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

   will face the loss of its reputation, risk the loss of its *licence*[1] or other regulatory sanctions (where regulated and supervised), damage the integrity of Jersey's finance industry as a whole, and may risk prosecution for criminal offences.

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

3. 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***").

4. Each *relevant person* in Jersey must recognise the role that it must 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.

5. The Jersey Financial Services Commission (the **"Commission"**) strongly believes that the key to the prevention and detection of *money laundering* and the *financing of terrorism* lies in the implementation of, and strict adherence to, effective *systems and controls*, including sound customer due diligence ("***CDD***") measures based on international standards. The *AML/CFT*[2] *Handbook* therefore establishes standards which match international standards issued by the Financial Action Task Force (the "***FATF***"). The *AML/CFT Handbook* also has regard to the standards promoted by the *Basel Committee* on Banking Supervision (the "***Basel Committee***"), International Organisation of Securities Commissions ("***IOSCO***") and the International Association of Insurance Supervisors (the "***IAIS***"). The *AML/CFT Handbook* takes account of the

[1] In this handbook "**licence**" is being used as a generic term to cover: a registration granted under the Banking Business (Jersey) Law 1991 (the "***BB(J) Law***"); a permit or certificate granted pursuant to the Collective Investment Funds (Jersey) Law 1988 (the "***CIF(J) Law***"); a registration granted under the Financial Services (Jersey) Law 1998 (the "***FS(J) Law***"); and a permit granted pursuant to the Insurance Business (Jersey) Law 1996 (the "**IB(J) Law**").

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

requirements of European Union (the "**EU**") legislation to counter *money laundering* and the *financing of terrorism* and its application of standards set by the *FATF*.

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

7. Throughout this *AML/CFT Handbook*, references to:

- **Customer** include, where appropriate, a prospective customer (an applicant for business). A customer is a person with whom a business relationship has been formed or one-off transaction conducted.
- ***Financing of terrorism*** means:
  - conduct which 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 (Jersey) Law 2002 (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 (Jersey) Law 1999 (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.

1.1 Objectives of the AML/CFT Handbook

8. The objectives of the *AML/CFT Handbook* are as follows:

- to outline the requirements of: the *Proceeds of Crime Law*; the *Terrorism Law*; the Money Laundering and Weapons Development (Directions) (Jersey) Law 2012 (the "***Directions Law***"); and the Sanctions and Asset-Freezing (Jersey) Law 2019 ; the Sanctions and Asset-Freezing (Implementation of External Sanctions) (Jersey) Order 2021 (the **"*Terrorist Sanctions Measures*"**);
- to outline the requirements of the Money Laundering Order which supplements the above legislation by placing more detailed requirements on *relevant persons*;
- to outline the requirements of the EU Legislation (Information Accompanying Transfers of Funds) (Jersey) Regulations 2017 (the "***Wire Transfers Regulations***") which introduce additional obligations for those remitting or receiving wire transfers;
- to set out the *Commission's* requirements - to be followed by all *relevant persons* that are regulated by the *Commission* under the *CIF(J) Law*, the *BB(J) Law*, the *IB(J) Law*, and the *FS(J) Law* (referred to as the "***regulatory laws***") and that hold a *Licence* ("**relevant persons carrying on regulated business**");

- to assist a *relevant person* to comply with the requirements of the legislation described above and the *Commission's* requirements through practical interpretation;
- to provide a base from which a *relevant person* 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 the *financing of terrorism*;
- to emphasise the responsibilities of the Board of a *relevant person* in preventing and detecting *money laundering* and the *financing of terrorism*;
- to promote the use of a proportionate, risk based approach to *CDD* measures, which directs resources towards higher risk customers;
- to provide more practical guidance on applying *CDD* measures, including finding out identity and obtaining evidence of identity;
- 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*.

9. The *AML/CFT 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.

10. The *AML/CFT Handbook* is intended for use by senior management and compliance staff in the development of a *relevant person's systems and controls*, and detailed *policies and procedures*. The *AML/CFT Handbook* is not intended to be used by a *relevant person* as an internal procedures manual.

1.2 Structure of the AML/CFT Handbook

11. Part 1 of the *AML/CFT Handbook* describes Statutory Requirements, sets out principles and detailed requirements (AML/CFT Code of Practice), and presents ways of complying with Statutory Requirements and the AML/CFT Code of Practice (Guidance Notes).

12. **Statutory Requirements** describe the statutory provisions that apply to 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.

13. 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 of 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].

[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 23 of the *Terrorism Law* have been complied with.

14. **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 *relevant person* 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 *relevant person* discretion as to how to apply requirements in the particular circumstances of its business, products, services, transactions and customers. The soundly reasoned application of the provisions contained within the Guidance Notes will provide a good indication that a *relevant person* is in compliance with the Statutory Requirements and *AML/CFT Codes of Practice*.

15. The provisions of the Statutory Requirements and of the *AML/CFT Codes of Practice* are described using the term **must**, indicating that these requirements are mandatory. However, in exceptional circumstances, where strict adherence to any of the *AML/CFT 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. Paragraph 46 also explains that an obligation to do something outside Jersey may be met through applying measures that are at least equivalent to *AML/CFT Codes of Practice*.

16. 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 the *AML/CFT Handbook* should be similarly construed.

17. The *AML/CFT Handbook* also contains Overview text which provides some background information relevant to particular sections or sub-sections of the *AML/CFT Handbook*.

18. The *AML/CFT 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 Statutory Requirements and *AML/CFT Codes of Practice*, and in applying the Guidance Notes, a *relevant person* 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.

19. The Statutory Requirements text necessarily paraphrases provisions contained in the *Proceeds of Crime Law*, *Terrorism Law*, *Directions Law*, *Terrorist Sanctions Measures*, *Wire Transfers Regulations* and *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.

20. Unless otherwise specified, references to sections in Part 1 of the *AML/CFT Handbook* are to sections contained within Part 1.

21. 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*. Part 3 of the *AML/CFT Handbook* sets out the *Commission's* policy for the supervision of compliance of a *relevant person carrying on regulated business* with the Statutory Requirements and *AML/CFT Codes of Practice* of Part 1. *Regulated business* is defined in Article 1 of the Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008 (the "***Supervisory Bodies Law***").

1.3 Legal Status and Sanctions for Non-compliance

1.3.1 AML/CFT Handbook

22. The *AML/CFT Handbook* is issued by the *Commission*:

    › pursuant to its powers under Article 8 of the Financial Services Commission (Jersey) Law 1998,

    › in accordance with 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 light of Article 37 of the *Proceeds of Crime Law* (which provides for the *Money Laundering Order* to prescribe measures to be taken).

23. The *AML/CFT Codes of Practice* in this *AML/CFT Handbook* cover *relevant persons carrying on regulated business*[4].

24. Separate handbooks have been published for *relevant persons* in the accountancy and legal sectors, and estate agents and high value dealers.

25. *Relevant persons* that are not carrying on *regulated business* or are not covered by other handbooks should refer to paragraph 27 to better understand the status of this *AML/CFT Handbook*.

1.3.2 Money Laundering Order

26. The *Money Laundering Order* is made by the Chief Minister under Article 37 of the *Proceeds of Crime Law*. The Order prescribes measures to be taken (including measures not to be taken) by persons who carry on a *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*.

27. 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 *relevant person* has complied with any of the requirements of the *Money Laundering Order*, the Royal Court is, pursuant to Article 37(8) of the *Proceeds of Crime Law*, required to take account of 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. 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 body corporate is proved to have been committed with the consent of, or to be attributable to any neglect on the part of, a director, manager or other similar officer, that individual, as well as the body corporate shall be guilty of the offence and subject to criminal sanctions.

28. 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 the *AML/CFT 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.

[4] Except an unclassified fund that is a *relevant person* but not hold a certificate under the *CIF(J) Law*.

1.3.3 AML/CFT Code of Practice

29. 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*, *Proceeds of Crime Law*, *Terrorism Law*, *Directions Law*, *Terrorist Sanctions Measures*, the *Wire Transfers Regulations*, and the *Money Laundering Order* 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*.

30. 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*.

31. 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.

32. 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; and
    - imposing a direction and making this public, including preventing an individual from working in a *relevant person*.

33. The ability of a *relevant person carrying on regulated business* to demonstrate compliance with *AML/CFT Codes of Practice* will also be directly relevant to its regulated status and any assessment of fitness and propriety of its principals. Non-compliance with any *AML/CFT Codes of Practice* may be regarded by the *Commission* as an indication of:

    - a lack of fitness and propriety under Articles 7 or 8B of the *CIF(J) Law*, Article 10 of the *BB(J) Law*, Article 7 of the *IB(J) Law*, and Article 9 of the *FS(J) Law*; and/or
    - a failure to follow certain fundamental principles within a Code of Practice issued under each of the *regulatory laws*.

34. In addition to the regulatory sanctions that are available under the *Supervisory Bodies Law*, consequences of non-compliance with the *regulatory laws* could also include imposing a *licence* condition, objecting to the appointment, or continued appointment, of a principal person (or equivalent controller or manager of the *relevant person*) or key person, revocation of a *licence* and appointment of a manager.

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 Financial Services Business Carried on in Jersey

35. 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* in or from within Jersey. This will include Jersey-based branches of companies incorporated outside Jersey conducting *financial services business* in Jersey.

36. 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 a *financial services business* in or from within Jersey. This will include Jersey-based branches of companies incorporated outside Jersey conducting *financial services business* in Jersey.

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

37. 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.

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

39. Article 10A(3) of the *Money Laundering Order* requires a person who: (i) is registered, incorporated or otherwise established under Jersey law[5], but who is not a legal person; and (ii) carries on a *financial services business* in or from within Jersey, to apply measures that are at least equivalent to the requirements of the *Money Laundering Order* in respect of any *financial services business* carried on by that person through an overseas branch. This requirement will apply to a limited partnership registered under the Limited Partnerships (Jersey) Law 1994 and general partnership established under Jersey customary law.

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

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

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

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

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

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

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

45. 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.

46. 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*.

47. By virtue of the *AML/CFT Codes of Practice* set in Section 2.7, a person who (i) is registered, incorporated or otherwise established under Jersey law[6], 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.

48. By virtue of the *AML/CFT Codes of Practice* set in Section 2.7, 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.

49. By virtue of the *AML/CFT Codes of Practice* set in Section 2.7, a person who (i) is registered, incorporated or otherwise established under Jersey law, but who is not a Jersey incorporated company; and (ii) carries on a *financial services business* in or from within Jersey, 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. This requirement will apply to a foundation or partnership established under Jersey law.

[6] 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.

50. 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 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 of Financial Services Business

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

52. Included in Part 4 is a document explaining the rationale for exempting certain activities from Schedule 2.

1.6 Risk Based Approach

53. To assist the overall objective to prevent *money laundering* and the *financing of terrorism*, the *AML/CFT Handbook* adopts a risk based approach. Such an approach:

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

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

55. 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.

1.7 Equivalence of Requirements in Other Countries and Territories

1.7.1 Equivalent Business

56. Articles 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 customer carrying on a *financial services business* that is overseen for *AML/CFT* compliance in Jersey or carrying on business that is "**equivalent business**". Sections dealing with the acquisition of a business or block of customers and verification of identity concession also provide concessions from *AML/CFT Codes of Practice* on a similar basis.

57. 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*;

- 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.

58. 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

59. 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.

60. 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

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

62. 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.

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

64. 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.
- 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.

2.1 Overview of Section

1. The Cadbury Report on corporate governance states that corporate governance is the system by which enterprises are directed and controlled. The Cadbury Report adds that the responsibilities of the Board include setting strategic aims, providing the leadership to put them into effect and supervising the management of the business. The Organisation for Economic Co-operation and Development builds on this definition by stating that the corporate governance structure specifies the distribution of rights and responsibilities among different participants, such as the Board, managers and other stakeholders, and spells out the rules and procedures for making decisions on corporate affairs.
2. Under the general heading of corporate governance, this section considers:
   - Board responsibilities for the prevention and detection of *money laundering* and *financing of terrorism*;
   - requirements for *systems and controls*, training and awareness; and
   - the appointment of a Money Laundering Compliance Officer (the "***MLCO***") and Money Laundering Reporting Officer (the "***MLRO***").
3. The *AML/CFT Handbook* describes a *relevant person's* general framework to combat *money laundering* and *financing of terrorism* as its **"*systems and controls*"**. The *AML/CFT Handbook* refers to the way in which those *systems and controls* are implemented into the day-to-day operation of a *relevant person* as its **"*policies and procedures*"**.
4. Where a *relevant person* is not a company, but is, for example, a partnership, references in this section to "the Board" should be read as meaning the senior management function of that person. In the case of a sole trader, the board will be the sole trader. In the case of an overseas company carrying on a *financial services business* in Jersey through a branch, "the Board" should be read as including the local management function of that branch in Jersey.

2.2 Measures to Prevent Money Laundering and Financing of Terrorism

Statutory Requirements

5. *In accordance with Article 37 of the Proceeds of Crime Law, a relevant person must take prescribed measures to prevent and detect money laundering and 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, he too shall be deemed to have committed a criminal offence.*
6. *Article 37 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 Board Responsibilities

Overview

7. The key responsibilities of the Board are set out in further detail below. The Board is assisted in fulfilling these responsibilities by a *MLCO* and *MLRO*. Larger or more complex *relevant persons* may also require dedicated risk and internal audit functions to assist in the assessment and management of *money laundering* and *financing of terrorism* risk.

Statutory Requirements

8. *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 financing of terrorism.*

9. *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).*

AML/CFT Codes of Practice

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

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

12. Taking into account the conclusions of the business risk assessment and strategy, the Board must: (i) organise and control its 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 *financing of terrorism* (see Section 2.4).

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

14. The Board must assess both the effectiveness of, and compliance with, *systems and controls* (including *policies and procedures*) and take prompt action necessary to address any deficiencies. (See Sections 2.4.1 and 2.4.2).

15. The Board must consider what barriers (including cultural barriers) exist to prevent the operation of effective *systems and controls* (including *policies and procedures*) to counter *money laundering* and *financing of terrorism*, and must take effective measures to address them. (See Section 2.4.3).

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

2.3.1 Business Risk Assessment

AML/CFT Codes of Practice

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

Guidance Notes

18. The Board of a *relevant person* may demonstrate that it has considered its exposure to *money laundering* and *financing of terrorism* risk by:

- Involving all members of the Board in determining the risks posed by *money laundering* and *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 *financing of terrorism*, e.g. outsourced aspects of regulated activities or compliance functions.
- Considering the nature, scale and complexity of its business, the diversity of its operations (including geographical diversity), the volume and size of its transactions, and the degree of risk associated with each area of its operation.
- Considering who its customers are and what they do.
- Considering whether any additional risks are posed by the countries and territories with which its customers are connected. Factors such as high levels of organised crime, increased vulnerabilities to corruption and inadequate frameworks to prevent and detect *money laundering* and *financing of terrorism* will impact the risk posed by relationships connected with such countries and territories.
- Considering the characteristics of the products and services that it offers and assessing the associated vulnerabilities posed by each product and service. For example:
  a. Products that allow a customer to "pool" third party funds will tend to be more vulnerable - because of the anonymity provided by the co-mingling of assets or funds belonging to several third parties by the customer.
  b. Products such as standard current accounts are more vulnerable because they allow payments to be made to and from external parties, including cash transactions.
  c. Conversely, those products that do not permit external party transfers or where redemption is permitted only to an account from which the investment is funded will be less vulnerable.
- Considering the risk that is involved in placing reliance on *obliged persons* to apply *reliance identification measures*.
- Considering how it establishes and delivers products and services to its customers. For example, risks are likely to be greater where relationships may be established remotely (non-face to face), or may be controlled remotely by the customer (straight-through processing of transactions).
- Considering the accumulation of risk for more complex customers.

19. In the case of a *relevant person* that is dynamic and growing, the Board 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 *relevant person* with stable products and services. In all cases, the Board 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 *financing of terrorism* risk.

2.4 Adequate and Effective Systems and Controls

Overview

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

Statutory Requirements

21. *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 financing of terrorism.*

22. *Parts 3, 3A, 4 and 5 of the Money Laundering Order set out the measures that are to be applied in respect of CDD, record-keeping and reporting.*

23. *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.*

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

25. *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 financing of terrorism. Article 11(10) of the Money Laundering Order requires a relevant person to provide relevant employees with training in the recognition and handling of transactions carried out by or on behalf of persons who are, or appear to be, engaged in money laundering or financing terrorism.*

26. *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.*

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

28. *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

29. A *relevant person* must establish and maintain appropriate and consistent *systems and controls* to prevent and detect *money laundering* and *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 ("***JFCU***") when it knows, suspects, or has reasonable grounds to know or suspect that another person is involved in *money laundering* or *financing of terrorism*, including attempted transactions - in line with Section 8.
- Adequately screen *relevant employees* when they are initially employed, make employees aware of certain matters and provide training - in line with Section 9.
- Keep complete records that may be accessed on a timely basis - in line with Section 10.
- 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.
- Monitor and review instances where exemptions are granted to *policies and procedures*, or where controls are overridden.

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

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

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

2.4.1 Effectiveness of Systems and Controls

Guidance Notes

32. A *relevant person* may demonstrate that it checks that *systems and controls* (including *policies and procedures*) are adequate and operating effectively where the Board periodically considers the efficacy (capacity to have the desired outcome) of those *systems and controls* (including *policies and procedures*, and those in place at branches and in respect of subsidiaries) in light of:

- Changes to its business activities or business risk assessment;

- Information published from time to time by the *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 *Proceeds of Crime Law*, *Terrorism Law*, *Directions Law*, *Terrorist Sanctions Measures*, 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.

33. A *relevant person* may demonstrate that it checks that *systems and controls* (including *policies and procedures*) are operating effectively where the Board periodically considers the effect of those *systems and controls* (including *policies and procedures*, and those in place at branches and in respect of subsidiaries) in light of the information that is available to it, including:

- Reports presented by the *MLCO* and others (e.g., where appropriate, risk management and internal audit functions) on compliance matters and *MLRO* on reporting.
- Reports summarising findings from supervisory and themed examinations and action taken or being taken to address recommendations.
- The number and percentage of customers that have been assessed by the *relevant person* 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 customers" that have still to be remediated under Section 4.7.2
- Details of failures by an *obliged person* or customer to provide information and evidence on demand and without delay under Articles 16, 16A and 17B-D of the *Money Laundering Order*, and action taken.
- The number of alerts generated by automated on-going monitoring systems.
- The number of internal *SARs* made to the *MLRO* (or *deputy MLRO*), the number of subsequent external *SARs* submitted to the *JFCU*, and timeliness of reporting (by business area if appropriate).
- Inquiries made by the *JFCU*, or production orders received, without issues having previously been identified by *CDD* or reporting *policies and procedures*, along with reasons.
- Results of testing of awareness of *relevant employees* with *policies and procedures* and legislation.
- The number and scope of exemptions granted to *policies and procedures*, including at branches and subsidiaries, along with reasons.

2.4.2 Testing of Compliance with Systems and Controls

Guidance Notes

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

35. A *relevant person* may demonstrate that it has tested compliance with *systems and controls* (including *policies and procedures*) where testing covers all of the *policies and procedures* maintained in line with Article 11(1) of the *Money Laundering Order* and paragraph 30 above, and in particular:

- The application of simplified and enhanced *CDD* measures.
- Reliance placed on *obliged persons* under Article 16 of the *Money Laundering Order*.
- Action taken in response to notices highlighting countries and territories in relation to which the *FATF* has called for the application of countermeasures or enhanced *CDD* measures.
- Action taken to comply with *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

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

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

Guidance Notes

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

- An unwillingness on the part of employees to subject high value (and therefore important) customers to effective *CDD* measures for commercial reasons.
- Pressure applied by management or customer relationship managers outside Jersey upon employees in Jersey to transact without first conducting all relevant *CDD*.
- Undue influence exerted by relatively large customers in order to circumvent *CDD* measures.
- Excessive pressure applied on employees to meet aggressive revenue-based targets, or where employee or management remuneration or bonus schemes are exclusively linked to revenue-based targets.
- An excessive desire on the part of employees to provide a confidential and efficient customer service.
- Design of the customer risk classification system in a way that avoids rating any customer as presenting a higher risk.
- The inability of employees to understand the commercial rationale for business relationships, resulting in a failure to identify non-commercial and therefore potential *money laundering* and *financing of terrorism* activity.

- Negative handling by managerial staff of queries raised by more junior employees regarding unusual, complex or higher risk activity and transactions.
- An assumption on the part of more junior employees that their concerns or suspicions are of no consequence.
- A tendency for line managers to discourage employees from raising concerns due to lack of time and/or resources, preventing any such concerns from being addressed satisfactorily.
- Dismissal of information concerning allegations of criminal activities on the grounds that the customer has not been successfully prosecuted or lack of public information to verify the veracity of allegations.
- The familiarity of employees with certain customers resulting in unusual or higher risk activity and transactions within such relationships not being identified as such.
- Little weight or significance is attributed to the role of the *MLCO* or *MLRO*, and little cooperation between these post-holders and customer-facing employees.
- Actual practices applied by employees do not align with *policies and procedures*.
- Employee feedback on problems encountered applying *policies and procedures* are ignored.
- Non-attendance of senior employees 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

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

40. Depending on the nature and size of a *relevant person*, the roles of *MLCO* and *MLRO* may require additional support and resourcing. Where a *relevant person* elects to bring in additional support, or to delegate areas of the *MLCO* or *MLRO* functions to external parties, the *MLCO* or *MLRO* will remain directly responsible for *his* respective role.

