- ***where the customer is a legal person**, understanding the ownership and control structure of that customer and the provisions under which the customer can enter into contracts, or other similarly legal binding arrangements, with third parties. See Article 3(2)(c)(ii) of the Money Laundering Order;*
- ***where the customer is a legal person**, finding out the identity of individuals who are the beneficial owners or controllers of the customer and obtaining evidence of the identity of those individuals. See Article 3(2)(c)(iii) of the Money Laundering Order;*
- *determining whether the customer is acting for a third party (or parties), whether directly or indirectly. See Article 3(2)(b) of the Money Laundering Order;*
- *finding out the identity of any **third party** (or parties) on whose behalf the customer is acting and obtaining evidence of the identity of those persons. See Article 3(2)(b)(i) of the Money Laundering Order;*
- ***where the third party is a legal person**, understanding the ownership and control of that third party, finding out the identity of the individuals who are the beneficial owners or controllers of the third party and obtaining evidence of the identity of those individuals. See Article 3(2)(b)(ii) of the Money Laundering Order;*
- ***where the third party is a legal arrangement**, e.g., a trust, understanding the nature of the legal arrangement under which the third party is constituted. See Article 3(2)(b)(iii)(A) of the Money Laundering Order;*

- ***where the third party is a legal arrangement**, e.g., a trust, finding out the identity of the persons who are listed in Article 3(7) of the Money Laundering Order. See Article 3(2)(b)(iii)(B) of the Money Laundering Order;*
- ***where the third party is a legal arrangement**, e.g., a trust, where any person listed in Article 3(7) is not an individual, finding out the identity of the individuals who are the beneficial owners or controllers of the person and obtaining evidence of the identity of those individuals. See Article 3(2)(b)(iii)(C) of the Money Laundering Order;*
- *obtaining information on the purpose and intended nature of the business relationship or one-off transaction. See Article 3(2)(d) of the Money Laundering Order.*

9. *Article 3(5) of the Money Laundering Order requires identification measures to include the assessment (i.e., CRA) 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) of the Money Laundering Order requires, in cases where a customer is acting for a third party, and where the customer is a legal person, measures for obtaining evidence of identity for third parties, persons purporting to act on behalf of the customer, and individuals who are the customer's beneficial owners or controllers, to involve reasonable measures having regard to all the circumstances of the case, including the degree of risk assessed.*

11. *For persons who are not individuals, Article 2 of the Money Laundering Order describes:*

- *beneficial owners as individuals with ultimate beneficial ownership of that person;*
- *beneficial controllers as individuals who ultimately control that person or otherwise exercise control over the management of that person.*

12. *The description of a beneficial owner or controller will apply whether the individual satisfies the description alone or jointly with other persons.*

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

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 customer, including the customer's business and risk profile. See Article 3(3)(a) of the Money Laundering Order;*
- *keeping documents, data, or information up to date and relevant by undertaking reviews of existing records, particularly in relation to higher risk categories of customers. See Article 3(3)(b) of the Money Laundering Order.*

Policies and procedures

15. *Among other things, Article 11(1) and (2) of the Money Laundering Order requires a relevant person to maintain policies and procedures for the application of CDD measures that are appropriate and consistent having regard to the degree of risk of money laundering and the financing of terrorism taking into account:*

- *the level of risk identified in a national or sector-specific risk assessment in relation to money laundering carried out in respect of Jersey;*

- *the type of customers, business relationships, products, and transactions with which the relevant person's business is concerned.*

16. *Among other things, Article 11(3) of the Money Laundering Order requires that the appropriate and consistent policies and procedures include policies and procedures which:*

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

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

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

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

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

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

3.3 Risk-based approach to *identification measures*

Overview

20. A risk-based approach to the application of *identification measures* involves several discrete stages. The overall objective is to assess the most effective and proportionate way to manage the *money laundering, terrorist financing, and proliferation financing risk* faced by a *supervised person*. While these stages are required to be incorporated into *policies and procedures*, they do not need to take place in the sequence outlined below. They may also occur simultaneously.