AML/CFT Codes of Practice

41. A *relevant person* must follow the *Commission's* policy statement and guidance notes on outsourcing, as may be amended from time to time.

42. A *relevant person* must consider the effect that outsourcing has on *money laundering* and *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.

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

44. Where an outsourced activity is a *financial services business* activity, then a *relevant person* must be satisfied with the *policies and procedures* that are put in place by the provider of the outsourced service.

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

2.5 The Money Laundering Compliance Officer (MLCO)

Overview

46. The *Money Laundering Order* requires a *relevant person* 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 *financing of terrorism* and *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law*.

47. The *Money Laundering Order* also requires a *relevant person* 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 *relevant person* shall have regard to the risk of *money laundering* and *financing of terrorism* and matters that have an impact on risk, such as size and structure of the *relevant person's* business.

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

49. 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

50. *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 financing of terrorism and AML/CFT Codes of Practice are being complied with. The same person may be appointed as both MLCO and MLRO.*

51. *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.*

52. *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 appointed 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.*

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

AML/CFT Codes of Practice

54. A *relevant person* must appoint a *MLCO* that:

- is employed by the *relevant person* or enterprise in the same financial group as the *relevant person*[1];
- is based in Jersey[2]; and
- has sufficient experience and skills.

55. A *relevant person* must ensure that the *MLCO*:

- has appropriate independence, in particular from customer-facing, business development and system and control development roles;
- reports regularly and directly to the Board and has a sufficient level of authority within the *relevant person* so that the Board reacts to and acts upon reports made by the *MLCO*;
- has sufficient resources, including sufficient time and (if appropriate) a deputy *MLCO* and compliance support staff; and
- is fully aware of both *his* and the *relevant person's* obligations under the *Proceeds of Crime Law*, *Terrorism Law*, *Directions Law*, *Terrorist Sanctions Measures*, the *Money Laundering Order* and *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law*.

56. 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 *relevant person* must take action to appoint a member of the Board (or other appropriate member of senior management) to the position on a temporary basis.

57. Where temporary circumstances arise where the *relevant person* has a limited or inexperienced compliance resource, it must ensure that this resource is supported as necessary.

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

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

Guidance Notes

59. A *relevant person* 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:

---

1 In the case of a *relevant person* that: carries on the business of being a functionary, recognized fund, or unclassified fund or is a Category B insurance permit holder, a managed bank, or other managed entity; has no employees of its own; and is administered by a person carrying on a *financial services business* that is a *regulated person*, it is acceptable for an employee of the administrator to be appointed by the *relevant person* as its *MLCO*.

2 In the case of a *relevant person* that is a Category A insurance business permit holder with no employees of its own in Jersey, it is acceptable to appoint an employee outside Jersey. In the case of a *relevant person* that is carrying on a money service business and has no employees of its own in Jersey, it is acceptable for the *relevant person* to appoint an employee outside Jersey as its *MLCO*, provided the employee is based in an equivalent jurisdiction.

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

60. In a case where the *MLCO* is also **responsible** for the development of *systems and controls* (including *policies and procedures*) in line with evolving requirements, a *relevant person* may demonstrate that the *MLCO* has appropriate independence where such *systems and controls* are subject to periodic independent scrutiny.

2.6 The Money Laundering Reporting Officer (MLRO)

Overview

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

Statutory Requirements

62. *Article 8 of the Money Laundering Order requires a relevant person to appoint a MLRO. The MLRO's function is to receive and consider internal SARs in accordance with internal reporting procedures. The same person may be appointed as both MLCO and MLRO.*

63. *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.*

64. *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.*

65. *Article 8 of the Money Laundering Order recognises that a relevant person that is also a regulated person may have notified the Commission of the appointment or cessation of a MLRO under other legislation. If so, a duplicate notification is not required under the Money Laundering Order.*

66. *Article 9 allows a relevant person to designate one or more deputy MLROs, in addition to the MLRO, to whom internal SARs may be made.*

AML/CFT Codes of Practice

67. A *relevant person* must appoint a *MLRO* that:

- is employed by the *relevant person* or enterprise in the same financial group as the *relevant person*[3];
- is based in Jersey[4]; and
- has sufficient experience and skills;

68. A *relevant person* must ensure that the *MLRO*:

- has appropriate independence, in particular from customer-facing and business development roles;
- has a sufficient level of authority within the *relevant person*;
- has sufficient resources, including sufficient time, and (if appropriate) is supported by *deputy MLROs*;
- is able to raise issues directly with the Board; and
- is fully aware of both *his* and the *relevant person's* obligations under the *Proceeds of Crime Law*, *Terrorism Law*, *Directions Law*, *Terrorist Sanctions Measures*, the *Money Laundering Order* and *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law*.

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

70. Where a *relevant person* has appointed one or more *deputy MLROs*, it must provide that the *MLRO*:

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

71. 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 *relevant person* must take action to appoint a member of the Board (or other appropriate member of senior management) to the position on a temporary basis.

72. Where temporary circumstances arise where the *relevant person* has a limited or inexperienced reporting resource, the *relevant person* must ensure that this resource is supported as necessary.

Guidance Notes

73. A *relevant person* may demonstrate that its *MLRO* (and any *deputy MLRO*) is receiving and considering *SARs* in accordance with Article 21 of the *Money Laundering Order* where, inter alia, its *MLRO*:

---

[3] In the case of a *relevant person* that: carries on the business of being a functionary, recognized fund, or unclassified fund, or is a Category B insurance permit holder, a managed bank, or other managed entity; has no employees of its own; and is administered by a person carrying on *financial services business* that is a *regulated person*, it is acceptable for an employee of the administrator to be appointed by the *relevant person* as its *MLRO*.

[4] In the case of a *relevant person* that is a Category A insurance business permit holder with no employees of its own in Jersey, it is acceptable to appoint an employee outside Jersey In the case of a *relevant person* that is carrying on a money service business and has no employees of its own in Jersey, it is acceptable for the *relevant person* to appoint an employee outside Jersey as its *MLRO*, provided the employee is based in an equivalent jurisdiction.

- maintains a record of all requests for information from law enforcement authorities and records relating to all internal and external *SARs* (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 *financing of terrorism*.

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

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

2.7 Financial Groups

Overview

75. A Financial Group of which a relevant person 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

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

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

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

78. *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

79. 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.

80. A person who:

- is 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.

81. A person who:

- is 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 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 person.

82. Where overseas legislation prohibits compliance with an AML/CFT Code (or measures that are at least equivalent) then the AML/CFT Codes do not apply and the *Commission* must be informed that this is the case. In such circumstances, a *relevant person* must take other reasonable steps to effectively deal with the risk of *money laundering* and *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 through 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 *relevant person* is required to apply a risk based approach to the application of such measures.
2. This section should be read and understood in conjunction with the following sections:
   - Section 4 – which explains the basis for finding out identity and obtaining evidence of identity;
   - Section 5 – which considers the circumstances in which reliance might be placed on another party to have applied *identification measures*; and
   - Section 7 - which explains the application of enhanced *CDD* measures (including the case of a customer that is assessed as presenting a higher risk) and simplified *identification measures*.
3. Sound *identification measures* are vital because they:
   - help to protect the *relevant 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;
   - 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; and
   - help to guard against identity fraud.
4. The inadequacy or absence of *identification measures* can subject a *relevant 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 business employees to determine whether a *SAR* is appropriate.
5. A customer may be an individual (or group of individuals) or legal person. Section 4.3 deals with a customer who is an individual (or group of individuals), Section 4.4 deals with a customer (an individual or legal person) who is acting for a legal arrangement, and Section 4.5 deals with a customer who is a legal person.
6. Throughout this section, references to "customer" include, where appropriate, a prospective customer (an applicant for business). A customer 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 on-going monitoring. Identification measures must be applied:*

   › *Subject to Article 13(4) to (11) of the Money Laundering Order, before the establishment of a business relationship or before carrying out a one-off transaction.*

   › *Where a relevant person suspects money laundering.*

   › *Where a relevant person has doubts about the veracity of documents, data or information previously obtained under CDD measures.*

Identification Measures

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

   › *Finding out the identity of a customer and obtaining evidence of identity from a reliable and independent source that is reasonably capable of verifying that the person to be identified is who the person is said to be and satisfies the person responsible for the identification of a person that the evidence does establish that fact (referred to as "**obtaining evidence**"). See Article 3(2)(a) of the Money Laundering Order.*

   › *Finding out the identity of any person purporting to act on behalf of the customer and verifying the authority of any person purporting so to act. See Article 3(2)(aa) of the Money Laundering Order.*

   › *Where the customer is a legal person, understanding the ownership and control structure of that customer and the provisions under which the customer can enter into contracts, or other similarly legal binding arrangements, with third parties. See Article 3(2)(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 by a relevant person of the risk that a business relationship or one-off transaction will involve money laundering. This must include obtaining appropriate information for assessing that risk.*

10. *Article 3(6) requires, in cases where a customer is acting for a third party, and where the customer is a legal person, measures for obtaining evidence of identity for third parties, persons purporting to act on behalf of the customer, and individuals who are the customer's beneficial owners or controllers to involve reasonable measures having regard to all the circumstances of the case, including the degree of risk assessed.*

11. *For persons who are not individuals, Article 2 of the Money Laundering Order describes:*
    - *beneficial owners as individuals with ultimate beneficial ownership of that person; 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*

On-going Monitoring

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

Policies and Procedures

15. *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 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 customers, 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.*
- *Which 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.*
- *Which assess and manage the risk of money laundering or financing of terrorism occurring as a result of completing identification measures after the establishment of a business relationship (where permitted), and ensure period 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 *financing of terrorism* risk faced by a *relevant person*. While these stages must be incorporated into *policies and procedures*, they do not need to take place in the sequence outlined below, and may occur simultaneously.

20. The risk assessment of a particular customer 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 the *AML/CFT Handbook* requires the Board of a *relevant person* 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 *financing of terrorism* risk. This business risk assessment will enable a *relevant 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 *relevant person* to consider whether the specific circumstances of the customer will necessitate the application of further measures.

22. Part 3A of the *Money Laundering Order* sets out exemptions from customer 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 relevant person who is exempt from applying third party identification requirements (See Article 17D).

23. The following are stages in the identification process:

Stage	Identification Measure	Article(s)	Guidance
1.1	In the case of a customer that is a legal person, a *relevant person* must understand the ownership and control structure of the customer (and provisions under which the customer can enter into contracts).	3(2)(c)(ii)	Section 3.3.1
1.2	A *relevant person* must find out the identity of: • the customer; • any beneficial owners and controllers of the customer; • any third party (or parties)[1] – 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)); and • others listed in Article 3(2).	3(2)(a) to (c) 3(4)(a)	Section 4
1.3	A *relevant person* must obtain information on the purpose and intended nature of the business relationship or one-off transaction.	3(2)(d)	
1.4	A *relevant person* must obtain appropriate information for assessing the risk that a business relationship or one-off transaction will involve *money laundering* or *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 *relevant person* must, on the basis of information collected at stage 1, assess the risk that a business relationship or one-off transaction will involve *money laundering* or *financing of terrorism* risk (risk profile).	3(5)	Section 3.3.4
2.2	A *relevant person* must prepare and record a customer business and risk profile.	3(3)(a)	Section 3.3.5
3	A *relevant person* must obtain evidence of the identity of those whose identity is found out at stage 1.2.	3(2)(a) to (c) 3(4)(b) 15(1)	Section 4 Section 7

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

[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 customer.

25. *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 *relevant person* and on customers with the risk that the business may be used in *money laundering* or to finance terrorism by focusing resources on higher risk areas.

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

AML/CFT Codes of Practice

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

3.3.1 Understanding Ownership Structure – Stage 1.1

Overview

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

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

Guidance Notes

Step 1

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

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

Step 2

31. A *relevant person* may demonstrate that it understands the legal ownership and control structure of a customer that is a legal person where it takes into account information that is held: (i) by the customer, 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.

32. A *relevant person* may demonstrate that it understands the beneficial ownership and control structure of a customer that is a legal person where it takes into account information that is:

- Held by the customer, e.g. in line with company law, *AML/CFT* 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

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

3.3.2 Information for Assessing Risk – Stage 1.4

Guidance Notes

34. A *relevant 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* or *financing of terrorism* risk where it collects the following information:

All Customer Types	
All customer 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 *relevant person*.

Additional Relationship Information: legal arrangements and legal persons	
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.

[2] https://www.jerseyfsc.org/media/1901/ps-sound-business-practice-policy-august-2018.pdf

Additional Relationship Information: legal arrangements and legal persons	
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.

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

3.3.3 Source of Funds – Stage 1.4

Overview

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

37. The "***source of funds***" is the activity which generates the funds for a customer, e.g. a customer's occupation or business activities. Information concerning the geographical sphere of the activities may also be relevant.

38. The *Money Laundering Order* and the *AML/CFT Handbook* stipulate record-keeping requirements for transaction records, which 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 is not to be confused with *source of funds*.

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

40. In finding out a *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

41. The following factors - country risk, product (or service) risk, delivery risk, and customer specific risk - will be relevant when assessing and evaluating the information collected at Stage 1, and are not intended to be exhaustive. A *relevant 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.

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

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

44. 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

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

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

47. A *relevant person* may demonstrate that it has assessed the risk that a business relationship or one-off transaction will involve *money laundering* or *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 customer 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.

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

    › The business of some *relevant person*s, 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 business' products are assessed to present, may be appropriate for most customers, with the focus being on those customers who fall outside the norm.

    › Others may have a greater level 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

Country Risk

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

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

50. Relevant connection to a country or territory that presents a lower risk of *money laundering* or *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**.

51. Familiarity of a *relevant person* with a country or territory, including knowledge of its local legislation, regulations and rules, as well as the structure and extent of regulatory oversight, for example, as a result of a *relevant person*'s own or group operations within that country or territory.

Product or Service Risk

52. Features that may be attractive to money launderers or those financing terrorism:
- Ability to make payments to external parties.
- Ability to pay in or withdraw cash.
- Ability to migrate from one product to another.
- Use of numbered accounts (without reference to the name of the customer).
- Ability 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 boxes.

Delivery Risk

53. 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 etc. where there is no physical contact with the customer.
- Availability of "straight-through processing" of customer transactions (where payments may be made electronically without the need for manual intervention by a *relevant person*).

Customer Specific Risk

54. Features that may indicate whether a customer is a money launderer or is financing terrorism:

- Type of customer. 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.
- Nature and scope of business activities generating the funds/assets. For example, a customer 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 customer engaged in higher risk trading activities; or a customer engaged in a business which involves handling significant amounts of cash, may indicate higher risk.
- Transparency of customer. For example, persons that are subject to public disclosure rules, e.g. on exchanges or regulated markets (or consolidated subsidiaries of such persons), or subject to licensing by a statutory regulator, e.g. the Channel Islands Competition & Regulatory Authorities, may indicate lower risk. Customers where the structure or nature of the entity or relationship makes it difficult to identify the true beneficial owners and controllers may indicate higher risk e.g. those with nominee directors or nominee shareholders or which have issued bearer shares.
- Reputation of customer. 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 customer. For example, where there is no commercial rationale for a customer using the products or services that he seeks or setting up a particular structure, 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, this may indicate higher risk.
- The regularity or duration of the relationship. For example, longstanding relationships involving frequent customer contact that result in a high level of understanding of the customer 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, and the use of nominee and bearer shares may indicate higher risk.
- Value of assets handled, 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 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.
- 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.
- 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.

3.3.4.2 External Data Sources

Overview

55. 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.

56. Information on the proliferation of nuclear and other weapons, and sanctions may be found on the *Commission*'s website.

57. Appendix D2 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 customer, 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 more, or four or more, separate external sources, it is more prominently highlighted in the appendix.

58. 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.

59. External data sources may also assist in establishing customer specific risk. For example, electronic subscription databases list individuals entrusted with prominent public functions.

3.3.5 Customer Business Profile – Stage 2.2

Guidance Notes

60. A *relevant person* may demonstrate that it has prepared a customer business profile where it enables it to:

    › Identify a pattern of expected transactions and activity within each business relationship; and

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

61. For certain types of products or services, a *relevant person* may demonstrate that it has prepared a customer business profile where it does so on the basis of generic attributes, so long as this enables it to recognise the transactions and activity referred to in paragraph 60 above. For more complex products or services, however, tailored profiles will be necessary.

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

Overview

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

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

Guidance Notes

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

65. A *relevant person* may demonstrate that documents, data and information obtained under *identification measures* are kept up to date and relevant under Article 3(3)(b) of the *Money Laundering Order* where they are reviewed on a risk sensitive basis, including where additional "factors to consider" become apparent.

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

3.5 Identification Measures – taking on a book of business

Overview

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

Guidance Notes

68. A *relevant 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 *relevant person* or carries on *equivalent business* as defined by Article 5 of the *Money Laundering Order* (refer to Section 1.7);
    - The *relevant 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; and

- Before, or at the time of the transfer, the *relevant person* obtains from the vendor all of the relevant documents, data or information (or copy thereof) held for each customer acquired.

69. In a case where the vendor is not a *relevant person*, or is not carrying on *equivalent business* (refer to Section 1.7), or where deficiencies in the vendor's *CDD policies and procedures* are identified (either at the time of transfer or subsequently), a *relevant 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 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 through 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 the *AML/CFT Handbook* is to explain what information on identity is to be found out when establishing a business relationship or carrying out a one-off transaction (or otherwise under Article 13 of the *Money Laundering Order*), and what evidence is to be obtained that is reasonably capable of verifying that the person to be identified is who the person is said to be and satisfies a *relevant person* 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 *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 customer that is assessed as presenting a higher risk of *money laundering* or *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 *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 customers".

5. Inter alia, the requirement to find out identity and obtain evidence will apply when there is a:

   - change in information found out for a customer, e.g. following marriage or change of nationality;
   - change in beneficial ownership and control of a customer; or
   - change in a third party (or parties) (or beneficial ownership or control of a third party (or parties) on whose behalf a customer acts.

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

7. Throughout this section, references to "customer" include, where appropriate, a prospective customer (an applicant for business). A customer 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 customer is the person that he, she, or it claims to be is a combination of being satisfied that:

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

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

9. Evidence of identity can take a number of forms. In respect of individuals, 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 customer's identity by obtaining other forms of confirmation, including independent data sources, E-ID and, in appropriate circumstances, written assurances from *obliged person*s.

10. When obtaining evidence of identity, a *relevant person* 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 customer who is a legal person.*

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

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

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

   › *In the case of a trust, the settlor.*

   › *In the case of a trust, the protector.*

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

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

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

4.3 Obligation to Find Out Identity and Obtain Evidence: Individuals

Overview

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

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

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

4.3.1 Finding out Identity

Guidance Notes

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

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

19. However, in the case of a lower risk relationship, a *relevant person* may demonstrate that it has found out the identity of an individual who is a customer under Article 3(2)(a) of the *Money Laundering Order* where it collects 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 (see Section 4.3.2)
- 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 *relevant person* should also 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 relevant person will need to ensure that its CDD systems and controls include measures specifically designed to do so.

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

23. Where a *relevant person* is not familiar with the form of the evidence obtained, 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 business), and must be translated into English at the request of the *JFCU* or the *Commission*.

Guidance Notes

26. A *relevant person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that an individual to be identified is who 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;
- Passport or national identity number; and
- Sex.

27. However, in the case of a lower risk relationship, a *relevant person* may demonstrate that it has obtained evidence that is reasonably capable of verifying under Article 3(2)(a) of the *Money Laundering Order* that an individual to be identified is who 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 *relevant person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that an individual to be identified is who 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.

All elements of Identity
› A current national identity card or copy of such a national identity card certified by a suitable certifier - providing photographic evidence of identity. › A current driving licence or copy of such a driving licence certified by a suitable certifier - providing photographic evidence of identity - where the licensing authority carries out a check on the holder's identity before issuing.
Residential Address
› Correspondence from a central or local government department or agency (e.g. States and parish authorities). › A letter of introduction confirming residential address from: (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. › A tenancy contract or agreement.

29. However, in the case of a lower risk relationship with a customer who is resident in Jersey, a *relevant person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that an individual to be identified is who 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 *relevant person* may also demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that an individual to be identified is who 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 *relevant person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that an individual to be identified is who 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 *relevant person* may demonstrate that a country or territory is well-regulated for the purpose of a letter of introduction, where it has regard to:

    › the development and standing of the country or territory's regulatory framework; and

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

4.3.3 Suitable Certification

Overview

33. "Suitable certification" is a process where, rather than requesting a person to present evidence of identity directly to a *relevant person*, 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 *relevant person*. The effect of this is to create an environment in which *identification measures* are applied through a trusted external party and where the customer (or other person) is seen on a face to face basis.

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

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

36. 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.

37. 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.

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

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

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

40. 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

41. A *relevant person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a person to be identified is who 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 42 and adequate information set out in paragraph 44 so that he may be contacted in the event of a query; and

    › takes additional steps in line with paragraph 45 to validate the credentials of the suitable certifier, where that person is connected to a higher risk country or territory, 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 36 and 37).

42. 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.

43. In a case where the document to be certified relates to a legal arrangement or legal person, then paragraphs 41 and 42 of this section apply, except that the documents to be certified will be those that provide evidence of identity of that arrangement or person.

44. 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.

45. 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 *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.

4.3.4 Obtaining Evidence of Identity - Independent Data Sources

Overview

46. Independent data sources can provide a wide range of confirmatory material on a customer, 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.

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

Guidance Notes

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

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

49. A *relevant person* 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 *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 customer 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 *relevant person* to capture and record the data or information.

4.3.5 Guarding Against the Financial Exclusion of Jersey Residents

Overview

50. 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

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

Guidance Notes

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

53. 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 financial services and products, a *relevant person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a person to be identified is who 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 *relevant person* is satisfied that it can place reliance on, confirming the identity of the resident.

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

- A letter from a Jersey employer, which a *relevant person* is satisfied that it can place reliance on, that confirms residence of an individual at a stated Jersey address, and, in the case of a seasonal worker, indicates the expected duration of employment and gives the worker's principal residential address in *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 customer 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 *relevant person* is satisfied that it can place reliance on, that confirms residence of the individual at a stated address. In the case of a Jersey student studying outside the Island, a residential address in Jersey should also be collected.

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

4.3.6 Residential Address: Overseas Residents

Overview

56. On occasions, an individual that resides abroad may be unable to provide evidence of *his* principal residential address using the sources set out at Section 4.3.2. 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 a private address may not be obtained through a personal visit.

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

AML/CFT Codes of Practice

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

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

Guidance Notes

60. Where an individual has a valid reason for being unable to produce more usual evidence for a residential address, a *relevant person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a person to be identified is who 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.

61. Where an individual has a valid reason for being unable to produce more usual evidence for a residential address, a *relevant person* may demonstrate that it has found out the identity of that person under Article 3(2)(a) of the *Money Laundering Order* where, in addition to principal residential address, it collects a "locator" address. In such a case, a *relevant person* 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.

62. 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

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

64. 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.

65. 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.

66. 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 *relevant person* on behalf of the legal arrangement and who will be considered to be the customer(s). In line with Article 3 of the *Money Laundering Order*, the trust or limited partnership will be considered to be the third party on whose behalf the trustee(s) or general partner(s) act(s).

67. In forming a business relationship or carrying out a one-off transaction with a trustee or general partner, a *relevant person* 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 (Section 3.3), the risk factors set out in Section 3.3.4.1 and Section 7.15.1 will be relevant in deciding whether it is appropriate to use information provided by the trustee or general partner. In addition, the monitoring measures maintained by a *relevant person* (Section 6) may provide additional comfort that relevant and up to date information on identity has been found out.

68. 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).

69. The following provisions apply to situations where a trustee of an express trust or general partner of a limited partnership is the **customer** of a *relevant person*. A sector specific section for trust company business explains the *identification measures* to be applied by a trustee or general partner itself in respect of the legal arrangement. See Section 13.

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

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

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

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

73. 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.

74. Where a *relevant person* 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.

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

4.4.1 Finding Out Identity – Legal Arrangement that is a Trust

Guidance Notes

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

- Name of trust.
- Date of establishment.
- Official identification number (e.g. tax identification number or registered charity or non-profit organisation number).
- Mailing address of trustee(s).

77. A *relevant person* may demonstrate that it has found out the identity of the settlor of a trust which is a third party under Article 3(2)(b)(iii)(B) of the *Money Laundering Order* where it finds out the identity of the settlor (including any persons subsequently settling funds into the trust), any person who directly or indirectly provides trust property or makes a testamentary disposition on trust or to the trust, and any other person exercising ultimate effective control over the trust. This information may be provided by the trustee.

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

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

80. A *relevant person* 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.

81. A *relevant person* 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.

82. In any case where a settlor, protector, beneficiary, object of a power, or other person referred to in paragraphs 77 to 81 (the "**person**") is not an individual, a *relevant person* may demonstrate that it has identified each individual who is the person's beneficial owner or controller under Article 3(2)(b)(iii)(C) of the *Money Laundering Order* where it has identified:

    - 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).

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

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

AML/CFT Codes of Practice

84. 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*.

85. A *relevant person* 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

86. A *relevant person* may demonstrate that it has obtained evidence under Article 3(2)(b)(i) of the *Money Laundering Order* that is reasonably capable of verifying that a trust which is a third party 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

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

- Name of partnership.
- Any trading names.
- Date and country 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).

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

89. 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 *relevant person* may demonstrate that it has found out the identity of a person who has a beneficial interest in a limited partnership which is a third party under Article 3(2)(b)(iii)(B) of the *Money Laundering Order* where it finds out the identity of those who exercise **control through other means**, e.g. those who exert control through personal connections, by

participating in financing, because of close and intimate family relationships, historical or contractual associations or as a result of default on certain payments.

90. Where no person is otherwise identified under this section, a *relevant person* may demonstrate that it has found out the identity of a person who has a beneficial interest in a limited partnership which is a third party under Article 3(2)(b)(iii)(B) of the *Money Laundering Order* where it finds out the identity of persons who **exercise control through positions held** (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.

91. In any case where a partner or other person referred to in paragraphs 88 to 90 is not an individual, a *relevant person* may demonstrate that it has identified each individual who is that person's beneficial owner or controller under Article 3(2)(b)(iii)(C) of the *Money Laundering Order* where it has identified:

- 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).

92. 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.

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

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

AML/CFT Codes of Practice

94. 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*.

95. A *relevant person* 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

96. A *relevant person* may demonstrate that it has obtained evidence under Article 3(2)(b)(i) of the *Money Laundering Order* that is reasonably capable of verifying that a limited partnership which is a third party to be identified is 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).

97. However, in the case of a lower risk relationship, a *relevant person* may demonstrate that it has obtained evidence under Article 3(2)(b)(i) of the *Money Laundering Order* that is reasonably capable of verifying that a limited partnership which is a third party to be identified is 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.

98. A *relevant person* may demonstrate that it has obtained evidence under Article 3(2)(b)(i) of the *Money Laundering Order* that is reasonably capable of verifying that a limited partnership which is a third party to be identified is 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 customers):

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

99. A *relevant person* may also demonstrate that it has obtained evidence under Article 3(2)(b)(i) of the *Money Laundering Order* that is reasonably capable of verifying that a partnership which is a third party is 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.

100. 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 *relevant person* may demonstrate that it has taken reasonable measures to find out the identity of that person and to obtain evidence under Article 3(2)(b)(iii)(B) of the *Money Laundering Order* where it obtains the following:

- the full name of the partner; 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

101. 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 67), a *relevant person* may demonstrate that it has taken reasonable measures to obtain evidence of identity for that person under Article 13 of the *Money Laundering Order* where it obtains a copy of a document that is listed in paragraph 28 from the regulated trust and company services provider, along with confirmation on certain matters.

102. 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 *relevant person*, or the document that has been copied to the *relevant person* 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 *relevant person* is a true copy of a document that is held by the regulated trust and company services provider.

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

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

105. 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

106. 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.

107. 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.

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

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

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

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

110. The *Companies Law* allows for the incorporation of cell companies: incorporated cell companies ("*ICC***s**") and protected cell companies ("***PCC*s**").

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

112. 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.

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

114. 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 *relevant person* 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 customer.

115. 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 130.

116. 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.

117. For the purpose of this section, provisions that are said to apply to a company are to be taken to apply, with appropriate modification, to: any other body that can establish a business relationship with a *relevant person* or otherwise own property; an anstalt; an incorporated or unincorporated association, club, society, charity, church body, or institute; a mutual or friendly society; a co-operative; and a provident society.

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

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

120. 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.

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

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

4.5.1 Finding Out Identity – Legal Person that is a Company

Guidance Notes

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

- Name of company.
- Any trading names.
- Date and country 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].

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

125. 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 *relevant person* may demonstrate that it has found out the identity of a person who is the customer's beneficial owner or controller under Article 3(2)(c)(iii) of the *Money Laundering Order* where it finds out the identity of those who exercise **control through other means**, e.g. those who exert control through personal connections, by participating in financing, because of close and intimate family relationships, historical or contractual associations or as a result of default on certain payments.

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

126. Where no person is otherwise identified under this section, a *relevant person* may demonstrate that it has found out the identity of a person who is the customer's beneficial owner or controller under Article 3(2)(c)(iii) of the *Money Laundering Order* where it finds out the identity of persons who **exercise control through positions held** (who have and exercise strategic decision-taking powers or have and exercise executive control through senior management positions, e.g. directors[2]).

127. This information may be provided by the company.

128. In any case where a person identified under paragraphs 124 to 126 is not an individual, a *relevant person* may demonstrate that it has identified each individual who is that person's beneficial owner or controller under Article 3(2)(c)(iii) of the *Money Laundering Order* where it has identified:

- Each individual with a **material controlling ownership interest** in the capital of the 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).

129. 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.

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

131. 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*.

Guidance Notes

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

- Name of company.
- Date and country of incorporation/registration.

[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

- Official identification number.
- Registered office address.
- Principal place of business/operations (where different to registered office).

133. However, in the case of a lower risk relationship, a *relevant person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a company which is a customer to be identified is who 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.

134. A *relevant person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a company which is a customer to be identified is who 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 customers):

- 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.

135. A *relevant person* may also demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a company which is a customer is who 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.

136. 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 *relevant person* may demonstrate that it has taken reasonable measures to find out the identity of that person and to obtain evidence under Article 3(2)(c)(iii) of the *Money Laundering Order* where it obtains the following:

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

4.5.3 Finding Out Identity – Legal Person that is a Foundation

Guidance Notes

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

- Name of foundation.
- Date and country 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).
- Names of all council members and, if any decision requires the approval of any other person, the name of that person.

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

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

139. This information may be provided by the foundation.

140. In any case where a founder, guardian, beneficiary or other person listed in paragraph 138 (the "**person**") is not an individual. a *relevant person* may demonstrate that it has identified each individual who is the person's beneficial owner or controller under Article 3(2)(c)(iii) of the *Money Laundering Order* where it has identified:

- Each individual with a **material controlling ownership interest** in the capital of the person (through direct or indirect holdings of interests or voting rights) or who exerts control through **other ownership means**.
- To the extent that there is doubt as to whether the individuals exercising control through ownership are beneficial owners, or where no individual exerts control through ownership, any other individual exercising **control 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).

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

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

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

AML/CFT Codes of Practice

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

Guidance Notes

144. A *relevant person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a foundation which is a customer is who 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).

145. However, in the case of a lower risk relationship, a *relevant person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a foundation which is a customer to be identified is who 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.

146. A *relevant person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a foundation to be identified is who 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.

147. A *relevant person* may also demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a foundation which is a customer is who 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).

148. Where a council member who is an individual 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 *relevant person* may demonstrate that it has taken reasonable measures to find out the identity of that person and to obtain evidence under Article 3(2)(c)(iii) of the *Money Laundering Order* where it obtains the 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

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

- Name of partnership.
- Any trading names.
- Date and country 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).

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

151. 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 *relevant person* may demonstrate that it has found out the identity of a person who is the customer's beneficial owner or controller under Article 3(2)(c)(iii) of the *Money Laundering Order* where it finds out the identity of those who exercise **control through other means**, e.g. those who exert control through personal connections, by participating in financing, because of close and intimate family relationships, historical or contractual associations or as a result of default on certain payments.

152. Where no person is otherwise identified under this section, a *relevant person* may demonstrate that it has found out the identity of a person who is the customer's beneficial owner or controller under Article 3(2)(c)(iii) of the *Money Laundering Order* where it finds out the identity of persons who exercise **control through positions held** (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).

153. This information may be provided by the partnership.

154. In any case where a partner or other person referred to in paragraphs 150 to 152 is not an individual, a *relevant person* may demonstrate that it has identified each individual who is that person's beneficial owner or controller under Article 3(2)(c)(iii) of the *Money Laundering Order* where it has identified:

- Each individual with a **material controlling ownership interest** in the capital of the partnership (through direct or indirect holdings of interests or voting rights) or who exerts **control** 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).

155. 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.

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

157. 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*.

Guidance Notes

158. A *relevant person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a partnership which is a customer to be identified is who 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.
- Official identification number.
- Registered office/business address.
- Principal place of business/operations (if different).

159. However, in the case of a lower risk relationship, a *relevant person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a partnership which is a customer to be identified is who 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.

160. A *relevant person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a partnership which is a customer to be identified is who 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 customers):

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

161. A *relevant person* may also demonstrate that it has obtained evidence that is reasonably capable of verifying that a partnership which is a customer is who the partnership is said to be under Article 3(2)(a) of the *Money Laundering Order* where the data or information comes from an independent data source 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.

162. 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 *relevant person* may demonstrate that it has taken reasonable measures under Article 3(2)(c)(iii) of the *Money Laundering Order* to find out the identity of that person and to obtain evidence where it obtains the following:

› the full name of the partner; 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

163. 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 who is a beneficial owner or controller of a legal person (following an assessment of risk in line with paragraph 118), a *relevant person* 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 28 from the regulated services provider, along with confirmation on certain matters.

164. 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 *relevant person*, or the document that has been copied to the *relevant person* 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 *relevant person* is a true copy of a document that is held by the regulated trust and company services provider.

165. This will be different to a case where a *relevant person* 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 *relevant person* in respect of record-keeping and access to records - Section 5 is relevant.

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

167. 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 Customer

Overview

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

169. Article 18 allows this particular identification measure (or part of the identification measure) to be simplified in some limited cases.

AML/CFT Codes of Practice

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

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

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

Guidance Notes

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

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

4.7 Timing of Identification Measures

Statutory Requirements

Initial

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

176. *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.*

177. *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 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.*

178. *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 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.*

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

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

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

<u>During Business Relationship</u>

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

182. *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.*

<u>Existing Customers</u>

183. *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.*

184. *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 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 financing of terrorism (unless agreed otherwise with the JFCU).*

185. *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.*

186. *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

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

- *suspects money laundering in respect of any business relationship or transaction with a person;*
- *reasonably believes that the application of identification measures is likely to alert the person to the relevant person's suspicions of money laundering;*
- *has made a report under procedures maintained under Article 21 to a designated police officer or a designated customs officer; 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

188. Article 13(4) of the *Money Laundering Order* allows, in certain circumstances, a *relevant person* 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, in order to comply with Article 14(2) of the *Money Laundering Order*, a *relevant person* must terminate the relationship (Section 4.8).

189. Funds may be received from a customer during the course of establishing a business relationship. A relationship is considered to be established as soon as a *relevant person* acts on instructions as to the operation of that relationship, for example, invests funds in a financial product at the request of a customer.

AML/CFT Codes of Practice

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

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

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

Guidance Notes

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

193. A *relevant person* may demonstrate that *money laundering* and *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 over an account.

194. A *relevant person* may demonstrate that periodic reporting is in line with Article 11(3)(fa) of the *Money Laundering Order* where it highlights to the Board:
    - the number of customers for which evidence of identity has not been obtained during a reporting period (also expressed as a percentage of the total number of business relationships established during the reporting period) and summarises reasons; and
    - in any case where the delay is for more than a particular period of time, the name of the customer, the reason for the delay, the extent to which evidence of identity has not been obtained, the risk rating given to that customer, and action that is to be taken to obtain evidence or terminate the relationship (and by when).
195. Guidance as to appropriate steps to take where a *relevant person* is unable to complete *identification measures* is provided in Section 4.8.

4.7.1 Timing of Identification Measures During Business Relationship – Obtaining Evidence

Guidance Notes

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

4.7.2 Timing for "Existing Customers"

Overview

200. 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.

201. For the purposes of the *Money Laundering Order*, an existing customer means a business relationship established before the *Money Laundering Order* came into force on 4 February 2008 and which continues.

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

203. 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 customer to have been found out by 31 December 2014. There is no similar deadline for obtaining evidence of identity.

204. 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 4 February 2008 (on the basis that documents, data or information will have been obtained under the *CDD* measures prescribed in Article 3).

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

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

AML/CFT Codes of Practice

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

Guidance Notes

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

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

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

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

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

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

4.8 Failure to Complete Identification Measures

Overview

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

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

214. Wherever possible, a *relevant person* should return assets or funds directly to the customer.

215. In a case where a customer requests that assets or funds be transferred to an external party, a *relevant person* should assess whether this provides grounds for knowledge or suspicion, or reasonable grounds for knowledge or suspicion, of *money laundering* or *financing of terrorism*.

216. Where contact has been lost with a customer so that it is not possible to complete termination of a business relationship, assets or funds held should be "blocked" or placed on a "suspense" account until such time as contact is re-established.

Statutory Requirements

217. *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 in the circumstances set out in Article 13(4) of the Money Laundering Order), Article 14(1) of the Money Laundering Order requires that a relevant person shall not establish that business relationship or carry out that one-off transaction.*

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

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

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

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

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 through 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 *relevant person* 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 customer and to obtain evidence of identity.

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

3. Where an *obliged person* has met its customer, who is resident in the same country 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 *relevant person* in a case where the *relevant person* is resident in a different country to the *obliged person* and customer, and where it has not met its customer. Even in a case where the *relevant person* and *obliged person* have met a customer and are resident in the same country, the measures taken by the *obliged person* may still differ to those to be applied by the *relevant person* to the extent that other factors are different, for example the nature of the product or service to be provided.

4. The effect of this is that the *obliged person* may not have found out all of the same information on identity as the *relevant person* needs, and may have obtained evidence of identity using different documents, data or information. This means that, in practice, the scope to place reliance may sometimes be quite limited, and that it may be necessary for a *relevant person* 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 *relevant person*, 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 *relevant person* is permitted to place reliance on the *obliged person* to have found out the identity and to have obtained evidence of the identity of: (i) the *relevant person's* customer; (ii) any beneficial owner or controller of that customer; (iii) any third party for which that customer is acting; (iv) any beneficial owner or controller of a third party for

whom that customer is acting; and/or (v) any person purporting to act on behalf of that customer.

7. It is not possible to place reliance on an *obliged person* to obtain information on the purpose and intended nature of a business relationship or one-off transaction, nor to apply on-going monitoring during a business relationship.

8. Further, Article 16 of the *Money Laundering Order* cannot be applied in any case where a *relevant person* suspects *money laundering* or the *financing of terrorism*, in any case where a *relevant person* considers that there is a higher risk of *money laundering* or the *financing of terrorism* on the basis of a risk assessment carried out under Article 16(4) of the Money Laundering Order (see Section 5.1.1), or 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 *relevant person* immediately before establishing a relationship or carrying out a one-off transaction, a *relevant person* is not also required to immediately obtain evidence of identity. Evidence of identity may be held by an *obliged person*, so long as the *relevant person* is satisfied that the *obliged person* will provide the evidence that it holds on request and without delay. However, it is not uncommon for evidence of identity to be called for at the same time as information on identity is provided by the *obliged person*.

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

    › An investment advisor who arranges for a customer to invest in a financial product provided by a *relevant person*, where the investment is to be held in the name of the customer and not that of the investment advisor.

    › A trust and company services provider who establishes a bank or investment account for a client company, trust or foundation.

11. A *relevant person* 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 *relevant person* 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 customer will have a direct relationship with a *relevant person* and not with the delegate carrying on the outsourced activity. Although the delegate may have substantial contact with the customer, the customer is a customer of the *relevant person* and not of the delegate. The delegate will be carrying on the outsourced activity for the *relevant person* according to the terms of a contract with the *relevant person*. 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 *relevant person* in order to comply with requirements to counter *money laundering* and the *financing of terrorism*, the Data Protection (Jersey) Law 2018 restricts the use of the information to that purpose, except where another condition for processing personal data applies.

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

16. Throughout this section, references to "customer" include, where appropriate, a prospective customer (an applicant for business). A customer 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 measures have already been applied by an obliged person. Obliged person means a person who the relevant person knows or has reasonable grounds for believing is:*

- *A relevant person in respect of whom the 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 *relevant person* must be able to demonstrate that the conditions required by the *Money Laundering Order* are met.

35. All evidence of identity passed by the *obliged person* to a *relevant person* (on request) must be confirmed by the *obliged person* as being a true copy of either an original or copy document held on its file.

Guidance Notes

Assurance in writing about reliance identification measures

36. A *relevant person* may demonstrate that it has obtained adequate assurance in writing from an *obliged person* under Article 16(4)(a) of the *Money Laundering Order* that it has applied *reliance identification measures* to the customer, where the *obliged person*:

    › provides information on identity that it has found out using an information template, 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 36 above will be considered to be reasonably capable of being regarded as reliable under Article 16(6)(a) of the *Money Laundering Order*.

38. Where, as a result of Article 16(6)(b) of the *Money Laundering Order*, a *relevant person* has a more general arrangement with an *obliged person*, such as terms of business, that more general arrangement may be used to explain what evidence of identity will routinely be obtained by the *obliged person*.

Access to evidence of identity

39. A *relevant person* will have demonstrated that an *obliged person* is providing evidence of identity without delay if it is provided within two working days. If it is provided later than five working days, it is not provided without delay. If it is provided between two and five working days, the 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 *relevant person'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 customer risk assessment that is conducted under Section 3.3.4.1 in the cases highlighted at Section 4.4 (paragraph 67) and Section 4.5 (paragraph 118).

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 Code 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 *relevant person* must review the basis upon which it has placed reliance on that *obliged person* for other relationships (if any) in order to determine whether it is still appropriate to do so.

Guidance Notes

46. Immediately before relying upon an *obliged person*, a *relevant person* may demonstrate that it has had regard for the higher risk of *money laundering* and the *financing of terrorism*, and risk that an *obliged person* will fail to provide the *relevant person* with evidence of identity without delay if requested to do so where it considers the following factors:

- The stature and regulatory track record of the *obliged person*.
- The risks posed by the country 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 *relevant person* may demonstrate that it has considered the adequacy of *identification measures* applied by an *obliged person* where it takes one or more of the following steps:

- Reviews previous experience (if any) with the *obliged person*, in particular the adequacy and accuracy of information on identity found out by the *obliged person* and whether that information is current.
- Makes specific enquiries, e.g. through use of a questionnaire or series of questions.
- Reviews relevant *policies and procedures*.
- Where the *obliged person* is a member of a financial group, makes enquiries concerning the extent to which group standards are applied to and assessed by the group's internal audit function.