21. The risk assessment of a particular *customer* (i.e. the *CRA*) will determine:

- the extent of information which will be requested;
- what evidence of identity will be obtained;

- the extent to which the resulting relationship will be scrutinised; and
- how often documents, data or information held will be reviewed.

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

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

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

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

Stage	***Identification measures***	**Article(s) of the *MLO***	**Section in *the Handbook***
1.1	In the case of a *customer* that is a legal person, a *supervised person* must understand the *ownership and contro*l structure of the *customer* (and provisions under which the *customer* can enter into contracts).	3(2)(c)(ii)	Section 3.3.1
1.2	A *supervised person* must find out the identity of: › the *customer*; › any *Beneficial owners and controllers* of the *customer*; › any third party (or parties) – including a legal arrangement - on whose behalf the *customer* acts. Whether directly or indirectly (and *Beneficial owners and controllers* of the third party (or parties)); ○ For the avoidance of doubt, the above will include any person who is a named beneficiary of a life assurance policy entered into by the *customer*. Where there is no named beneficiary and they are designated by characteristics or by class or by other means, this means obtaining sufficient information about who the beneficiaries of a life policy are, sufficient to enable an assessment of risk of the *customer* relationship and to enable beneficiaries to be identified and verified at the time of the pay-out and › others listed in Article 3(2) of the *Money Laundering Order*.	3(2)(a) to (c) 3(4)(a)	Section 4

Stage	*Identification measures*	Article(s) of the *MLO*	Section in *the Handbook*
1.3	A *supervised person* must obtain information on the purpose and intended nature of the *business relationship* or *one-off transaction*. Also note additional *AML/CFT/CPF Codes of Practice* requirement to **understand** purpose and intended nature.	3(2)(d)	Sections 3.3.2 and 3.3.3 Section 7
1.4	A *supervised person* must obtain appropriate information for assessing the risk that a *business relationship* or *one-off transaction* will involve *money laundering*, the *financing of terrorism,* or the *financing of proliferation*. It may be necessary to repeat this stage following an assessment of risk under stage 2.1 below.	3(5) 15(1)	Sections 3.3.2 and 3.3.3 Section 7
2.1	A *supervised person* must, based on information collected at stage 1 above, assess the risk that a *business relationship* or *one-off transaction* will involve *money laundering*, *the financing of terrorism,* or the *financing of proliferation* (risk profile).	3(5)	Section 3.3.4
2.2	A *supervised person* must prepare and record a *customer* business and risk profile.	3(3)(a)	Section 3.3.5
3	A *supervised person* must obtain evidence of the identity of those whose identity is found out at stage 1.2 above.	3(2)(a) to (c) 3(4)(b) 15(1)	Section 4 Section 7

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

27. As shown in the table above, in some cases the *Money Laundering Order* requires *supervised person*s to simply obtain information. For example, finding out identity (Stage 1.2 above).

28. However, in other cases the *Money Laundering Order* requires *supervised person*s to also understand the information they obtain. For example, the ownership and control structure of the *customer* (Stage 1.1 above).

29. For each stage of the process, it is important for *supervised person*s to be aware of the distinction between factual information which they simply need to collect (name, address, date of birth, etc.) and that which requires further analysis (structure charts relating to ultimate *beneficial ownership*, publicly available adverse media, credit reports, etc.). This will assist in the identification and risk assessment process being carried out effectively.

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

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

AML/CFT/CPF Codes of Practice

[COP33] A *supervised person* must apply a risk-based approach to determine the extent and nature of the measures to be taken when undertaking the identification process set out above.

[COP34] A *supervised person* must understand the purpose and intended nature of a *business relationship* or *one-off transaction.*

[COP35] A *supervised person* must understand the nature and scope of the business activities generating a *customer*'s funds/assets.