5.2 Group Reliance

Overview

48. In some strictly limited cases, a *relevant person* 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 *similar identification measures* that have already been applied by a party outside Jersey who is a member of the same financial group as the *relevant person* but not also an *obliged person*.

49. The effect of Article 16A of the *Money Laundering Order* is therefore to extend the application of Article 16 to an *external person* who could not otherwise be relied on, and the six conditions and provisions for testing outlined in Section 5.1 apply to an *external person* in the same way as an *obliged person*.

50. Under the definitions provided in Article 16A(1), in this section:

"***External person***" means a person outside Jersey, who -

- is not an obliged person;
- is a member of the same financial group as the relevant person; and
- carries on a business which, if that business were carried on in Jersey, would be a financial services business.

51. "***Similar identification measures***" means similar measures to those specified in Article 3(2)(a), (aa), (b) and (c) that satisfy Recommendation 10 of the FATF recommendations.

Statutory Requirements

52. *In some strictly limited circumstances, Article 16A of the Money Laundering Order provides that a relevant person may be considered to have applied similar identification measures specified in Article 3(2)(a), (aa), (b) and (c) of the Money Laundering Order where such measures have already been applied by an external person.*

53. *Under Article 16A of the Money Laundering Order, in order to place reliance on an external person, the financial group must:*

- *Apply CDD measures and record-keeping requirements in line with the Money Laundering Order or in line with FATF Recommendations 10, 11 and 12;*

- *Maintain a programme against money laundering and the financing of terrorism which includes policies and procedures by which every member of the group who carries on a financial services business (or equivalent) shares information that is appropriate for the purpose of preventing and detecting money laundering and the financing of terrorism (**AML/CFT programme**); and*
- *Be supervised by an overseas regulatory authority in its implementation of CDD measures and record-keeping requirements and its AML/CFT programme.*

In addition, any higher risk of money laundering must be adequately mitigated by the policies and procedures of the group.

54. *Article 16(A)(2), (3), (4), (5) and (6) of the Money Laundering Order states that reliance is always subject to a number of conditions. These are outlined at paragraphs 20 to 25 above, where references to obliged person should be read as referring to external person.*

55. *Articles 16(A)(7) and (8) of the Money Laundering Order state that reliance must always be subject to testing. Provisions in this respect are outlined at paragraphs 26 to 30 above, where references to obliged person should be read as referring to external person.*

56. *Article 1(5) of the Money Laundering Order explains that a person is a member of the same financial group as another person if there is, in relation to the group, a parent company or other legal person that exercises control over every member of that group for the purposes of applying group supervision under:*

- *The Core Principles for Effective Banking Supervision published by the Basel Committee;*
- *The Objectives and Principles for Securities Regulation issued by IOSCO; or*
- *The Insurance Supervisory Principles issued by the IAIS.*

AML/CFT Codes of Practice

57. A *relevant person* may not rely on an *external person* where it suspects *money laundering* or the *financing of terrorism*, considers that there is a higher risk of *money laundering* or the *financing of terrorism* on the basis of a risk assessment carried out under Article 16(3) of the *Money Laundering Order*, or where the *external person* has a relevant connection to a country or territory that is subject to a *FATF* call to apply enhanced *CDD* measures.

58. Despite a *relevant person's* reliance on an *external person* under Article 16A(9) of the *Money Laundering Order*, a relevant person is liable for any failure to apply *similar identification measures*.

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 through 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 *relevant person* 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 customer activity.
4. The requirement to keep documents, data or information up to date and relevant is discussed at Section 3.4 of the *AML/CFT 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 *relevant person* **monitors** all customer transactions and activity in order to **recognise notable transactions or activity,** i.e. those that:

› Are inconsistent with the *relevant person's* knowledge of the customer (unusual transactions or activity);

› Are complex or unusually large;

› Form part of an unusual pattern; or

› Present a higher risk of *money laundering* or *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 requires a *relevant person* to also scrutinise customer activity (though this will already be the effect of *policies and procedures* required by Article 11(3)(a)(iii) of the *Money Laundering Order*). This is particularly relevant where a business relationship does not involve transactions, e.g. where a *relevant person* gives investment advice or acts as a director to a company, but will be relevant also in a transaction-based business relationship.

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

14. Sections 3 and 4 of the *AML/CFT Handbook* address the capturing of sufficient information about a customer that will allow a *relevant person* to prepare and record a customer business and risk profile which will provide a basis for recognising notable transactions or activity.

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 customer, or with the normal business activities for the type of product or service that is being delivered.

16. Where a *relevant person's* customer base is homogeneous, and where the products and services provided to customers result in uniform patterns of transactions or activity, e.g. deposit-taking activity, it will be more straightforward to establish parameters to identify usual transactions and unusual activity. However, where each customer is unique, and where the product or service provided is bespoke, e.g. acting as trustee of an express trust, a *relevant person* will need to tailor monitoring systems to the nature of its business and facilitate the application of additional judgement and experience to the recognition of unusual transactions and activity. For such businesses, appropriate staff training in the recognition of unusual transactions and activity is vital, and will often already be necessary in order to satisfy fiduciary responsibilities placed on the *relevant person* under other legislation. For example, the approval of a transaction for a discretionary trust will involve two or three senior people in a person carrying on trust company business.

17. **Higher risk transactions or activity** may be recognised by developing a set of "red flags" or indicators which may indicate *money laundering* or *financing of terrorism*, based on a *relevant person's* understanding of its business, its products and its customers (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 *relevant person'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 customer business and risk profile, but on occasions this examination will involve requesting additional information from a customer.

21. Notable transactions or activity may indicate *money laundering* or *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 *financing of terrorism* is addressed in Section 8 of the *AML/CFT Handbook*.

22. Scrutiny may involve both **real time** and **post event** monitoring. Real time monitoring will focus on transactions and activity when information or instructions are received from a customer, before or as the instruction is processed. Post event monitoring may involve end of day, weekly, monthly or annual reviews of customer transactions and activity. Real time monitoring of transactions and activity will more effectively reduce a *relevant person's* exposure to *money laundering* and *financing of terrorism*. Post event monitoring may be more effective at identifying unusual patterns.

23. Monitoring may involve **manual** and **automated** procedures. Automated monitoring procedures may add value to manual procedures by recognising transactions or activity that fall outside set parameters. This will be particularly so where a *relevant person* processes large

volumes of customer transactions which are not subject to day to day oversight. However, automated monitoring procedures may not be appropriate in cases where there is close day to day overview of a business relationship, e.g. where a *relevant person* carries on trust company business, where the subsequent preparation of financial statements and periodic review of a business relationship may be expected to highlight notable transactions and activity.

24. The examination of notable transactions or activity may be conducted either by customer facing employees, or by an independent reviewer. In any case, the examiner must have access to all customer records.

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

26. In order to recognise *money laundering* and *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 9 of the *AML/CFT 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 *relevant person's* knowledge of the customer, including the customer's business and risk profile.

28. A *relevant person* must establish and maintain appropriate and consistent *policies and procedures* which provide for the identification and scrutiny of:

- Complex or unusually large activity;
- Unusual patterns of activity, which have no apparent economic or visible lawful purpose; and
- Any other activity, the nature of which causes the *relevant person* 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 *relevant person* must examine, as far as possible, their background and purpose and set forth its findings in writing.

Guidance Notes

30. A *relevant person* may demonstrate that *CDD policies and procedures* are appropriate where **scrutiny** of transactions and activity has regard to the following factors:

- Its business risk assessment (including the size and complexity of its business);
- Whether it is practicable to monitor transactions or activity in real time (i.e. before customer instructions are put into effect); and
- Whether it is possible to establish appropriate standardised parameters for automated monitoring.

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

- **Customer business and risk profile** - see Section 3.3.5 of the *AML/CFT Handbook*.
- **"Red flags" or indicators of higher risk** - that reflect the risk that is present in the *relevant person's* customer base – based on its business risk assessment (refer to Section 2.3.1 of the *AML/CFT 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.

› "**Red flags" or indicators of complex transactions** - based on its business risk assessment (refer to Section 2.3.1 of the *AML/CFT 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.

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

› Reference to the customer's business and risk profile;

› As far as possible, a review of the background and purpose of a transaction or activity (set in the context of the business and risk profile); and

› Where necessary, the collection of further information needed to determine whether a transaction or activity has an apparent economic or visible lawful purpose.

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

› Revises, as necessary, its customer's business and risk profile.

› Adjusts, as necessary, its monitoring system e.g. refines monitoring parameters, enhances controls for more vulnerable products/services/business units; and

› Considers whether its knows, suspects or has reasonable grounds for suspecting that another person is engaged in *money laundering* or *financing of terrorism*, or that any property constitutes or represents the proceeds of criminal conduct.

6.2.2 Monitoring and Recognition of Business Relationships and Transactions - 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 or transaction 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 *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 person or organization.**

36. As a part of its on-going monitoring procedures, a *relevant person* will establish appropriate procedures to **monitor** all customer transactions and activity in order to **recognise** whether any business relationships or one-off transactions 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 the *AML/CFT Handbook*.

38. There is not a statutory requirement to **examine**, or have *policies and procedures* in place to examine, business relationships or transactions 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 *relevant person* must establish and maintain appropriate and consistent *policies and procedures* which provide for the **examination** of transactions and activity recognised as being with a person connected with an enhanced risk state.

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

Guidance Notes

42. A *relevant person* may demonstrate that *CDD policies and procedures* are appropriate where **scrutiny** of transactions and activity has regard to the following factors:

- Its business risk assessment (including the size and complexity of its business);
- Whether it is practicable to monitor transactions or activity in real time (i.e. before customer instructions are put into effect); and
- Whether it is possible to establish appropriate standardised parameters for automated monitoring.

43. A *relevant person* may demonstrate that *CDD policies and procedures* are appropriate where the following are used to **recognise** connections with persons connected to enhanced risk states and sanctioned countries:

- **All -** Customer business and risk profile in line with Section 3.3.5 of the *AML/CFT 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 *relevant person* may demonstrate that *CDD policies and procedures* are appropriate if **examination** of transactions or activity recognised as being with a person connected with an enhanced risk state includes:

- Reference to the customer's business and risk profile;
- As far as possible, a review of the background and purpose of a transaction or activity (set in the context of the business and risk profile); and
- Where necessary, the collection of further information needed to determine whether a transaction or activity has an apparent economic or visible lawful purpose.

45. A *relevant person* may demonstrate that *CDD* and reporting *policies and procedures* are appropriate if **post-examination** of transactions or activity recognised as being with a person connected with an enhanced risk state it:

- Revises, as necessary, its customer's business and risk profile.
- Adjusts, as necessary, its monitoring system e.g. refines monitoring parameters, enhances controls for more vulnerable products/services/business units; and

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

› Considers whether its knows, suspects or has reasonable grounds for suspecting that another person is engaged in *money laundering* or *financing of terrorism*, or that any property constitutes or represents the proceeds of criminal conduct.

6.3 Automated Monitoring Methods

Overview

46. As noted in paragraph 23 above, 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 customer's business and risk profile.

48. Large or more complex *relevant persons* 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 customer 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 *relevant person*.

50. Where an automated monitoring method (group or otherwise) is used, a *relevant person* will need to understand:

› How the system works and when it is changed;

› Its coverage (who or what is monitored and what external data sources are used);

› How to use the system, e.g. making full use of guidance; and

› The nature of its output (exceptions, alerts etc).

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

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 customers may be particularly effective. However, where a *relevant person* uses group screening arrangements, it will need to be satisfied that it provides adequate mitigation of risks applicable to the Jersey business. In all cases, it is important that a *relevant person*:

› 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] https://www.jerseyfsc.org/media/1721/banking-aml-sanctions-summary-findings-2014.pdf

7 ENHANCED AND SIMPLIFIED CDD MEASURES AND EXEMPTIONS

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 through 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, 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 *relevant person* determines that a customer presents a higher risk of *money laundering* or *financing of terrorism*, Articles 15, 5A and 15B of the *Money Laundering Order* also requires enhanced *CDD* measures to be applied in the following specified scenarios:

Scenario	Section
Customer, or some other person, is not physically present for identification purposes	7.4
Customer has a "relevant connection" to an "enhanced risk state"	7.5
Customer, or some other prescribed person, is a *PEP*	7.6
Customer is a non-resident	7.7
Customer is provided with private banking services	7.8
Customer is a personal asset holding vehicle	7.9
Customer is a company with nominee shareholders or issues bearer shares.	7.10
Correspondent Banking or similar Relationships	7.11

3. It may be that *CDD* measures routinely applied under Article 13 of the *Money Laundering Order* already address some of the risk characteristics of these customers (for instance identification of beneficial owner(s) and understanding the nature and purpose of the relationship) and significantly reduce the risk that criminals may hide behind "shell" companies or that the basis for the relationship is not considered or understood. Therefore any additional measure 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 the *AML/CFT Handbook* and must address the particular risk

presented. This section provides some (non-exhaustive) examples for each category of customer.

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

6. Throughout this section, references to "customer" include, where appropriate, a prospective customer (an applicant for business). A customer 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 customer; (ii) a beneficial owner or controller of a customer; (iii) a third party for whom a customer is acting; (iv) a beneficial owner or controller of a third party described in (iii); or (v) a person acting, or purporting to act, on behalf of a customer is a PE*P; *(vi) a beneficiary under a life insurance policy.*

8. *Article 11(3)(d) of the Money Laundering Order requires a relevant person to maintain appropriate and consistent policies and procedures to determine whether a business relationship or one-off transaction is with a person connected with a country or territory that does not apply, or insufficiently applies, the FATF Recommendation*s.

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

   a) if a customer has, or proposes to have, a business relationship or proposes to carry out a one-off transaction with the relevant person and the relevant person is not resident in the customer's country of residence or in the same country as the country from which, or from within which, the customer is carrying on business;

   b) if a customer has not been physically present for identification purposes;

   c) if the relevant person has or proposes to have a business relationship or proposes to carry out a one-off transaction with a customer having a relevant connection with a country or territory (an "enhanced risk state") in relation to which the FATF has called for the application of enhanced customer due diligence measures;

   d) if the customer of the relevant person is a company with nominee shareholders or that issues shares in bearer form;

   e) if the customer of the relevant person is –

      i) a legal person established by an individual for the purpose of holding assets for investment purposes; or

      ii) a person acting on behalf of a legal arrangement established for an individual for the purpose of holding assets for investment;

   f) if the relevant person provides or proposes to provide a customer with private banking services;

   g) any situation which by its nature can present a higher risk of money laundering.

7.3 Higher risk customer

Overview

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

11. Enhanced *CDD* measures must be applied where a *relevant person*'s assessment is that there is a higher risk of *money laundering* or *financing of terrorism* (i.e. a situation which by its nature can present a higher risk of *money laundering* or *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 *relevant person* may demonstrate that it has applied enhanced *identification measures* to an individual who is a higher risk customer under Article 15 of the *Money Laundering Order* where it obtains evidence that verifies a:

    › Former name (such as maiden name); or

    › Passport or national identity card number.

14. A *relevant person* may demonstrate that it has applied enhanced *identification measures* to a higher risk customer under Article 15(1)(b) of the *Money Laundering Order* where it takes reasonable measures to find out the *source of funds* and *source of wealth* at the time that a relationship is established or one-off transaction carried out which are commensurate with risk and include one or more of the following:

    › Commissioning an independent and reliable report from a specialist security agency about the *source of funds* involved and/ or customer's *source of wealth*.

    › Where a *relevant person* is part of a group, obtaining reliable information from the group's internal security department or business intelligence unit (or equivalent) about the *source of funds* involved and /or customer's *source of wealth*.

    › Where a *relevant person* is part of a group, obtaining reliable information from a part of the group which has an office in the country or territory with which the customer has a connection about the *source of funds* involved and/ or customer's *source of wealth*.

    › Obtaining reliable information directly from the customer concerned, for instance during (or subsequent to) a face to face meeting inside or outside Jersey, or via a telephone "welcome call" on a home or business number which has been verified or by obtaining certified copies of corroborating documentation such as contracts of sale, property deeds, salary slips, etc.

    › Obtaining reliable information from an external party (for instance a solicitor, accountant or tax advisor) which has an office in the country or territory with which the customer has the relevant connection about the *source of funds* involved and/or customer's *source of wealth*.

    › Obtaining reliable information from a person eligible to be an *obliged person* (for instance a solicitor, accountant or tax advisor) about the *source of funds* involved and/ or customer's *source of wealth*.

    › Where information is publicly available or available through subscription databases, obtaining reliable information from a public or private source about the *source of funds* involved and/or customer's *source of wealth*.

- Obtaining reliable information through financial statements that have been prepared in accordance with generally accepted accounting principles and audited in accordance with generally accepted auditing standards.

15. Where a relevant connection is established during the course of an existing relationship, a *relevant person* may also demonstrate that it has taken reasonable measures to find out the *source of funds* and/or *source of wealth* where it reviews the relationship information that it already holds and concludes that it is reliable.

16. Where the measures set out in paragraph 13 to 15 above are not sufficient to mitigate the risk associated with the customer, a *relevant person* may demonstrate that it has applied enhanced *identification measures* where it does one or more of the following in a way that is commensurate with risk.

- In a case where a document that has been used to obtain evidence of identity for a higher risk customer, e.g. a passport, subsequently expires, a *relevant person* may demonstrate that documents, data or information obtained under *identification measures* are kept up to date and relevant where a copy of the document that replaces that originally used to obtain evidence of identity is requested and obtained.
- In a case where a relationship is to be established making use of a suitable certifier, it obtains confirmation that a photograph contained in the document certified bears a true likeness to the individual requesting certification (or words to that effect).

17. A *relevant person* may demonstrate that it has applied enhanced on-going monitoring to a higher risk customer where it:

- Reviews the business relationship on at least an annual basis, including all documents, data and information obtained under *identification measures* in order to ensure that they are kept up to date and relevant.
- Where monitoring thresholds are used, sets lower thresholds for transactions connected with the business relationship.

7.4 Customer not physically present for identification measures

Overview

18. Frequently, relationships will be established where there is no face to face contact with the customer 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 customer, but where documentary evidence is to be provided at a time when the customer is not present.

20. Such circumstances may increase the risk of *money laundering* or *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 *relevant person*. 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 relevant person must apply enhanced CDD measures on a risk-sensitive basis.*

AML/CFT Code of Practice

23. A *relevant person* must apply enhanced *CDD* measures on a risk-sensitive basis where a person who falls within Article 3(7) of the *Money Laundering Order*, or who is the beneficial owner or controller of a customer, or is a person who must otherwise be identified under Article 3 of the *Money Laundering Order* is not physically present for identification purposes.

Guidance Notes

24. A *relevant person* may demonstrate that it has applied enhanced *identification measures*: (i) under Article 15 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 *relevant person* 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 *relevant person* 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 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 *relevant person*'s risk assessment for A, including:
  - Requiring the first payment for the financial services product or service to be drawn on an account in the customer's name at a bank that is a *regulated person* or carries on *equivalent business* (refer to Section 1.7).
  - Telephone contact with the customer prior to establishing a relationship on a home or business number which has been verified, or a "welcome call" to the customer before transactions are permitted, using the call to verify additional components of identity found out.
  - Internet sign-on following verification measures where the customer uses security codes, tokens, and/or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address.
  - Specific card or account activation measures.

7.5 Customer with relevant connection to an "enhanced risk state"

Overview

27. The *FATF* has identified a number of countries and territories which have failed to address their own *money laundering* and *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 *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 Customer with a Relevant Connection

Statutory Requirements

29. *Under Article 15(2)(a) of the Money Laundering Order, for the purpose of the Article 151(c), the following definitions apply: 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 Codes of Practice

30. The enhanced *CDD* measures applied to a customer with a relevant connection to an enhanced risk state must include:

- Requiring any new business relationship (and continuation thereof) or one-off transaction to be approved by senior management; and
- Where there is a relevant connection because a customer's *source of funds* is, or derives, from: (i) assets held in the state by the customer or by any person on behalf of the customer; or (ii) income arising in the state, taking reasonable measures to find out the source of the wealth of the customer.

Guidance Notes

31. A *relevant person* 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 *relevant person* may also demonstrate that it has taken reasonable measures to find out the *source of wealth* where it reviews the relationship information that it already holds and concludes that it is reliable.

33. A *relevant person* may demonstrate that it has otherwise applied enhanced *CDD* measures where it does all of the following:

    › In a case where a document that has been used to obtain evidence of identity for a higher risk customer, e.g. a passport, subsequently expires, a *relevant person* may demonstrate that documents, data or information obtained under *identification measures* are kept up to date and relevant where a copy of the document that replaces that originally used to obtain evidence of identity is requested and obtained.

    › In a case where a relationship is to be established making use of a suitable certifier, it obtains confirmation that a photograph contained in the document certified bears a true likeness to the individual requesting certification (or words to that effect).

    › Reviews the business relationship on at least an annual basis, including all documents, data and information obtained under *identification measures* in order to ensure that they are kept up to date and relevant.

    › Where monitoring thresholds are used, sets lower thresholds for transactions connected with the business relationship.