Guidance notes

32. A *supervised person* may demonstrate that it understands the nature and scope of a *customer's* business activities where it collects and considers information regarding those activities. The volume of information collected and considered should be determined on a risk-based approach and may include, but is not limited to, the following:

- the industry sectors within which the business operates. The *supervised person* is not required to have an expert understanding of each industry sector, rather it should be sufficient to understand the potential risk exposure of the sector to *money laundering*, the *financing of terrorism*, or the *financing of proliferation*;
- whether the business activities display any higher risk indicators of *money laundering*, the *financing of terrorism*, or the *financing of proliferation*. These include, but are not limited to, the indicators listed at paragraph 77 below;
- whether the business is a state-owned enterprise or receives any government funding;
- the geographical scope of the business activities. For example, where the business operates and what it does in those countries;
- the reputation of the *customer's* business. For example, using a search engine to identify if any adverse media comment has been made on the conduct of the business and its *Beneficial owners and/or controllers*; and
- further clarification from the *customer* regarding any of the above, where necessary.

33. When undertaking the above activities, a *supervised person* should document their consideration (i.e., their thought process) and record their conclusions.

34. Where information is provided by someone other than the *customer* themselves, additional questions may need to be asked to assess whether it is reasonable to use this information, and consideration of the *AML/CFT/CPF* risk should be undertaken as part of the CRA.

3.3.1 Understanding ownership structure – Stage 1.1

Overview

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

36. Understanding ownership involves taking three separate steps:

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

Guidance notes

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

- it requests the *customer* to provide a statement of legal and *Beneficial ownership and control* as part of its application to become a *customer*. In the case of a legal person that is part of a group, this will include a group structure;
- to the extent that a *customer* is, or has been, provided with professional services by a *Lawyer* or *Accountant*, or is "administered" by a *TCSP*, it requests that *Lawyer*, *Accountant* or *TCSP* 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.

38. Where there is a reason to doubt the accuracy, or veracity of the statement or where higher risk factors are present, a *supervised person* who has been provided with a statement of legal and *Beneficial ownership and control* from a third party such as a Lawyer, Accountant or TCSP should not accept such document/information on face value but should consider whether it is reasonable to use this document/information and factor such consideration into any risk assessment undertaken.

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

- by the *customer*, e.g. recorded in its share register;
- by a *Lawyer*, *Accountant* or *TCSP*;
- by a trusted external party, in the case of a legal person with bearer shares, where bearer certificates have been lodged with that trusted external party;
- publicly, e.g., information that is held in a central register in the country of establishment.

40. A *supervised person* may demonstrate that it understands the ***Beneficial*** *ownership and control* structure of a *customer* that is a legal person where it considers information that is:

- held by the *customer*, e.g., in line with the *Company Law*, *AML/CFT/CPF* requirements, or listing rules, e.g., a declaration of trust in respect of shares held by a nominee shareholder;
- held by a *Lawyer, Accountant* or *TCSP*, e.g., in order to meet *AML/CFT/CPF* requirements;
- held in a public register, e.g., information that is held in a central register of *beneficial ownership* in the country of establishment, information that is published in financial statements prepared under generally accepted accounting principles, or information available as a result of a listing of securities on a stock exchange;
- provided directly by the ultimate *beneficial owner(s)* of the legal person;
- publicly available, e.g., in commercial databases and press reports.

41. **Step 3** – A *supervised person* may demonstrate that it understands the *ownership and control* structure of a *customer* that is a legal person where it applies one or more of the following *identification measures*:

- it considers the purpose and rationale for using an entity with a separate legal personality;
- in the case of a legal person that is part of a group, it considers whether the corporate structure makes economic sense, considering complexity and multi-jurisdictional aspects.

3.3.2 Information for assessing risk – Stage 1.4

Guidance notes

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

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

Additional relationship information	
Express trusts	› Type of trust (e.g., fixed interest, discretionary, testamentary). › Classes of beneficiaries, including any charitable causes named in the trust instrument.
Foundations	› Classes of beneficiaries, including any charitable objects.
Legal persons and legal arrangements (including *express trusts* and foundations)	› Ownership structure of any underlying legal persons. › Type of activities undertaken by any underlying legal persons (having regard for the *JFSC's* Sound Business Policy and trading activities). › Geographical sphere of activities and assets. › Name of regulator, if applicable.

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

3.3.2.1 Terms of business

Overview

44. It may be helpful to:

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

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

45. Whether or not to advise the *customer* of these issues is a decision to be taken by individual *supervised persons*. However, if it is to be done it is important that the policy should apply consistently for all *customers*. A decision only to do so once a suspicion has arisen could result in the *supervised person* committing a tipping-off offence (see Section 9.5 of *this Handbook*).

3.3.2.2 Issues that might be covered when drawing up a profile

Guidance notes

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

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

- carrying out background searches and database screening; and
- communicating with existing or previous providers of professional accountancy, banking, and legal services to the *customer*.

3.3.3 Source of funds – Stage 1.4

Overview

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

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

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

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

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

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

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

3.3.4 Assessment of risk – Stage 2.1

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

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

57. The sophistication of the risk assessment process may be determined according to factors supported by the *BRA*.

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

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

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

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

62. A *supervised person* may demonstrate that it has assessed the risk that a business relationship or one-off transaction will involve *money laundering*, the *financing of terrorism*, or *proliferation financing* where it takes into account the potential effect of the person or persons collating the *CDD* of the *customer* being a third party, e.g. they might be twice or even further removed from the *supervised person.*

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

- the business of some *supervised persons*, their products, and *customer* base, can be relatively simple, involving few products, with most *customers* falling into similar risk categories. In such circumstances a simple approach, building on the risk that the *supervised person's* products are assessed to present, may be appropriate for most *customers*, with the focus being on those *customers* who fall outside the norm;
- other *supervised persons* may have a greater volume of business, but large numbers of their *customers* may be predominantly "retail", served through delivery channels that offer the

possibility of adopting a standardised approach to many procedures. Here too, the approach for most *customers* may be relatively straight forward - building on product risk;

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

3.3.4.1 Factors to consider

64. **Country Risk** – A connection to a country, territory or area that presents a higher risk of *money laundering*, the *financing of terrorism*, or the *financing of proliferation*. The following types of countries, territories or areas may be considered to present a higher risk (non-exhaustive):

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

- when the *FATF* places jurisdictions under increased monitoring where they are identified as having strategic deficiencies. The list of jurisdictions under increased monitoring which **have committed** to addressing their issues is often informally referred to as *FATF's* "grey list". Jurisdictions which **do not** have an action plan are placed on a list of high-risk jurisdictions subject to a call for action. This is informally known as *FATF's* "black list";
- where a *customer* has a connection to a country on the *FATF's grey list* or *black list*, such as a portion of their *source of wealth* originating from that country, it is possible they may try to disguise or obscure that connection to avoid additional scrutiny. *Supervised persons* should be mindful of *customer*s whose *source of wealth* is routed through multiple intermediate layers, and seek to understand the ultimate geographic origin of the *source of wealth*;
- up-to-date versions of both the *FATF's* grey list and black lists are maintained on the *FATF* website.

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

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

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

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

› those that are vulnerable to corruption, e.g., those with poor ratings in Transparency International's Corruption Perception Index or highlighted as a concern in the Worldwide Governance Indicators project;

i) when considering the level of corruption risk in a country, it is important to consider the wider context of any issues affecting the country which may increase that risk. As

noted below, this may include there being an ineffective government, or political instability;

ii) the level of corruption risk may increase where the *customer* is a *PEP*. *Supervised persons* should therefore consider how much influence their *customer* deploys in that country and assess the risk that their *source of wealth* has been tainted by the proceeds of corruption;

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

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

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

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

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

67. **Product or service risk** – Features that may be attractive to money launderers or those financing terrorism or proliferation of weapons of mass destruction:

- ability to make payments to, or receive funds from, external parties;
- ability to pay in or withdraw cash;
- ability to migrate from one product or service to another;
- use of numbered accounts (without reference to the name of the *customer*);
- ability to use "hold mail" facilities and "care of" addresses which are not temporary arrangements;
- ability to place funds in client, pooled, nominee or other accounts, where funds are mingled with those of other persons;
- ability to place sealed parcels or sealed envelopes in safe custody boxes.