7.6 Customer who is a politically exposed person (PEP)

Overview

34. Corruption 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 countries and territories concerned. This is in addition to the possibility of criminal charges.

36. Indications that a customer may be connected with corruption include excessive revenue from “commissions” or “consultancy fees” or involvement in contracts at inflated prices, where unexplained “commissions” or other charges are paid to external parties.

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 *relevant person* to a *PEP*:

- Who is the Minister of Finance in a country that is prone to corruption may be very different to the measures to be applied to a senior politician with a limited portfolio in a country or territory that is not prone to corruption.
- 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. *PEP* status itself does not, of course, incriminate individuals or entities. It will mean, however, that the customer may be subject to enhanced *CDD* measures. The nature and scope of a *relevant person*'s activities will generally determine whether the existence of *PEP*s in its customer base is a practical issue for the *relevant person*.

7.6.1 Determining whether a customer is a politically exposed person

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 relevant person need only have regard to information which is in that person's possession or is publicly known.*

7.6.2 Enhanced customer due diligence measures in relation to politically exposed persons

Statutory Requirements

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

- *who has or proposes to have a business relationship with, or proposes to carry out a one-off transaction with, a foreign politically exposed person; or*
- *who has or proposes to have a high risk business relationship, or proposes to carry out a high risk one-off transaction with, a domestic politically exposed person or prominent person; or*
- *if any of the following is a foreign politically exposed person or, in the case of a high risk business relationship or one-off transaction, a domestic politically exposed person or prominent person –*
  - *i) a beneficial owner or controller of the customer of the relevant person*
  - *ii) a third party for whom the customer of the relevant person is acting,*
  - *iii) a beneficial owner or controller of a third party described in clause (ii),*
  - *iv) a person acting or purporting to act on behalf of the customer of the relevant person.*

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

- *unless the relevant person is a sole trader, measures requiring a new business relationship or continuation of a business relationship or a new one-off transaction to be approved by the senior management of the relevant person;*
- *measures to establish the source of the wealth of the politically exposed person and source of the funds involved in the business relationship or one-off transaction;*
- *measures to conduct the enhanced ongoing monitoring of that relationship; and*
- *if the relevant business relationship relates to a life insurance policy, measures requiring the senior management to be informed before any payment is made under the policy or any right vested under the policy is exercised.*

"enhanced ongoing monitoring" *means ongoing monitoring that involves specific and adequate measures to compensate for the higher risk of money laundering.*

"high risk", *in relation to a business relationship or one-off transaction, means any situation which by its nature can present a higher risk of money laundering.*

"source of the wealth" *means the source generating the total net worth of funds of the politically exposed person, whether those funds are used in the business relationship or one-off transaction.*

AML/CFT Codes of Practice

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

Guidance Notes – foreign PEPs

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

    › Assesses those countries and territories with which customers 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 customers 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 *relevant person* 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. See Section 3.3.4.2.

    › Exercises vigilance where customers are involved in business sectors that are vulnerable to corruption such as, but not limited to, oil or arms sales.

47. Where a *relevant person* runs the details of all its customers 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 customers 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 customer, or person acting, or purporting to act for a customer, and where no property of that *PEP* is handled in the particular business relationship or one-off transaction, a *relevant person* may demonstrate that it applies specific and adequate measures under Article 15A(2) of the *Money Laundering Order* where it considers the nature of the *PEP*'s 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 customer, or is a beneficiary or object of a power of a trust, and where no property of that *PEP* is handled in the particular business relationship or one-off transaction, a *relevant person* may demonstrate that it applies specific and adequate measures under Article 15A(2) of the *Money Laundering Order* where it considers the nature of the *PEP*'s connection and reason why the *PEP* has such a connection.

Guidance Notes – domestic PEPs

50. In determining whether someone is a domestic PEP, a relevant person 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 Greffe
- Comptroller of Taxes
- 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 PEPs

53. Mandatory enhanced measures are only required in relation to higher risk relationships or transactions with domestic PEPs, 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 relevant person considers that other specific risk factors indicate a higher risk. Particular consideration should be given to the following characteristics that might indicate a higher risk:

- responsibility for, or ability to influence, large public procurement exercises;
- responsibility for, or ability to influence, allocation of government licenses (or similar);
- personal wealth or lifestyle inconsistent with known legitimate sources of income or wealth;
- credible allegations of financial misconduct.

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 relevant person considers that other specific risk factors indicate a higher risk. Particular consideration should be given to the following characteristics that might indicate a higher risk:

- wealth or lifestyle inconsistent with known legitimate sources of income or wealth;
- credible allegations of financial misconduct;
- wealth derived from the granting of government licences (or similar);
- wealth derived from preferential access to the privatisation of former state assets.

7.7 Non-resident customer

Overview

56. Customers who are not resident in a country or territory but who nevertheless seek to form a business relationship or conduct a one-off transaction with a *relevant person* in that country or territory will typically have legitimate reasons for doing so. Some customers will, however, pose a risk of *money laundering* or *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 relevant person and the relevant person is not resident in the customer's country of residence or in the same country as the country from which, or from within which, the customer is carrying on business, a relevant person must apply enhanced customer due diligence measures on a risk-sensitive basis.*

Guidance Notes

58. A *relevant person* may demonstrate that it has applied enhanced *CDD* measures under Article 15(1)(a) of the *Money Laundering Order*, where it has applied additional measures that are commensurate with risk. Additional measures may include one or more of the following:

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

7.8 Customer provided with private banking services

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 customers may therefore present a higher risk of *money laundering* or *financing of terrorism*.

60. For the avoidance of doubt, a trustee who may from time to time facilitate such banking or investments services as part of carrying on trust company business is not considered to be providing private banking services, where such facilitation is ancillary to the core business of acting as a trustee.

Statutory Requirements

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

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 *relevant person* 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 Customer 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.

65. Article 15(1)(e) of the *Money Laundering Order* is intended to apply in two specific scenarios. Firstly, where the personal asset holding vehicle is the customer. Secondly, where the personal asset holding vehicle is the third party for whom a trustee or general partner (the customer) is acting.

Guidance Notes

66. A *relevant person* may demonstrate that it has applied enhanced *CDD* measures under Article 15(1)(e) of the *Money Laundering Order*, where it has applied additional measures that are commensurate with risk. Additional measures may include:

› Determining the purpose and rationale for making use of such a vehicle, and being satisfied that the customer's use of such an investment vehicle has a genuine and legitimate purpose.

› Taking reasonable measures to find out and document the *source of funds* and *source of wealth.*

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

Overview

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 customer should not be considered to be a customer that issues bearer for the purpose of Article 15(1) of the *Money Laundering Order*:

- The bearer shares are issued by a company in a country or territory that has fully enacted appropriate legislation to require bearer shares to be registered in a public registry and the bearer shares are so registered; or
- The bearer shares are traded on an approved stock exchange; or
- All issued bearer shares are held in the custody of the *relevant person*, the customer or trusted external party along with an undertaking from that trusted external party or customer to inform the *relevant person* of any transfer or change in ownership.

Guidance Notes

70. A *relevant person* may demonstrate that it has applied enhanced *CDD* measures under Article 15(1)(d) of the *Money Laundering Order*, where it has applied additional measures that are commensurate with risk.

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

- Determining and being satisfied with the reasons why the customer is making use of nominees; 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.

72. In the case of customers who are companies with bearer shares (or the ability to issue bearer shares in the future), additional measures may include:

- Determining and being satisfied with the reasons why the customer has issued bearer shares or retains the ability to do so;
- Ensuring that any new or continued relationship or any one-off transaction is approved by the senior management of the *relevant person*; 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 customer due diligence measures in relation to correspondent banking (or similar) relationships

Overview

73. Correspondent banking is a term given to the provision of services by one bank (the "correspondent") to another bank (the "respondent") for the benefit of the customers of the respondent. As a result, the correspondent bank indirectly makes its services available to the customers of the respondent business; in doing so, the correspondent potentially exposes itself to additional risk. This section sets out the additional customer due diligence measures required where a bank enters into a correspondent banking relationship to appropriately manage the risk presented by that relationship.

74. Due to the nature of Jersey's banking industry, Jersey-based banks will in most cases be a respondent rather than correspondent bank.

75. FATF standards also require financial institutions to apply enhanced measures in relation to other similar relationships, for example, those established for securities transactions or funds transfers, whether for the cross-border financial institution as principal or for its customers.

Statutory Requirements

76. *Article 15B of the Money Laundering Order applies to a relevant person who has or proposes to have a banking or similar relationship with an institution whose address for that purpose is outside Jersey.*

77. *Under Article 15B(2) of the Money Laundering Order a relevant person must apply enhanced customer due diligence measures on a risk-sensitive basis including –*

- *gathering sufficient information about the institution to understand fully the nature of its business;*
- *determining the reputation of the institution and the quality of its supervision, including whether it has been subject to any money laundering investigation or regulatory action;*
- *assessing the institution's systems and controls to combat money laundering in order to determine whether they are consistent with the requirements of the FATF recommendations and their effectiveness;*
- *requiring any new relationship to be approved by the senior management of the relevant person;*
- *ensuring that both the relevant person and the institution clearly understand their respective responsibilities to prevent and detect money laundering and recording those responsibilities; and*
- *being satisfied that, in respect of customers of the institution who have services provided directly by the relevant person, that the institution has applied customer due diligence measures at least equivalent to those set out in this Order and is able to provide a copy, at the request of the relevant person, of the evidence, documents, data and information obtained when applying such measures.*

78. *Article 23A(1) of the Money Laundering Order provides that a relevant person that is a correspondent bank must not enter into a correspondent banking relationship, or continue an existing correspondent banking relationship, with a respondent that is a shell bank.*

79. *Article 23A(2) of the Money Laundering Order provides that a relevant person that is a correspondent bank must take appropriate measures to ensure that it does not enter into a correspondent banking relationship, or continue an existing correspondent banking relationship, with a bank that is known to permit its accounts to be used by a shell bank.*

Guidance Notes

80. A relevant person may demonstrate that it has gathered sufficient information about the respondent to understand fully the nature of its business where it obtains information concerning the following:

- the geographic location of the customer base;
- the general nature of the customer base;
- the nature of the services which the respondent provides to its customers;
- whether relationships are conducted by the respondent on a non-face to face basis; and

› the extent to which the respondent relies on third parties to identify and hold evidence of identity or to conduct other customer due diligence measures on customers.

81. A relevant person that is a correspondent bank may also determine the reputation of a respondent by assessing its stature.

82. A relevant person that is a correspondent bank may determine that a respondent's systems and controls are consistent with the requirements of the FATF Recommendations where the respondent is a bank that carries on equivalent business to deposit -taking (refer to section 1.7 of Part 1).

83. Where customers of the respondent have direct access to the services of the correspondent bank, a relevant person that is a correspondent bank may satisfy itself as to the adequacy of a respondent's customer due diligence measures, and its ability to provide relevant customer due diligence information and documents on request where it obtains a written assurance from the respondent to this effect. The correspondent bank may also satisfy itself as to the adequacy of the customer due diligence measures of the respondent and its ability to produce information and documentation on request by periodically requesting relevant customer due diligence information and documents.

7.12 Enhanced CDD measures - transitional arrangements

Overview

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

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

86. 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 *relevant person* 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 *relevant person* 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*.

7.13 Exemptions from CDD Requirements

Overview

87. Part 3A of the *Money Laundering Order* provides for exemptions from CDD requirements that apply in some strictly limited circumstances, as set out in Articles 17B - D and 18.

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

a) the relevant person suspects money laundering;

b) the relevant person 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.

89. In addition to above a relevant person 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.

90. For the purpose of Part 3A , "**relevant customer**" means a customer of a relevant person that the relevant person knows or reasonably believes is –

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

b) a person wholly owned by a relevant person 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 1988[4], except that the offer of units in the scheme or arrangement is not an offer to the public within the meaning of that Article

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

Statutory Requirements

91. *Under Article 17B(1) of the Money Laundering Order, a relevant person is exempt from applying third party identification requirements in relation to a third party for which a relevant customer is acting where the relevant customer is acting in the course of a business –*

› *that falls within paragraph (a), (b) or (d) in the definition of "regulated business", or equivalent business; or*

› *that is an investment business or fund services business registered under the Financial Services (Jersey) Law 19985, or equivalent business.*

92. *Under Article 17B(2) of the Money Laundering Order, a relevant person must record the reasons for applying the exemption, having regard to the risk of money laundering inherent in the relevant customer's business and the higher risk of money laundering associated with that type of business should the relevant customer fail to –*

a) apply the identification measures specified in Article 3(2)(b) or if the relevant customer is not in Jersey, similar identification measures required to be applied to satisfy the requirements in Recommendation 10 of the FATF recommendations; or

b) keep records, or keep them for the period required to be kept.

AML/CFT Code of Practice

93. A *relevant person* must be able to demonstrate that the conditions required by the *Money Laundering Order* are met.

7.15 Exemption from applying third party identification requirements in relation to certain relevant customers involved in unregulated or non-public funds, trust company business or the legal profession

Statutory Requirements

94. *Under Article 17C(1) of the Money Laundering Order a relevant person is exempt from applying third party identification requirements in relation to a third party for which a relevant customer is acting if the relevant customer –*

a) is, or carries on business in respect of, an unregulated fund, within the meaning of the Collective Investment Funds (Unregulated Funds) (Jersey) Order 2008[6], 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 1998[7], or equivalent business, but only if the relevant person is –

i) carrying on deposit-taking business,

ii) a lawyer carrying on business described in paragraph 1 of Part B of Schedule 2 to the 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 20088, but only if the relevant person is carrying on deposit-taking business.

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

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

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

96. *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 relevant person in relation to a business relationship or transaction.

97. *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 Article 17C(2)(b) (or under an equivalent provision that applies outside Jersey) may, if requested by the other person, provide the person with the information or evidence obtained from applying the identification measures referred to in Article 17C(2)(b)(i) (See paragraph 95 above).*

Guidance Notes

98. In relation to the exemption set out at Article 17C(1)(a) or (b), a relevant person may be satisfied that there is little risk of money laundering or 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

99. In relation to the exemption set out at Article 17C(1)(c)(i), a relevant person may be satisfied that there is little risk of money laundering or financing of terrorism occurring where:

› deposited funds are held only temporarily for one or more third parties in a client account operated by a person carrying on trust company business, pending the transfer to a designated account for a third party, where the funds are not to be held on an undisclosed basis for longer than 40 days;

› deposited funds are held only temporarily for one or more third parties in a client account operated by a person carrying on trust company business, pending the receipt of instructions when exiting a customer relationship, where the funds are not to be held on an undisclosed basis for longer than 40 days;

› deposited funds are held only temporarily for one or more third parties in a client account operated by a person carrying on trust company business, to facilitate ad hoc (not routine) cheque payments where designated accounts do not otherwise have this facility;

› deposited funds are held only temporarily for one or more third parties in a client account operated by a person carrying on trust company business, to facilitate the aggregation of statutory fees for onward payment;

› deposited funds are held only temporarily for one or more third parties in a client account operated by a person carrying on trust company business, to receive fees payable to the customer which have been paid in advance;

› deposited funds are held only temporarily for one or more third parties in a client account operated by a person carrying on trust company business, to receive customer money on an ad hoc basis paid to the customer in error.

- deposited funds are held for one or more third parties in a client account operated by a person carrying on trust company business, where the number and value of third party transactions effected is low, e.g. to provide third parties with access to low cost banking facilities where third parties' liquid assets are of insufficient value and volume for the establishment of a designated relationship (e.g. balances of £1,000 or less per relationship, with little activity); or
- deposited funds are aggregated by a person carrying on trust company business in order to attract a better return on investment for third parties, and where the aggregated deposit is received from and paid back (including income or profit generated) to an account held with another person carrying on deposit-taking business who is registered to do so by the Commission, the Guernsey Financial Services Commission or the Isle of Man Financial Supervision Commission.

100. In relation to the exemption set out at Article 17C(1)(d), a relevant person may be satisfied that there is little risk of money laundering or financing of terrorism occurring where the deposit is in respect of a third party's registered contract within the meaning of the Control of Housing and Work (Jersey) Law 2012.

101. In relation to the exemption set out at Article 17C(1)(c)(ii) or (iii), guidance on when a relevant person may be satisfied that there is little risk of money laundering or financing of terrorism occurring is provided in the *AML/CFT Handbook for the Legal Sector* and the *AML/CFT Handbook for Accountancy sector.*

7.15.1 Assessment of Risk

Overview

102. The risk factors that are set out in this section will also be relevant to a customer risk assessment that is conducted under Section 3.3.4.1 in the cases highlighted at Section 4.4 (paragraph 66) and Section 4.5 (paragraph 117).

Statutory Requirements

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

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

105. *Article 17D(3) of the Money Laundering Order also provides testing requirements for application of CDD exempts 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.

106. *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

107. In a case where, for a particular business relationship, testing under Article 17D(3) of the *Money Laundering Order* highlights that a customer has not found out information or obtained evidence of identity for a third party (or parties), does not keep that information or evidence of identity, or will not provide it on request and without delay when requested to do so, a *relevant person* must review the basis upon which it has applied CDD exemptions to other relationships with that particular customer (if any) in order to determine whether it is still appropriate to apply those measures.

Guidance Notes

108. Immediately before applying the exemption under this Part, a *relevant person* may demonstrate that it has had regard to a customer's business where it considers the following factors:

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

109. Immediately before applying the exemption under this Part, a *relevant person* may demonstrate that it has had regard for the higher risk of *money laundering* and *financing of terrorism* should its customer fail to apply *identification measures*, keep records, or keep records for the required period where it considers the following factors:

- The stature and regulatory track record of its customer.
- The adequacy of the framework to combat *money laundering* and *financing of terrorism* (including, for the avoidance of doubt, financial sanctions) in place in the country or territory in which its customer is based and the period of time that the framework has been in place.
- The adequacy of the supervisory regime to combat *money laundering* and *financing of terrorism* to which its customer is subject.
- The adequacy of *identification measures* applied by its customer to combat *money laundering* and *financing of terrorism*.
- The extent to which the customer itself relies on obliged parties (however described) to identify its clients and to hold evidence of identity, and whether such obliged parties are *relevant person*s or carry on an *equivalent business*.

110. A *relevant person* may demonstrate that it has considered the adequacy of *identification measures* applied by its customer where it takes one or more of the following steps:

- Reviews previous experience (if any) with the customer.
- Makes specific enquiries, e.g. through use of a questionnaire or series of questions.
- Reviews relevant *policies and procedures*.
- Where the customer is a member of a financial group, makes enquiries concerning the extent to which group standards are applied to and assessed by the group's internal audit function.
- Conducts (or commissions from an external expert) sample testing of the adequacy of the customer's *policies and procedures* to combat *money laundering* and *financing of terrorism*, whether through onsite visits, or through requesting specific CDD information and/or copy documentation to be provided.

7.16 Further exemptions from applying identification requirements

Overview

111. Article 18 of the Money Laundering Order provides specified circumstances where exemptions from applying identification requirements

Statutory Requirements

Case 1. Insurance business

112. *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

113. *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

114. *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

115. *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

116. *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.

Case 6. Schedule 2 Business (Lawyers and Estate Agents)

117. *Under Article 18(6), a relevant person is exempt from applying the identification requirements in Article 13 to the extent that the measures require identification of a person within the meaning of Article 3(4)(b) if –*

a) the relevant person's business falls within paragraph 1 or 3 of Part B of Schedule 2 to the Law; and

b) that person enters into a business relationship or carries out a one-off transaction for the purpose of enabling a customer, directly or indirectly, to enter into a registered contract (within the meaning of the Control of Housing and Work (Jersey) Law 2012.

AML/CFT Codes of Practice

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

119. A relevant person must obtain and retain documentation establishing that the customer is entitled to benefit from an exemption in Article 18 of the Money Laundering Order.

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

Overview

120. Where a *relevant person* enters into a business relationship or carries out a one-off transaction relating to a pension, superannuation, employee benefit, share option or similar scheme, in some limited circumstances there is no requirement to apply *identification measures*.

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

Guidance Note

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

7.16.2 Jersey public authority

Overview

123. Where a customer 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 body authority, on the beneficial owners and controllers of the authority, or those purporting to act on behalf of the authority.

124. 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.

125. 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.

7.16.3 Body corporate with listed securities

Overview

126. Where a customer 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).

127. 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.

128. 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.

129. 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.

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

7.16.4 Regulated person and those carrying on equivalent business

Overview

131. Where a customer 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 customer, the beneficial owners and controllers of the customer, or those purporting to act on behalf of the customer. Nor is there a requirement to verify the authority of any person purporting to act for the customer.

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

7.16.5 Person authorised to act on behalf of a customer

Guidance Notes

133. Where a person authorised to act on behalf of a customer holds this role by virtue of *his* employment by (or position in) a business that is a *regulated person* (or equivalent), a *relevant person* 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.

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

Overview

134. 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 customer who is an individual (or are individuals),

then the receipt of funds from such an account may be considered to be reasonably capable of verifying that the person to be identified is who the person is said to be where the product or service requested by the customer is considered to present a very low *money laundering* or *financing of terrorism* risk. This will be the case where funds may only be received from, and paid to, an account in the customer's name, i.e. a product or service where funds may not be paid in by, or paid out to, external parties.

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

AML/CFT Codes of Practice

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

137. 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 customer;
- no initial or future payments may be received from external parties;
- cash withdrawals are not permitted, with the exception of face to face withdrawals by the customer, where 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 customer, or on the death of the customer to a personal representative named in the grant of probate or the letters of administration; and
- no future changes must be made to the product or service that enable funds to be received from or paid to external parties.