68. **Product or service risk** – Features that may indicate a higher risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*:

- work which is outside the *supervised person's* normal range of expertise – the *money launderer* might be targeting the *supervised person* to avoid answering too many potentially revealing questions.

69. Instructions that are unusual in themselves or that are unusual for the *supervised person,* or the *customer* may give rise to concern, particularly where no rational or logical explanation can be given. Additional service area vulnerabilities and risk factors specific to certain types of *supervised business* are set out in the sector-specific Sections 12 - 21 of *this Handbook*.

70. When assessing product or service risk, it is important not to restrict the assessment to the specific services being provided by the *supervised person* to the *customer*. For example, whilst the *supervised person* may only provide services regarding the portion of a *customer*'s wealth based in the *UK*, the *customer* themselves may also have diverse, volatile holdings in higher-risk jurisdictions and carry out activities considered to be more exposed to *money laundering*, *terrorist financing*, or *proliferation financing* risk. The wider context of the *customer's* activities should be considered.

71. In respect of the above paragraph, a *supervised person* is not required to obtain a granular list of every asset held by the *customer* globally. The information obtained should be sufficient for the *supervised person* to make an informed assessment of the risk presented by the *customer's* wider activities.

72. An additional section covering the issuance of **Prepaid Cards** and their associated risks is set out as section 14.2 of *this Handbook*.

73. **Delivery risk** – Features that may be attractive to *money launderers* or those *financing terrorism*:

- non-face to face relationships - product or service delivered exclusively by post, telephone, internet, video call etc. where there is no physical contact with the *customer*;

- indirect relationship with the *customer* - use of reliance on *obliged persons* or other third parties;
- availability of "straight-through processing" of *customer* transactions (where payments may be made electronically without the need for manual intervention by a *supervised person*).

74. ***Customer*-specific risk** – Features that may indicate whether a *customer* is a money launderer or is financing terrorism or financing proliferation:

- type of *customer*. An example would be an individual who meets any of the definitions of a *PEP*. This may (but not always) present a higher risk:
    i) a *supervised person* should be particularly aware of the enhanced corruption risk which may be posed by 'sovereign actors'. These individuals are *PEPs* who work for or are connected to national governments and have control over pooled national funds. A common example would be the senior executive of a State-owned body which pools funds from sources like central bank reserves and export revenue, such as a sovereign wealth fund;
    ii) engaging with a *customer* who holds a senior position in a State-owned body, or having a *business relationship* with the body itself, can pose an enhance risk of corruption. Examples of how the increased risk of corruption linked to these types of *PEPs* might crystallise include:
    iii) if the *PEP* siphons away money which legitimately belongs to the sovereign wealth fund via a trust and company structure, for their own personal gain; or
    iv) where the State-owned corporation itself is involved in illicit activity, as opposed to one or two 'bad actors' within the organisation. In this scenario, the corporation might utilise a structure to buy up key resources to deliberately manipulate their market price, for the benefit of the equally corrupt national government.
- nature and scope of business activities generating the funds/assets. The below examples may indicate higher risk:
    i) a *customer* conducting "sensitive" activities (as defined by the *JFSC*'s Sound Business Policy) or conducting activities which are prohibited if carried on with certain countries;
    ii) a *customer* engaged in higher risk trading activities (examples include, but are not limited to, trading in volatile currency pairs, assets linked to emerging market, cryptocurrencies and crypto assets);
    iii) a *customer* engaged in business activities which fall within the Table of the *JFSC*'s Sound Business Policy;
    iv) a *customer* engaged in a business which involves handling significant amounts of cash.
- transparency of *customer*. For example:
    i) persons that are subject to public disclosure rules, e.g., on exchanges or *regulated markets* (or majority-owned and consolidated subsidiaries of such persons), or subject to licensing by a statutory regulator, e.g. the Jersey Competition Regulatory Authority may indicate lower risk;
    ii) *customers* where the structure or nature of the entity or relationship makes it difficult to identify the true *Beneficial owners and controllers* may indicate higher