138. A *relevant person* must obtain and retain evidence confirming that payment has been received from an account at a bank that is a *regulated person* or carries on an *equivalent business* to deposit-taking (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 customer'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).

139. If a *relevant person* 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 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 through the use of italic text. The Glossary is available from the JFSC website.

8.1 Overview of section

1. 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. It also sets *AML/CFT Codes* for and provides guidance to:
   - Employees making a report to their *MLRO* (or *deputy MLRO*) (referred to as **internal *SAR***); and
   - *MLROs* (and *deputy MLROs*) making a report to the *JFCU* (referred to as an **external *SAR***).
2. The 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.
3. 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.
4. A report may also be based on information from other sources, including law enforcement agencies, other government bodies, the media, or the customer.
5. Whilst this section describes reports made to the *JFCU* under the *Proceeds of Crime Law* and *Terrorism Law* as *SARs*, depending on the circumstances such reports may involve knowledge of *money laundering* or *financing of terrorism*, rather than suspicion (or reasonable grounds for knowledge or suspicion).
6. Additional information on reporting is contained within Part 2 of the *AML/CFT Handbook*.

8.2 Reporting knowledge or suspicion

Overview

7. Legislation deals with reporting by a *relevant person* 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 *financing of terrorism* offence, the person shall not be guilty of that offence (where certain conditions are fulfilled) where it makes a **protective report**.

8. In practice, a report made in accordance with the **reporting requirement** will also provide **protection**. Take the situation of a *relevant person* 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.

9. 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 *relevant person'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*.

10. 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*).

11. 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.

12. 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 report knowledge or suspicion

Overview

13. In the course of carrying on a *financial services business*, employees of a *relevant person* 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.

14. 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 *relevant person* would have inferred knowledge or formed a suspicion (the so called "objective test"[1]).

15. 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.

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

16. A *relevant person's MLRO* (or *deputy MLRO*) must consider all internal *SARs* as soon as practicable.

17. A *relevant person'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.

18. 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.

19. 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.

20. 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.

21. Other than in the course of carrying on a *financial services business* (i.e. any other trade, profession or business carried on by the revenant person), employees of a *relevant person* 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.

22. 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

23. *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.*

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

    › *Another person is engaged in money laundering or the financing of terrorism; or*

    › *Any property constitutes or represents the proceeds of criminal conduct.*

25. *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****.*

26. *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.

27. *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).*

28. *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.*

29. *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.*

30. *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 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.*

31. *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.*

32. *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.*

33. *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 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.*

34. *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.*

35. *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.*

36. *"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.*

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

38. *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.*

39. *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.*

40. *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.***

41. *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 proposes 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.*

42. *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

43. In the course of carrying on its business, employees of a *relevant person* will raise an internal *SAR* in order to be protected where they suspect or believe that:

    › Property constitutes or represents the proceeds of criminal conduct;

    › Property is terrorist property; or

    › They are providing a service for the purposes of terrorism or for the support of a terrorist entity.

44. 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.

45. A *relevant person's MLRO* (or *deputy MLRO*) must consider all internal *SARs* as soon as practicable.

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

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

48. 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 *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.

49. 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.

50. 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.

51. 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

52. *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.*

53. *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.*

54. *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.*

55. *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 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.*

56. *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.*

57. *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.*

58. *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.*

59. *"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.*

60. *Article 18 of the Terrorism Law contains similar provisions in circumstances where 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.*

61. *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.*

8.3 Procedures for reporting

Overview

62. Reporting procedures provide the interface between *CDD* measures carried out by a *relevant person* and the work of the *JFCU's* intelligence wing. Like all *policies and procedures*, they should be drafted in a way that can be readily understood by employees, should be tailored to the *relevant person's* risk assessment, and applied in every case where functions are outsourced (in line with Section 2.4.4 of the *AML/CFT Handbook*).

Statutory requirements

63. *Article 21 of the Money Laundering Order requires that a relevant person must establish and maintain reporting procedures which:*

- *communicate to employees the identity of the MLRO (and any deputy MLROs) to whom an internal SAR is to be made;*
- *provide for that report to be considered by the MLRO (or deputy MLRO) in the light of all other relevant information for the purpose of determining whether or not the information or other matter contained in the report gives rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering or financing of terrorism;*
- *allow the MLRO (or deputy MLRO) to have access to all other information which may be of assistance in considering the report;*
- *provide for the information or other matter contained in an internal SAR to be disclosed as soon as is practicable by the MLRO (or deputy MLRO) to a designated police officer or designated customs officer using the approved form, where the MLRO (or deputy MLRO) knows, suspects or has reasonable grounds to know or suspect that another person is engaged in money laundering or 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.*

64. *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 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 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

65. In addition to reporting procedures that must be maintained under Article 21 of the *Money Laundering Order*, a *relevant person* 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 *SARs* 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 *SARs* to be made in a set format and to include as full a statement as possible of the information or matter giving rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion, date that the information or matter came to the employee's attention, and full details of the customer, transaction or activity that it has on its records.

› Require internal *SARs* to be acknowledged by the *MLRO* (or *deputy MLRO*) as soon as is practicable.

› Require the *MLRO* (or *deputy MLRO*) to record all internal *SARs* 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).

66. A *relevant person* must not allow internal *SARs* to be filtered by line management such that they do not reach the *MLRO* (or *deputy MLRO*). Where procedures allow employees to discuss relationships and transactions with line managers before an internal *SAR* is made, they must emphasise that the decision on reporting remains with that employee.

67. A *relevant person* 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

68. A *relevant person* may demonstrate that it has established and maintained arrangements for disciplining employees by ensuring that employment contracts and employment handbooks provide for the imposition of disciplinary sanctions for failing to report knowledge, suspicion or

reasonable grounds for knowledge or suspicion without reasonable excuse, or as soon as it is practicable.

69. A *relevant person* may demonstrate that employees make internal *SARs* as soon as practicable where the *MLRO* (or *deputy MLRO*) periodically considers (by business area if appropriate):

- The 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 *SARs*, and concludes that both are consistent with the *relevant person's* business risk assessment.

8.3.2 External SARs

Overview

70. The *MLRO* (or *deputy MLRO*) must consider each internal *SAR*. In order to do so, the *Money Laundering Order* requires that the *MLRO* (or *deputy MLRO*) has access to all necessary records. The *MLRO* (or *deputy MLRO*) may also require further information to be obtained from the customer. Any such approach will need to be made sensitively and probably by someone other than the *MLRO* (or *deputy MLRO*) to minimise the risk of alerting the customer that a report to the *JFCU* may be being considered (though this may not yet be tipping off).

71. 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

72. In addition to reporting procedures that must be maintained under Article 21 of the *Money Laundering Order*, a *relevant person* must maintain procedures that:

- Require the *MLRO* (or *deputy MLRO*) to document all enquiries made in relation to each internal *SAR*.
- Require the *MLRO* (or *deputy MLRO*) to document the basis for reporting to the *JFCU* or deciding not to make such a report, which must be retained with the internal *SAR*.
- Require the *MLRO* (or *deputy MLRO*) to record all external *SARs* 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

73. A *relevant person* 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 accounts 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.

74. A *relevant person* may demonstrate that the *MLRO* (or *deputy MLRO*) reports as soon as practicable where the Board 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 *SARs* not processed within a period of time set by the Board, together with an explanation.

8.4 JFCU consent

Overview

75. Protective reports before or after doing an act are not equal options which a *relevant person* can choose between.

- A report should be made **before doing an act** where a customer instruction is received prior to an activity or transaction taking place, or arrangements being put in place. However, when a transaction which gives rise to concern is already within an automated clearing or settlement system where a delay would lead to a breach of a contractual obligation or where it would breach market settlement or clearing rules, the *MLRO* (or *deputy MLRO*) may need to let the transaction proceed and report it later.
- A report should be made **after doing an act** where something appears suspicious only with the benefit of hindsight or following the receipt of additional information.

76. 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 *relevant person* will generally be provided with consent to maintain the customer 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.

77. 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.

78. 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.

79. 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 *relevant person* that consent will not be given, a *relevant person* should be aware of the risk of committing a tipping off offence where it fails to act on a customer instruction. In any written communication with that customer it should consider using general wording such as "highlighting its compliance with statutory obligations".

80. Where a *relevant person* is refused consent it should contact the *JFCU* for guidance on what, if any, information can be provided to the customer (though the *JFCU* is not obligated to provide such guidance). In circumstances where consent is withheld, the *JFCU* may expressly allow the

relevant person to notify the customer of the fact that they are the subject of a police investigation without the risk of committing a tipping off offence. Such notification will not be sanctioned by the *JFCU* where it might prejudice a domestic or overseas investigation.

81. Where a *relevant person* does not wish to act upon a customer's instruction, this may lead to civil proceedings being instituted by the customer for breach of contract. It may be necessary in circumstances where a customer has instigated civil proceedings for the *relevant person* to seek legal advice or the directions of the court.

82. A *relevant person* may reduce the potential threat of civil proceedings by ensuring that customers' terms of business specifically:

- Allowing an instruction to be delayed or deferred, pending investigation.
- Exclude breaches in circumstances where following a customer instruction may lead to the *relevant person* committing an offence.

8.5 Tipping off

Overview

83. 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*.

84. 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 collection 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.

85. Inter alia, the effect of this is that a *relevant person* or employee of a *relevant person*:

- Cannot, at the time, tell a customer that a transaction or activity is being delayed because an internal *SAR* is about to be made or has been made to the *MLRO* (or *deputy MLRO*).
- Cannot, at the time, tell a customer that a transaction or activity is being delayed because an external *SAR* is about to be made or awaiting consent from the *JFCU*.
- Cannot later tell a customer that a transaction or activity was delayed because an internal or external *SAR* had been made.
- Cannot tell the customer that law enforcement is conducting an investigation.

86. However, a tipping off offence is not committed when a *relevant person* discloses: that an internal *SAR* has been made; that it will make, or has made, an external *SAR*; information relating to such *SARs*; or information relating to a criminal investigation 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 *relevant person's* financial statements (except where the disclosure is made with a view to furthering a criminal purpose).

87. 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**.

88. 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*.

89. 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 *financing of terrorism*.

90. 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).

91. In a case where a *relevant person*:

- Is the customer 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*.

92. 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.

93. 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

94. *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 of suspects that a SAR has been, or will be, made - except if the disclosure is a* ***protected disclosure*** *under the Tipping Off Regulations.*

95. *Article 35(2) of the Proceeds of Crime Law and Article 35(2) of the Terrorism Law make it an offence to disclose any information relating to an investigation, or to interfere with material which is likely to be relevant to such an investigation, where a person knows or suspects that the Attorney General or any police officer is acting or proposing to act in connection with money laundering or financing of terrorism investigation - except if the disclosure is a* ***protected disclosure*** *under the Tipping Off Regulations.*

96. *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.*

97. *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

98. *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.*

99. *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 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 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.*

100. *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).*

101. *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.*

102. *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.*

103. *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.*

104. *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.*

105. *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.*

106. *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).*

107. *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.*

108. *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

109. In addition to reporting procedures that must be maintained under Article 21 of the *Money Laundering Order*, a *relevant person* must maintain procedures that remind employees making internal *SARs* of the risk of committing a tipping off offence.

8.5.1 CDD measures

Overview

110. 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 *relevant person* suspects *money laundering* or *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.

111. Where a *relevant person* suspects *money laundering* or *financing of terrorism*, the application of *identification measures* could unintentionally lead to the customer being tipped off, where the process is managed without due care.

112. 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 customer (and its advisers) may be minimised by:

- Ensuring that employees applying *identification measure*s 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 *relevant person* is concerned that applying *identification measures* will lead to the customer being tipped off.

113. Where a relevant person reasonably believes that the application of *identification measures* could lead to the customer being tipped off, then under Article 14(6) of the *Money Laundering Order* it is not necessary to apply such measures, where an external *SAR* has been made and the *JFCU* has agreed that the measures need not be applied.

114. Reasonable enquiries of a customer 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 business relationship

Overview

115. The giving of consent by the *JFCU* following an external *SAR* is not intended to override normal commercial judgement, and a *relevant person* is not committed to continuing a business relationship with a customer if such action would place the *relevant person* at commercial risk.

116. 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 *relevant person* must be free to make such judgements. However, in certain circumstances, a *relevant person* should consider liaising with the *JFCU* to consider whether it is likely that termination would alert the customer or affect an investigation in any way. If there is continuing suspicion and there are funds which need to be returned to the customer, a *relevant person* should seek advice from the *JFCU*.

8.6 Disclosure to group companies and networks

Overview

117. 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 *financing of terrorism*, where a *relevant person* 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 *financing of terrorism* at group or network level.

118. Accordingly, it is important that there should be no legal impediment to providing certain information to a group company or network.

119. Where a *relevant person* 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 customer to do so in certain circumstances.

Statutory Requirements

120. *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 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.*

121. *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.*

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 through the use of italic text. The Glossary is available from the JFSC website.

9.1 Overview of 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 *financing of terrorism* risks; and (ii) well trained in the recognition of notable transactions or activity which may indicate *money laundering* or *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 *relevant person* takes action to make sure that customer-facing and other employees are:
   - Competent and have probity;
   - Aware of policies and procedures and their obligations under the Proceeds of Crime Law, Terrorism Law, Directions Law, Terrorist Sanctions Measures, 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 *financing of terrorism*) or transactions and activity with enhanced risk states and/ or sanctioned countries (Section 6).
4. In particular, customer facing employees and those who handle or are responsible for the handling of customers and transactions will provide a *relevant person* with its strongest defence, or its weakest link.
5. The term "employee" is to be understood to include officers of a *relevant person* and is not limited to individuals working under a contract of employment. It will include temporary and contract employees, and the employee of any external party fulfilling a function in relation to a *relevant person* under an outsourcing agreement.
6. A *relevant person* should also encourage its 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 *relevant person* must screen the competence and probity of the following employees at the time of recruitment and where there is a subsequent change in an employee's role:

   › Those undertaking any customer facing functions, or handling or responsible for the handling of business relationships or one-off transactions;

   › Those directly supporting a colleague who undertakes any customer facing functions, or who handles or is responsible for the handling of business relationships or one-off transactions, e.g. individuals processing and book-keeping customer transactions;

   › The *MLRO* (and any *deputy MLRO*) and *MLCO*; and

   › The Board and senior managers.

Guidance Notes

9. A *relevant person* may demonstrate that employees are screened where it does one or more of the following, as appropriate for the nature of the employee's role and responsibilities:

   › Obtains and confirms references.

   › 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 a financial services business (hereafter referred to as "***relevant employees***"), and not to all employees of a *relevant person*. However, *money laundering* and *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 relationship managers, trust and company administrators, and stock-brokers.

Statutory Requirements

12. *Article 11(9), (10), (10A) and (11) of the Money Laundering Order require that a relevant person must, in relation to employees whose duties relate to the provision of a financial services business:*

   › Take appropriate measures from time to time for the purposes of making them aware of:

      a. *The CDD, record-keeping, reporting and other policies and procedures for the purposes of preventing and detecting money laundering and 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.

b. *The enactments in Jersey relating to money laundering and the financing of terrorism and any relevant Code of Practice;*

› Provide those employees from time to time with training in the recognition and handling of:

a. *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*

b. *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 relevant person's policies and procedures, employees' awareness and the training provided to employees.

AML/CFT Code of Practice

13. A *relevant person* must:

› Provide employees who are not *relevant employee*s with a written explanation of the *relevant person*'s and employee's obligations and potential criminal liability under the *Proceeds of Crime Law*, *Terrorism Law*, *Directions Law*, and *Terrorist Sanctions Measures*, including the implications of failing to make an internal *SAR*; and

› Require such employees to acknowledge that they understand the *relevant person*'s written explanation and procedures for making internal *SAR*s.

14. In the case of a *relevant person* 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 *relevant person* 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 *relevant person* may demonstrate that it has satisfied awareness raising and training obligations that apply to *relevant employee*s where it includes:

› Employees undertaking any customer facing functions, or handling or responsible for the handling of business relationships or one-off transactions;

› Employees directly supporting a colleague who undertakes any customer facing functions, or handles or is responsible for the handling of business relationships or one-off transactions, e.g. individuals processing and book-keeping customer transactions;

› The *MLRO* (and any *deputy MLRO*) and *MLCO*; and

› The Board and senior managers.

17. A *relevant person* who is a sole trader may demonstrate that they are aware of relevant enactments (under paragraph 15) and able to recognise and handle transactions and other conduct (under paragraph 16) where they have received formal training or through self study.

9.4 Awareness of Relevant Employees

Overview

18. With the passage of time between training initiatives, the level of employee awareness of the risk of *money laundering* and *financing of terrorism* decreases. The utilisation of techniques to maintain a high level of awareness can greatly enhance the effectiveness of a *relevant person*'s defences against *money laundering* and the *financing of terrorism*.

Guidance Notes

19. A *relevant person* 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 *relevant person* 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 *relevant person* 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 *relevant person*'s and employee's obligations and potential criminal liability under the *Proceeds of Crime Law*, *Terrorism Law*, *Directions Law*, and *Terrorist Sanctions Measures*, 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 *relevant person*'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 *relevant person* may demonstrate that it takes appropriate measures to make *relevant employee*s who are officers (e.g. directors) 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 *relevant person*.

9.4.1 Monitoring and Testing Effectiveness

Guidance Notes

22. A *relevant person* may demonstrate that it maintains procedures for monitoring and testing the effectiveness of awareness raising where it periodically tests employees' awareness of:

- Risks and *policies and procedures*, and 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 *relevant person* has identified a risk that may arise in relation to new products, services, business practices and technology, including where developed at group level or by outside developers (in Jersey and elsewhere), a *relevant person* 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 *relevant person* 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 products, 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 *relevant person* 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 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 *relevant person* 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-customer 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 *relevant person* must provide employees with adequate training at appropriate frequencies.

29. Such training must:

- Be tailored to the *relevant person* 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 *relevant person* may demonstrate the provision of adequate training to *relevant employee*s where it addresses:

- The Proceeds of Crime Law, Terrorism Law, Directions Law, Terrorist Sanctions Measures, Money Laundering Order and AML/CFT Codes of Practice issued under the Supervisory Bodies Law.
- Vulnerabilities of products and services offered by the *relevant person* (based on the *relevant person*'s business risk assessment), and subsequent *money laundering* and *financing of terrorism* risk.
- *Policies and procedures*, and employees' responsibilities.
- Application of risk based *CDD policies and procedures*.
- Recognition and examination of notable transactions and activity, such as activity outside of expected patterns, unusual settlements, abnormal payment or delivery instructions and changes in the patterns of business relationships.
- *Money laundering* and *financing of terrorism* developments, including techniques, methods, trends and typologies (having regard for reports published by the insular authorities, *FATF* and *FSRB*s).
- Management of business relationships or one-off transactions subject to an internal *SAR*, e.g. risk of committing the offence of tipping off, and dealing with questions from such customers, and/or their advisers.

9.5.2 The Board

Guidance Notes

31. A *relevant person* may demonstrate the provision of adequate training to board members 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 *relevant person* 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*) in place to prevent and detect *money laundering* and the *financing of terrorism*.

9.5.4 The MLRO and Deputy MLROs

Guidance Notes

33. A *relevant person* 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 *relevant person* 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 *relevant person* may demonstrate the provision of training at appropriate frequencies by:

    › Providing all employees with induction training within 10 working days of the commencement of employment and, when necessary, where there is a subsequent change in an employee's role.

    › 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 the *AML/CFT Handbook*.

37. Such monitoring and testing should also be considered in the context of the Board's periodic check that *systems and controls* (including *policies and procedures*) are operating effectively, as set out at Section 2.4.1 of the *AML/CFT Handbook*.

10 RECORD-KEEPING

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 through 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* and provides guidance on keeping records. More general obligations on *relevant person*s 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 or *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 *relevant person*s with statutory requirements and *AML/CFT Codes*. Records provide evidence of the work that a *relevant person* has undertaken to comply with statutory requirements and *AML/CFT Codes*. Records also provide a necessary context for the opinion that may be prepared on the truth and fairness of a *relevant person*'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 customer's identity, a *relevant person* must keep a copy, or references to the evidence of the customer's identity obtained during the application of *CDD* measures. In circumstances (such as where evidence is obtained at a customer'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 *relevant person* must keep supporting documents, data and information in respect of a business relationship or one-off transaction including: documents, data and information obtained under *identification measures*; accounts files; and business correspondence and the results of any analysis undertaken.

Statutory Requirements

7. *Article 19(2)(a) of the Money Laundering Order requires a relevant person to keep the following records:*
   - *copies of evidence of identity or information that enables a copy of such evidence to be obtained; and*
   - *all the supporting documents, data and information in respect of a business relationship or one-off transaction which is the subject of CDD measures, including the results of analysis undertaken in relation to the business relationship or any transaction.*
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 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.*
10. *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

11. A *relevant person* may demonstrate that it keeps all supporting documents, data and information in respect of a business relationship or one-off transaction where it keeps accounts files and business correspondence.

10.3 Recording Transactions

Overview

12. Details of all transactions carried out with or for a customer 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

13. *Article 19(2)(b) of the Money Laundering Order requires a relevant person to keep a record containing details of every transaction carried out with or for the customer in the course of a financial services business. In every case, sufficient information must be recorded to enable the reconstruction of individual transactions.*
14. *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.*
15. *Article 20(3) of the Money Laundering Order requires a relevant person to keep records relating to transactions for at least five years from the date when all activities relating to the transaction are completed.*

16. *Article 20(5) of the Money Laundering Order allows the Commission to require a relevant person to keep records of transactions for a period that is more than five years.*

AML/CFT Codes of Practice

17. A record must be kept of the following for every transaction carried out in the course of a business relationship or one-off transaction:
    - the name and address of the customer;
    - if a monetary transaction, the kind of currency and the amount;
    - if the transaction involves a customer's account, the number, name or other identifier for the account;
    - the date of the transaction;
    - details of the counterparty, including account details;
    - the nature of the transaction; and
    - details of the transaction.
18. Customer transaction records must provide a clear and complete transaction history of incoming and outgoing funds or assets.

Guidance Notes

19. A *relevant person* 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.
20. A *relevant person* may demonstrate that it has a clear and complete transaction history where it records all transactions undertaken on behalf of a customer within that customer's records. For example, a customer's records should include all requests for wire transfer transactions where settlement is provided other than from funds drawn from a customer's account with the *relevant person*.
21. When original vouchers or documents are used for account entry, e.g. credit/debit slips and cheques, are not returned to the customer, a *relevant person* may demonstrate that it has kept details of a transaction where such vouchers or documents are kept for at least one year to assist forensic analysis.

10.4 Other Record-keeping Requirements

10.4.1 Corporate Governance

AML/CFT Codes of Practice

22. A *relevant person* 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 the *AML/CFT Handbook*.
23. A *relevant person* 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 the *AML/CFT Handbook*.

24. A *relevant person* 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 the Board has assessed both the effectiveness of, and compliance with, *systems and controls* (including *policies and procedures*) in line with Section 2.3 of the *AML/CFT Handbook*, including reports presented by the *MLCO* on compliance matters and *MLRO* on reporting.

25. A *relevant person* 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 the *AML/CFT Handbook*.

26. A *relevant person* 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 the *AML/CFT Handbook*.

27. A *relevant person* 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 the *AML/CFT Handbook*:

    › Measures that are at least equivalent to *AML/CFT Codes of Practice* are applied to *financial services business* carried on by a *relevant person* 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 *relevant person* is required to apply an identification measure through an AML/CFT Code set in Sections 4, 5 and 7 of the *AML/CFT 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 *relevant person* 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 customer that has still to be remediated in line with Section 4.7.3 of the *AML/CFT Handbook*.

10.4.3 On-going Monitoring

30. A *relevant person* 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 *relevant person*'s knowledge of the customer (unusual transactions or activity);

    › Are complex or unusually large;

    › Form part of an unusual pattern; or

    › Present a higher risk of money laundering or *financing of terrorism*,

    for a period of five years from the end of the calendar year in which the examination is undertaken.

31. A *relevant person* 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 *relevant person* 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 the *AML/CFT Handbook*.

33. In line with procedures required under Sections 8.3.1 and 8.3.2 of the *AML/CFT Handbook*, a *relevant person* 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 customer 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 *relevant person* 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 *relevant person*s to be able to access and retrieve relevant information without undue delay.

AML/CFT Codes of Practice

36. A *relevant person* 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 *relevant person* must be readily accessible and retrievable by the person. Unless otherwise specified, records relating to evidence of identity, other *CDD* measures, and transactions must be accessible and retrievable within 5 working

days (whether kept in 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 *relevant person* must periodically review the condition of paper and electronic records and consider the adequacy of its record-keeping arrangements.

39. A *relevant person* 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.

41. When original documents (such as transaction related vouchers used to input data onto computer systems) that would ordinarily have been destroyed are requested for investigation purposes, a *relevant person* must ascertain whether the documents have in fact been destroyed.

10.5.1 External Record-keeping

Overview

42. Where records are kept by another person (group or otherwise) or kept outside Jersey, such as under outsourcing or storage arrangements, this will present additional factors for a *relevant person* to consider. Whatever the particular circumstances, a *relevant person* remains responsible for compliance with all record-keeping requirements.

43. Where an *obliged person* ceases to trade or have a relationship with a customer for whom it has provided an assurance to a *relevant person*, particular care needs to be taken to check that the 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 *relevant person* 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 relevant business merges with another person, continues as another person, is taken-over by another person, is subject to internal reorganisation, terminates its activities, or transfers a block of customers to another person.

AML/CFT Codes of Practice

46. A *relevant person* 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 *relevant person* terminates its activities, or transfers a block of customers 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) 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 an 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.*

11 WIRE TRANSFERS

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 through the use of italic text. The Glossary is available from the JFSC website.

11.1 Overview of Section

1. The FATF Recommendation 16 on Wire Transfers with the revised interpretative note ("**FATF Recommendation 16**") was implemented within the European Union by Regulation (EU) 2015/847 of 20 May 2015 on Information Accompanying Transfers of Funds ("**Regulation (EU) 2015/847**"), which repealed and replaced the previous regime under Regulation (EC) 1781/2006 to promote a more targeted and focused risk approach to the full traceability of transfers of funds for the purpose of prevention, detection and investigation of money laundering and terrorist financing.

2. Regulation (EU) 2015/847 further expands the regulatory requirements with the following objectives:

   - to prevent the abuse of fund transfers for money laundering, terrorist financing and other financial crime purposes,
   - to detect such abuse should it occur,
   - to support the implementation of restrictive measures, and
   - to allow relevant authorities to access the information promptly.

3. In Jersey, Regulation (EU) 2015/847 was implemented by virtue of the EU Legislation (Information Accompanying Transfers of Funds) (Jersey) Regulations 2017 ("**Wire Transfers Regulations** " or "**Regulations**") with an effect from 13 June 2017 as if it was an enactment to any extent that it doesn't otherwise have effect in Jersey, subject to certain exceptions, adaptations and modifications. Under Regulations, references to "Member State" and "the Union" shall be read as if Jersey were itself a Member State, its territory was included within the Union territory and for the purposes of European Union law were a separate country from the United Kingdom.

4. Under the Wire Transfers Regulations, the following definitions apply:

   "payment service provider" ("**PSP**") means a person, being a person registered under the Banking Business (Jersey) Law 1991, when:

   - the person is carrying out payment services in or from within Jersey; or
   - being a legal person established under Jersey law, the person is carrying out payment services in any part of the world other than in or from within Jersey;

   "intermediary payment service provider" ("**IPSP**") means PSP that is neither that of the payer nor that of the payee and that participates in the execution of transfers of funds;

   "*payer*" means a person that is the holder of an account held with a PSP that allows a transfer of funds from the account or, where there is no account, a person that places an order for a transfer of funds;

   "*payee"* means a person that is the intended final recipient of transferred funds.

5. The core requirement is that every wire transfer must be accompanied by specific information ("**complete information**") about the payer and the payee, which should be collected and retained by payment institutions, unless special exemptions and derogations apply, including funds transfers between the British Islands.

6. A PSP should establish for each transfer of funds whether it acts as the PSP of the payer, as the PSP of the payee or as an IPSP. This will determine what information has to accompany a transfer of funds and the steps to take to comply with the Regulations.

7. It also requires PSPs to put in place effective procedures to detect transfers of funds that lack the required information about the payer and the payee, and to determine whether to execute, reject or suspend such transfers of funds.

8. References to the British Islands in this section are to an area that comprises the United Kingdom, the Bailiwick of Jersey, the Bailiwick of Guernsey, and the Isle of Man.

9. In line with the Data Protection (Jersey) Law 2018, personal data obtained by PSPs, should be used only for the purpose of preventing money laundering and terrorist financing, and PSPs should ensure the confidentiality of such data.

10. Any record of information on payer/payee should not be kept longer than is necessary for the purposes of preventing, detecting and investigating money laundering and terrorist financing.

11. In this section, any reference to a numbered Article, without more, is a reference to the Article so numbered of Regulation (EU) 2015/847 as it is read in the Wire Transfers Regulations.

11.2 The scope of the Regulations

Statutory Requirements

12. *The Wire Transfer Regulations shall apply to transfers of funds, in any currency, which are sent or received by PSP or IPSP established in Jersey, unless the Regulations sets out exemptions and derogations (Article 1).*

13. *These include credit transfers, direct debits, money remittances and transfers carried out using a payment card, an electronic money instrument, or a mobile phone, or any other digital or IT prepaid or post-paid device with similar characteristics, irrespective of whether the payer and the payee are the same person and irrespective of whether the PSP of the payer and that of the payee are one and the same. For British Islands-based PSPs, it includes, but is not necessarily limited to, international payment transfers made via SWIFT, including various Euro payment systems, and domestic transfers via CHAPS and BACS.*

14. *Despite the wide scope, the Wire Transfer Regulations shall not apply to transfers of funds that are exempt, such as transfers of funds corresponding to services referred to in points (a) to (m) and (o) of the Directive 2007/64/EC of the European Parliament and of the Council; under Article 2(1):*

    (a) payment transactions made exclusively in cash directly from the payer to the payee, without any intermediary intervention;

    (b) payment transactions from the payer to the payee through a commercial agent authorised to negotiate or conclude the sale or purchase of goods or services on behalf of the payer or the payee;

    (c) professional physical transport of banknotes and coins, including their collection, processing and delivery;

    (d) payment transactions consisting of the non-professional cash collection and delivery within the framework of a non-profit or charitable activity;

(e) services where cash is provided by the payee to the payer as part of a payment transaction following an explicit request by the payment service user just before the execution of the payment transaction through payment for the purchase of goods or services;

(f) money exchange business, that is to say, cash-to-cash operations, where the funds are not held on a payment account;

(g) payment transactions based on any of the following documents drawn on the payment service provider with a view to placing funds at the disposal of the payee:

(i) paper cheques in accordance with the Geneva Convention of 19 March 1931 providing a uniform law for cheques;

(ii) paper cheques similar to those referred to in point (i) and governed by the laws of Member States which are not party to the Geneva Convention of 19 March 1931 providing a uniform law for cheques;

(iii) paper-based drafts in accordance with the Geneva Convention of 7 June 1930 providing a uniform law for bills of exchange and promissory notes;

(iv) paper-based drafts similar to those referred to in point (iii) and governed by the laws of Member States which are not party to the Geneva Convention of 7 June 1930 providing a uniform law for bills of exchange and promissory notes;

(v) paper-based vouchers;

(vi) paper-based traveller's cheques; or

(vii) paper-based postal money orders as defined by the Universal Postal Union;

(h) payment transactions carried out within a payment or securities settlement system between settlement agents, central counterparties, clearing houses and/or central banks and other participants of the system, and payment service providers, without prejudice to Article 28;

(i) payment transactions related to securities asset servicing, including dividends, income or other distributions, or redemption or sale, carried out by persons referred to in point (h) or by investment firms, credit institutions, collective investment undertakings or asset management companies providing investment services and any other entities allowed to have the custody of financial instruments;

(j) services provided by technical service providers, which support the provision of payment services, without them entering at any time into possession of the funds to be transferred, including processing and storage of data, trust and privacy protection services, data and entity authentication, information technology (IT) and communication network provision, provision and maintenance of terminals and devices used for payment services;

(k) services based on instruments that can be used to acquire goods or services only in the premises used by the issuer or under a commercial agreement with the issuer either within a limited network of service providers or for a limited range of goods or services;

(l) payment transactions executed by means of any telecommunication, digital or IT device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided that the telecommunication, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services;

(m) payment transactions carried out between payment service providers, their agents or branches for their own account;

(o) services by providers to withdraw cash by means of automated teller machines acting on behalf of one or more card issuers, which are not a party to the framework contract with the customer withdrawing 29 money from a payment account, on condition that these providers do not conduct other payment services as listed in the Annex."

15. *The point (n) is excluded from the previous list in paragraph 13 and therefore is in the scope of the Wire Transfer Regulations:*

(n) "payment transactions between a parent undertaking and its subsidiary or between subsidiaries of the same parent undertaking, without any intermediary intervention by a payment service provider other than an undertaking belonging to the same group."

16. *The Wire Transfer Regulations shall not apply to transfers of funds that represent a low risk of money laundering or terrorist financing under Article2(4)as follows:*

- *transfers of funds, that involve the payer withdrawing cash from the payer's own payment account;*
- *transfers of funds to a public authority as payment for taxes, fines or other levies within the British Islands;*
- *transfers of funds where both the payer and the payee are PSPs acting on their own behalf;*
- *transfers of funds carried out through cheque images exchanges, including truncated cheques.*

17. *By way of exception, under Article 2(3) the Regulations shall not apply to transfers of funds carried out using payment cards, electronic money instruments, mobile phones or other digital or information technology (IT) prepaid or postpaid devices with similar characteristics, where the following conditions are met:*

(a) that card, instrument or device is used exclusively to pay for goods or services; and

(b) the number of the card, instrument or device accompanies all transfers flowing from the transaction.

18. *By way of derogation, under Article 2(5), the Regulations shall not apply to transfers of funds within the British Islands to a payee's payment account permitting payment exclusively for the provision of goods and services where all of the following conditions are met:*

(a) the PSP of the payee is subject to the requirements of the Money Laundering (Jersey) Order 2008 or the Terrorism (Jersey) Law 2002 or is subject to equivalent requirements under enactments of the United Kingdom, Guernsey or the Isle of Man;

(b) the PSP of the payee is able to trace back, through the payee, by means of a unique transaction identifier, the transfer of funds from the person who has an agreement with the payee for the provision of goods or services;

(c) the amount of the transfer of funds does not exceed EUR,1000.

Guidance Notes

19. Relevant person shall have in place systems and controls (including policies and procedures) to ensure the conditions for the exemptions and derogations are met

20. PSPs and IPSPs may demonstrate compliance with the Wire Transfers Regulations if they have in place relevant systems and controls, including policies and procedures, which set out clearly:

- which criteria they use to determine whether or not their services and payment instruments fall under the scope of the Regulations;
- which of their services and payment instruments fall within the scope of the Regulations and which do not;

› which information relating to transfers of funds has to be recorded, how this information should be recorded, and where.

21. PSPs and IPSPs may demonstrate their compliance with the application of the exemption under Article 2(3) when they have procedures for identifying and documenting:

› that transfers by card, instrument or device are for goods or services, where the exemption applies, as opposed to person-to-person transfers, and

› that their systems and controls ensure that the number of the card, instrument or digital device, for example, the Primary Account Number (PAN), is provided in a way that allows the transfer to be traced back to the payer.

11.3 Outgoing Transfers - Obligations upon the PSP of the Payer

11.3.1 Transfers for Non-account Holders

Statutory Requirements

22. *Under Article 4(3), the PSP of the payer shall ensure that transfers of funds are accompanied by the following complete information on the payer and the payee:*

(a) the name of the payer;

(b) a unique transaction identifier (which can trace a transaction back to the payer); and

(c) one of either the payer's address, official personal document number, customer identification number or date and place of birth;

(d) the name of the payee; and

(e) a unique transaction identifier (which can trace a transaction back to the payee).

23. *These requirements apply to all types of transfers outside the British Islands and exceeding EUR 1, 000, whether those transfers are carried out in a single transaction or in several transactions which appear to be linked.*

24. *The 'unique transaction identifier' is defined as a combination of letters, numbers or symbols determined by the PSP, in accordance with the protocols of the payment and settlement systems or messaging systems used for the transfer of funds, which permits the traceability of the transaction back to the payer and the payee.*

25. *Under Article 5 and 6 of the Wire Transfer Regulations the following derogation applies, which allow for a reduced information to be provided:*

› *Under Article 5, where all of the PSPs involved in the payment chain are established in the British Islands, the transfer shall include at least the unique transaction identifier (which can trace a transaction back to the payer and payee) for the payer and the payee. If further information is requested by the PSP of the payee or the Intermediary PSP, such information shall be provided within three working days of the receipt of a request for such information.*

› *Under Article 6, where PSP of the payee is established outside the British Islands, transfers of funds not exceeding EUR 1,000 shall be accompanied by at least: the names of the payer and the payee and the unique transaction identifier.*

Note: For transfers of funds not exceeding EUR 1,000 the PSP of the payer need not verify the information on the payer unless the funds to be transferred have been received in cash or in anonymous electronic money, or the PSP has reasonable grounds for suspecting ML and/or FT.

11.3.2 Transfers for Account holders

Statutory Requirements

26. *Under Article 4(1) and 4(2), where a transfer of funds is made from or to an account, the PSP of the payer shall ensure that transfers of funds are accompanied by the following complete information:*

    (a) the name of the payer;

    (b) the payer's payment account number; and

    (c) one of either the payer's address, official personal document number, customer identification number or date and place of birth;

    (d) the name of the payee; and

    (e) the payee's payment account number

27. *These requirements apply to all types of transfers outside the British Islands and exceeding EUR 1,000, whether those transfers are carried out in a single transaction or in several transactions which appear to be linked.*

28. *Under Article 5 and 6 of the Wire Transfer Regulations the following derogation from the requirements of Article 4 apply:*

    › *Where all of the PSPs involved in a transfer are established in the British Islands, Article 5 of the Regulation requires that the transfer includes a payment account number of the payer and the payee. The account number could be but is not required to be, expressed as the IBAN. If further information (for example, the name and address of the payer) is requested by the PSP of the payee or the IPSP, such information shall be provided by the PSP within three working days.*

    › *Under Article 6, where PSP of the payee is established outside the British Islands, transfers of funds not exceeding EUR 1,000 that do not appear to be linked to other transfers of funds which, together with the transfer in question, exceed EUR 1 000, shall be accompanied by at least: the names of the payer and the payee and the payment account numbers of the payer and of the payee.*

    Note: For transfers of funds not exceeding EUR 1,000 the PSP of the payer need not verify the information on the payer unless the funds to be transferred have been received in cash or in anonymous electronic money, or the PSP has reasonable grounds for suspecting ML and/or FT.

AML/CFT CODES OF PRACTICE

29. In the case of a payer that is a company, a wire transfer must be accompanied by an address at which the company's business is conducted, or at which it may be contacted. In the case of a payer that is a trustee, a wire transfer must be accompanied by the address of the trustee.

Guidance Notes

30. Linked transactions are defined, at least, as those transactions that are sent from the same payment account or the same payer to the same payee and within a short time-frame, for example within six months. PSPs and IPSPs may demonstrate that they are able to detect transfers of funds that appear to be linked by reflecting all possible scenarios in their policies and procedures.

31. The exemptions for transfers within the British Islands arises from expediency, not principle, in order to accommodate transfers by domestic systems like BACS which are currently unable to include complete information. Accordingly, where the system used for a transfer within the British Islands has the functionality to carry complete information, it is considered a good practice to include it, and thereby reduce the likely incidence of inbound requests from payee PSPs for complete information.

32. The verification requirement set out in the Regulations will be met for an account holding customer of a PSP where the payer's identity has already been verified by CDD measures and is stored, in accordance with the Money Laundering (Jersey) Order 2008.

33. In order to meet the technical limitations and to manage cases with multiple account holders and different addresses, the PSP of the payer may demonstrate compliance with the Wire Transfer Regulations by documenting the priority given to the payer's information in line with law enforcement purposes to trace the payer and for sanctions screening. For example, by de-prioritising titles and full middle names, whilst prioritising the initial of the given name and the full family name and at least the country and the city of address; or for joint accounts holders to provide both names, giving priority to family name over given names.

11.3.3 Batch Files – payments either inside or outside of British Islands

Statutory Requirements

34. *Under Article 6(1), transfers of funds from a single payer to several payees that are to be sent in batch files containing individual transfers shall carry only the payment account number or the unique transaction identifier of the payer, as well as complete information on the payee, provided that the batch file contains complete information on the payer that is verified for accuracy and complete information on the payee that is fully traceable.*

35. *Where the transfer is at or below the EUR 1,000 threshold it need only include:*

    (a) the names of the payer and or payee; and

    (b) the payment account numbers of the payer and the payee or a unique transaction identifier if there is no payment account for one or both parties.

11.4 Incoming Transfers - Obligation on the PSP of the payee and IPSP

OVERVIEW

36. Under the Wire Transfer Regulations, the PSPs of the payee and IPSPs are required to implement a targeted and proportionate risk-based approach to the monitoring of incoming traffic of fund transfers, with the PSP of the payer holding responsibility for communicating all mandatory wire transfer information, which must be transmitted in the designated data fields of the payment message scheme.

37. If the required information on the payer or the payee has been provided only in part ("incomplete information") or has not been provided ("missing information"), given the potential threat of ML/TF presented by anonymous transfers, PSPs should put in place the following measures, which are proportionate to, and commensurate with the ML/TF risk to which the PSP or IPSP are exposed:

    › effective systems and controls to detect transfers of funds that lack required information, and

    › risk-based policies and procedures to determine whether to execute, reject or suspend a transfer of funds that lacks the required information.

38. Effective policies and procedures should be set up in a way that reflects a risk-based approach and document the following aspects clearly:

- which information relating to transfers of funds has to be recorded, how this information should be recorded, and where;
- which transfers of funds have to be monitored in real time and which transfers of funds can be monitored on an ex-post basis, and why;
- the obligations of members of staff where they detect a missing or incomplete information and the processes they should follow.

39. PSPs should document which high-risk factor or combination of high-risk factors are to be considered when determining the risk-based approach, for example:

- residuals risks (risk posed by the types of customers, products, services, and delivery channels);
- country risks (association with high-risk jurisdiction or relevant sanction regime);
- unusual value and volume of transactions (compare to their particular business model);
- a negative AML/CFT compliance record on the PSP of payer or the prior PSP in the payment chain.