risk, for example those with nominee directors, nominee shareholders or which have issued bearer shares.

- behaviour by the *customer* may indicate a higher risk. For example:
    i) whilst face-to-face contact with *customers* is not always necessary or possible, an excessively obstructive or secretive *customer* may be a cause for concern;
    ii) where a *customer* requests undue levels of secrecy, a *customer* is reluctant or unwilling to provide adequate explanations or documents, or where it appears that an "audit trail" has been deliberately broken or unnecessarily layered;
    iii) where there is no commercial rationale or logical explanation for use of the products or services that are being sought;
- reputation of *customer*. For example, a well-known, reputable person, with a long history in their industry, and with abundant independent and reliable information about it and its *Beneficial owners and controllers* may indicate lower risk;
- jurisdiction of *customer*. If the *customer* is based outside Jersey, *supervised persons* will need to consider the rationale as to why the *customer* is seeking services outside of their home jurisdiction. The lack of an appropriate rationale may indicate higher risk;
- the regularity or duration of the *business relationship*. For example, longstanding *business relationships* involving frequent *customer* contact that result in a high level of understanding of the *customer* may indicate lower risk;
- type and complexity of relationship. The below examples may indicate higher risk:
    i) the use of overly complex or opaque structures with different layers of entities situated in two or more countries;
    ii) cross-border transactions involving counterparties in different parts of the world;
    iii) the unexplained use of corporate structures and *express trust*s;
    iv) the use of nominee and bearer shares;
- value of assets handled, e.g., higher value assets may indicate higher risk;
- value and frequency of cash or other "bearer" transactions (e.g., travellers' cheques and electronic money purses), e.g., a higher value and/or frequency may indicate higher risk;
- delegation of authority by the *customer*. For example, the use of powers of attorney, mixed boards and representative offices may indicate higher risk;
- involvement of persons other than *Beneficial owners and controllers* in the operation of a *business relationship* may indicate higher risk;
- in the case of an *express trust*, the nature of the relationship between the settlor(s) and beneficiaries with a vested interest, other beneficiaries and persons who are the object of a power. For example, a trust that is established for the benefit of the close family of the settlor may indicate a lower risk;
- in the case of a life assurance policy, the identity and risk profile of any named beneficiary to the policy.

3.3.4.2 External data sources

75. 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 of *this Handbook*. 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.

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

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

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

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

3.3.5 *Customer* business and risk profile – Stage 2.2

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

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

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

3.4 Identification measures – taking on a book of business

Overview

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

Guidance notes

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

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

84. When taking on *customer*s which display higher risk characteristics (e.g., connections to higher risk jurisdictions and/or a background in diverse and higher risk businesses), the *supervised person* should seek to understand the full complexity of the *customer's source of wealth*.

85. When assessing the risk level of a *customer* being taken on, it may also be necessary to consider the underlying assets held in the *customer's* portfolio and activities undertaken by any underlying entities, e.g., trading companies. Where underlying entities are present, it may be necessary for these to be subjected to screening.

86. It is not sufficient to simply transfer the business without considering the documents, data and information held for the *customer*. A judgement needs to be made, on a risk-based approach, as to whether the material provided is adequate, or if further enquiries are necessary.

87. In cases where:

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

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