40. PSPs and IPSPs should implement three methods of wire transfer monitoring; Real-Time Monitoring, Post-Event Monitoring, and random Post-Event Sampling. It should be determined and documented which high-risk factors, or a combination of high-risk factors, will always trigger real-time monitoring, and which will trigger a targeted ex-post review. In cases of specific concern, identified through ex-post monitoring, transfers of funds should always be monitored in real time.

41. In addition to real-time and targeted ex-post monitoring, PSPs and IPSPs should regularly perform ex-post reviews on a random sample taken from all processed transfers of funds.

11.4.1 Admissible characters or input and missing information checks

Statutory Requirements

42. *Under Article 7(1) and Article 11(1), the PSP of the payee and IPSP respectively shall implement effective procedures to detect whether the fields relating to the information on the payer and the payee in the messaging or payment and settlement system used to effect the transfer of funds have been filled in using characters or inputs admissible in accordance with the conventions of that system.*

43. *Under Article 7(2) and Article 11(2), the PSP of the payee and IPSP shall implement effective procedures, including, where appropriate, ex-post monitoring or real-time monitoring, in order to detect whether the following information on the payer or the payee is missing or incomplete.*

AML/CFT CODES OF PRACTICE

44. A PSP must subject incoming payment traffic to an appropriate level of post-event risk-based sampling to detect non-compliant payments.

Guidance Notes

45. A relevant person may demonstrate compliance with the Regulations by conducting and documenting a current risk assessment that covers the payments activities, taking into account the overall volume and jurisdictions of funds transfers and the role of all bodies involved.

46. A relevant person may assume compliance with the obligation to detect inadmissible characters and inputs, if the system's validation rules meet certain requirements, in particular, automatically prevent the sending/receiving of payments with inadmissible characters or inputs.

47. Other specific measures may be considered for a "meaningful character check". Current SWIFT standards prevent payments being received without mandatory information, but in some cases the payer and payee information fields, could include incorrect or meaningless information, such as "our client", 'my customer'', which doesn't make sense, even if this information has been provided using characters or inputs in accordance with the conventions of the messaging or payment and settlement system. Although SWIFT continues to review its validation standards to support inward monitoring and has introduced structured remitter fields (50F), however, its use is not currently mandatory. A relevant person may identify these fields by undertaking sample testing, keeping a list of commonly found meaningless terms and updating it regularly.

48. In addition to real-time and targeted ex-post monitoring, PSP and IPSP may demonstrate an appropriate level of controls by performing ex-post reviews on a random sample taken from all processed transfers of funds.

49. Other specific measures might be considered, e.g. checking, at the point of payment delivery, that payer information is compliant and meaningful on all transfers that are collected in cash by payees on a "pay on application and identification" basis.

50. Where possible, a relevant person may draw on existing policies and procedures if they designed to meet their obligations under the Regulations, subject to periodic reviews, updates, availability and training provided to all relevant members of staff, including persons responsible for processing transfers of funds.

11.4.2 Managing transfer of funds with missing information or inadmissible characters or inputs

Statutory Requirements

51. *Under Article 8(1) and Article 12(1), PSP of the payee and IPSP shall implement effective risk-based procedures, including the measure referred to in Article 3(5) of the Money Laundering (Jersey) Order 2008 for determining whether to execute, reject or suspend a transfer of funds lacking the required complete payer and payee information and for taking the appropriate follow-up action.*

52. *The PSP of the payee and IPSP should consider the most appropriate course of action on risk-sensitive basis and where the requested information is not provided by the set deadline, the PSP or IPSP should, in line with its risk-based policies and procedures:*

    (a) decide whether to reject or execute the transfer;

    (b) consider whether or not the prior PSP in the payment chain's failure to supply the required information gives rise to suspicion; and

    (c) consider the future treatment of the prior PSP in the payment chain for AML/CFT compliance purposes.

53. *Under Article 9, separate from the decision whether to execute, suspend or reject a transaction, missing or incomplete information must be considered as a factor when assessing whether a transfer of funds, or any related transaction, is suspicious and whether a disclosure is to be made under Article 34D(4) of the Proceeds of Crime (Jersey) Law 1999, Articles 21(2) of the Money Laundering (Jersey) Order 2008 or Article 21(4) of the Terrorism (Jersey) Law 2002.*

Guidance Notes

54. In order to determine whether to reject, suspend or execute a transfer of funds in compliance with Articles 8 and 12, a relevant person may consider the ML/TF risk associated with that transfer of funds and documents it, for example:

    › what ML/TF concerns the type of missing information gives rise to; and

› what high-risk indicators have been identified that may suggest that the transaction presents a high ML/TF risk or gives rise to suspicion of ML/TF;

55. A relevant person may demonstrate implementation of effective risk-based procedures and processes by documenting and recording all of its actions and the reason for its actions or inaction, including:

› making a decision on rejecting the transfer and informing the prior PSP in the payment chain of the reason for the rejection;

› making a decision on execution of the transfer and sending of a request for information, before or after crediting the payee's payment account or making the funds available to the payee

› all appropriate follow up steps taken to obtain the response, including the issuing of warnings and setting of deadlines, before either rejecting any future transfers of funds from that payment service provider or restricting or terminating its business relationship with that PSP.

11.4.3 Failure to provide information

Statutory Requirements

56. *Under Article 8(2) and Article 12(2) should the PSP repeatedly fails to provide the required information on the payer or the payee, even after warnings and deadlines, the PSP of the payee or IPSP shall take further steps by:*

› *either rejecting any future transfers of funds from that PSP, or*

› *restricting or terminating its business relationship with that PSP.*

57. *The PSP of the payee or IPSP shall report that failure, and the steps taken, to the Commission.*

Guidance Notes

58. A combination of quantitative and qualitative criteria may be used to assess PSPs as 'repeatedly failing', for example:

› the percentage of transfers with missing information sent by a specific PSP or IPSP within a certain timeframe;

› the percentage of follow-up requests that were left unanswered or were not adequately answered by a certain deadline;

› the level of cooperation of the requested PSP or IPSP relating to previous requests for missing information;

› the type of information missing.

59. The report to the Commission should be completed without delay and contain the following information such as that published in Appendix E1:

› the name of the PSP or IPSP identified as repeatedly failing to provide the required information;

› the country in which the PSP or IPSP is authorised;

› the nature of the breach, including:

› the frequency of transfers of funds with missing information,

› the period of time during which the breaches were identified and

› any reasons the PSP or IPSP may have given to justify their repeated failure to provide the required information;

› details of the steps the reporting PSP or IPSP has taken including the issuing of warnings or deadlines up until the decision to restrict or terminate the relationship was made.

60. This reporting requirement does not apply to instances where a request for the missing or incomplete information which accompanied a transfer, is fulfilled by the PSP of the payer. The obligation to report applies to circumstances where information requests are not fulfilled and the PSP of the payee invokes measures which restrict or terminate the business relationship with that PSP.

11.4.4 Additional Obligations on IPSP

Statutory Requirements

61. *In addition to the requirements of Articles 11 and 12, addressed in section 11.4 above, under Article 10 of the Wire Transfers Regulations, IPSP shall ensure that all the information received on the payer and the payee that accompanies a transfer of funds is retained with the transfer.*

Guidance Notes

62. IPSPs should satisfy themselves that their systems and controls enable them to comply with their duty to ensure that all information on the payer and the payee that accompanies a transfer of funds is retained with that transfer. As part of this, IPSPs should satisfy themselves of their system's ability to convert information into a different format without error or omission.

11.5 Reporting of Breaches

Statutory Requirements

63. *Under Article 21, PSPs shall notify the Commission of breaches of the Wire Transfer Regulations.*

64. *PSPs shall establish appropriate internal procedures for their employees, or persons in a comparable position, to report breaches internally through a secure, independent, specific and anonymous channel, proportionate to the nature and size of the PSP (Article 21(2)).*

65. *Under Regulation 3 of the Wire Transfer Regulations, a relevant person who contravenes any requirement of Articles 21(2) shall be guilty of an offence and liable to imprisonment for a term of 2 years and to a fine. This applies to all PSPs, irrespective of the capacity within which the PSP is acting.*

Guidance Notes

66. A relevant person should ensure that any failure by it to comply with the Wire Transfer Regulations is promptly reported to the Commission.

67. A relevant person should report all material failures to comply with the Regulations and any serious breaches of the PSP's policies, procedures and controls in respect of transfers of funds.

68. The report to the Commission should be completed without delay and contain the following information such as that published in Appendix E2:

› the specific provision in the Wire Transfer Regulations, which have been breached;

› the nature of the breach, including its cause;

› the date the breach was identified by the PSP; and

› where possible a summary of the measures taken by the PSP in relation to the breach and any subsequent changes to its policies, procedures and controls to mitigate against a recurrence.

69. A relevant person should establish policies and procedures for the internal reporting of breaches of the Wire Transfer Regulations and maintain a record of those breaches and action taken, ensuring sufficient confidentiality and protection for employees who report breaches committed within the relevant person.

11.6 Information, Data Protection and Record retention

Statutory Requirements

70. *Under Regulation 3 of the Wire Transfer Regulations, a relevant person who contravenes any requirement of Articles 14, 15(2) or (3), or 16 shall be guilty of an offence and liable to imprisonment for a term of 2 years and to a fine. This applies to all PSPs, irrespective of the capacity within which the PSP is acting.*

71. *PSPs shall respond fully and without delay and in accordance with the procedural requirements laid down in the national law of the Member State in which they are established, to enquiries exclusively from the authorities responsible for preventing and combating money laundering or terrorist financing of that Member State concerning the information required under this Regulation (Article 14 Provision of information).*

72. *Personal data shall be processed by payment service providers on the basis of this Regulation only for the purposes of the prevention of money laundering and terrorist financing and shall not be further processed in a way that is incompatible with those purposes. The processing of personal data on the basis of this Regulation for commercial purposes shall be prohibited (Article 15(2) Data Protection).*

73. *Payment service providers shall provide new clients with the information required pursuant to the Data Protection (Jersey) Law 2018 before establishing a business relationship or carrying out an occasional transaction. That information shall, in particular, include a general notice concerning the legal obligations of payment service providers under this Regulation when processing personal data for the purposes of the prevention of money laundering and terrorist financing (Article 15(3) Data protection).*

74. *Information on the payer and the payee shall not be retained for longer than strictly necessary. Payment service providers of the payer and of the payee shall retain records of the information referred to in Articles 4 to 7 for a period of six years (Article 16 Record retention).*

Guidance Notes

75. Within the context of the Wire Transfer Regulations, "the authorities responsible for preventing and combating money laundering or terrorist financing are to be understood as the Commission and the Jersey Police Department, including the Jersey Financial Crime Unit (the "**JFCU**").

11.7 Offences and Criminal Liability

Statutory Requirements

76. *Under Regulation 3 of the Wire Transfer Regulations, a relevant person, whether acting in the capacity of PSP of the payer, PSP of the payee or an intermediary PSP, who contravenes any requirement of the specific provisions of its Articles, which have effect in Jersey by virtue of Regulation 2, shall be guilty of an offence and liable to imprisonment for a term of 2 years, and to a fine as follows:*

- *PSP of the payer - Articles 4, 5, 6 (see section 11.3 Outgoing Transfers - Obligations upon the PSP of the Payer)*
- *PSP of the payee - Articles 7, 8, 9 (see section 11.4 Incoming Transfers - Obligation on the PSP of the payee and IPSP)*
- *IPSP - Articles 10, 11, 12 (see section 11.4 Incoming Transfers - Obligation on the PSP of the payee and IPSP)*

77. *In deciding whether a person has committed an offence under the Wire Transfer Regulations, the court shall take into account whether the person followed any relevant guidance that applies to the person and which was at the time issued, adopted or approved by the Commission under any other enactment.*

78. *A person shall not be guilty of an offence under the Wire Transfer Regulation if he or she took all reasonable steps, and exercised all due diligence, to avoid committing the offence.*

79. *Under Regulation 4(1), if an offence under these Regulations committed by a limited liability partnership, a separate limited partnership, any other partnership having separate legal personality or a body corporate is proved to have been committed with the consent or connivance of –*

    (a) a person who is a partner of the partnership, or a director, manager, secretary or other similar officers of the body corporate; or

    (b) any person purporting to act in any such capacity, the person is also guilty of the offence and liable in the same manner as the partnership or body corporate to the penalty provided for that offence.

80. *Under Regulation 4(2), if the affairs of a body corporate are managed by its members, paragraph (1) applies in relation to acts and defaults of a member in connection with the member's functions of management as if he or she were a director of the body corporate.*

13 TRUST COMPANY BUSINESS

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 through the use of italic text. The Glossary is available from the JFSC website.

13.1 Overview of Section

1. The purpose of this section is to assist with the application of customer *identification measures* where a *relevant person* establishes a business relationship or carries out a one-off transaction in the course of carrying on trust company business.

2. This section applies where a *relevant person* carries on a business under Article 2(3) of the *FS(J) Law* that involves the provision of company administration services, the provision of trustee or fiduciary services, the provision of services to foundations or the provision of services to partnerships and, in the course of providing those services, the person provides any of the services specified in Article 2(4) of the *FS(J) Law* (except any activity that is explicitly excluded from the scope of Part A of Schedule 2 of the *Proceeds of Crime Law*). Inter alia, those services are:

   - acting as, or fulfilling the function of, or arranging for another person to act as or fulfil the function of, trustee of an express trust;
   - acting as, or fulfilling the function of, or arranging for another person to act as or fulfil the function of, a partner of a partnership;
   - acting as, or fulfilling the function of, or arranging for another person to act as or fulfil the function of, director or alternate director of a company; acting as, or fulfilling the function of, or arranging for another person to act as or fulfil the function of, a member of the council of a foundation;
   - acting as a partnership formation agent, a company formation agent, or a foundation formation agent;
   - acting, or arranging for another person to act, as secretary, alternate, assistant or deputy secretary of a company;
   - providing a registered office or business address for a partnership, a company, a foundation, or for any other person; and
   - providing an accommodation, correspondence or administrative address for any person.

3. This section also applies where a *relevant person* carries on a business that is described in paragraph 8 of Part B of Schedule 2 of the *Proceeds of Crime Law*. Paragraph 8 extends the provisions that are summarised at paragraph 1 above to legal persons and legal arrangements that are not otherwise covered by the *FS(J) Law*. For the purpose of this section, such business is covered by the term "trust company business".

4. This section does **not** deal with the provision of any service to a so called "COBO-only" fund. A COBO-only fund is a scheme that would be a collective investment fund (a term that is defined in the *CIF(J) Law*) except for the fact that the capital, the collective investment of which is the object or one of the objects of the scheme or arrangement, is not acquired by means of an offer to the public of *units* for subscription, sale or exchange.

5. Activity that is excluded from the scope of Part A of Schedule 2 of the *Proceeds of Crime Law* is listed in section 1 of Part 4 of the *AML/CFT Handbook*. This list includes an individual who: (i) acts as a director in the course of employment by a trading company (that is not administered by a person carrying on trust company business); (ii) acts as a director of a company that is prudentially supervised by the *Commission* under the *Regulatory Laws*; and (iii) acts as, or fulfils the function of, a director to six or less companies.

13.2 Overview of Section

13.2.1 Obligation to Apply Identification Measures

Overview

6. Inter alia, Article 13 of the *Money Laundering Order* requires a *relevant person* to apply *identification measures*:

   › before the establishment of a business relationship or before carrying out a one-off transaction; and

   › in the course of a business relationship, where the *relevant person* has doubts about the adequacy of information previously obtained under *identification measures*.

7. A *relevant person* ("**A**") that provides, acts as or fulfils one or more of the functions listed in paragraph 1 above, or arranges for another person ("**B**") to do so (where B is an officer or employee of A) will be considered to have established a business relationship under the *Money Laundering Order*.

8. Where B is not an officer or employee of A, then A will not be considered to have established a business relationship each time that it arranges for another person to act as or fulfil such function. However, a *relevant person* will need to consider whether such an arrangement (a transaction) is a one-off transaction as defined in Article 4 of the *Money Laundering Order*.

9. A *relevant person* that acts only as a formation agent will not be considered to have established a business relationship with its customer. However, a *relevant person* will need to consider whether forming a legal arrangement or legal person (a transaction) is a one-off transaction as defined in Article 4 of the *Money Laundering Order*.

10. For the avoidance of doubt, the requirement to apply *identification measures* will apply where the relationship that a *relevant person* has with its customer is conducted through another service provider, e.g. the *relevant person* provides a director to a company that is administered by another person carrying on trust company business.

13.2.2 Information for Assessing Risk – Stage 1.4

Note: This section must be read in conjunction with, and is supplemental to, section 3.3.2 of Part 1 of the *AML/CFT Handbook*.

Overview

Limited Services

11. Section 3.3.2 of Part 1 of the *AML/CFT Handbook* explains how a *relevant person* carrying on trust company business 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 *financing of terrorism*.

12. Where a *relevant person* provides **only:**

   › registered office services; or

   › secretarial services,

or a combination of the two (hereinafter referred to as "limited services"), that *relevant person* is unlikely to have any oversight of, or control over, the activities of the legal arrangement or legal person in the way that it would if it also provided one or more directors (or equivalent) or provided full administration services. The absence of oversight or control increases the risk that a legal arrangement or legal person may be used for *money laundering* or the *financing of terrorism*.

13. The effect of this additional risk will be to require a *relevant person* to request more information on its customer, and on the activities of the legal arrangement or legal person to which it is to provide only limited services, for the purpose of countering *money laundering* and *financing of terrorism* than is strictly necessary to provide only limited services.

14. The risk that a legal arrangement or legal person may be used for *money laundering* or the *financing of terrorism* is likely to be mitigated where a customer to whom only limited services are provided is a body corporate the securities of which are listed on an *IOSCO* compliant market or on a regulated market, or where a customer is a *regulated person* (or person who carries on *equivalent business* to any category of *regulated business*).

Co-trustees and Other General Partners

15. In some cases, an express trust or limited partnership may have more than one trustee or general partner respectively. In such cases, it will be necessary for a *relevant person* that is to act as trustee or general partner to obtain information on each co-trustee or other general partner (or limited partner that participates in the management of the limited partnership) in order to consider *money laundering* and *financing of terrorism* risk.

Guidance notes

Limited Services

16. In the case of a *relevant person* that provides **only** limited services to a legal arrangement or legal person, a *relevant 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* or *financing of terrorism* where it collects (at the time that a limited service is first provided and then on an ongoing basis thereafter) information on activities by reference to:

- copies of minutes of directors' and members' meetings that must be kept by a company (including, in the case of a protected cell company, copies of minutes of directors' and members' meetings of the cell company and each of its cells) under Part 15 of the *Companies Law* (or equivalent for other legal persons or legal arrangements); and
- copies of accounts that must be prepared by the directors of a company (including, in the case of a protected cell company, copies of accounts that must be prepared by the directors of the cell company and each of its cells) under Part 16 of the *Companies Law* (or equivalent for other legal persons or legal arrangements); or
- where accounts are not required to be prepared, underlying financial records that are maintained by the directors of that company (or equivalent for other legal persons or legal arrangements).

Co-trustees and Other General Partners

17. In the case of a *relevant person* that is to act as a trustee of an express trust, a *relevant 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* or *financing of terrorism* where it collects information on any co-trustees of the trust.

18. In the case of a *relevant person* that is to act as a general partner of a limited partnership, a *relevant 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* or *financing of terrorism* where it collects information on any other general partners or limited partners that participate in the management of the limited partnership.

19. Information requested may include information about why it is necessary to have more than one trustee or general partner, and the stature and regulatory track-record of the trustee or general partner.

13.2.3 Assessment of Risk – Stage 2.1

Note: This section must be read in conjunction with, and is supplemental to, section 3.3.4 of Part 1 of the *AML/CFT Handbook*.

Overview

20. Section 3.3.4 of Part 1 of the *AML/CFT Handbook* sets out a number of factors that are to be taken into account by a *relevant person* carrying on trust company business when assessing the risk that a business relationship or one-off transaction will involve *money laundering* or *financing of terrorism*.

Guidance notes

21. A *relevant person* that carries on trust company business may demonstrate that it has assessed the risk that a business relationship or one-off transaction will involve *money laundering* or *financing of terrorism* where it also takes into account:

- Any failure on the part of a customer to be open about the *source of funds*. In the case of a trust, this could, amongst other things, indicate that a settlor is in fact a "dummy" settlor who is using another's funds, and not *his* own.
- Any failure to be open about the purpose and intended nature of the business relationship or one-off transaction. In the case of a trust, this could, for example, indicate that a settlor is withholding information on persons really intended to benefit from a discretionary trust, e.g. a settlor nominates only charities as beneficiaries of a trust, where he does not intend that the charity will in fact benefit (known as a "blind" trust).
- Any request to include unusual or non-standard clauses in a trust instrument or other constitutive document that might indicate that the disclosed purpose of the structure is not genuine.
- Any request for unusually close supervision or control of assets, other than by the *relevant person*.

13.3 Identification Measures: finding out identity and obtaining evidence

Overview

22. The meaning of *identification measures* is set out in Article 3 of the *Money Laundering Order*. Inter alia, *identification measures* are measures for identifying the customer, so the **first step** will be to determine who the customer is.

23. In the case of a *relevant person* that carries on trust company business and is to act as the trustee of an express trust, customers will include the settlor, protector (if any), beneficiaries with a vested right, any other beneficiaries and persons who are the object of a power and that have been identified as presenting a higher risk (see section 13.3.1).

24. In the case of a *relevant person* that carries on trust company business and is to act as the general partner of a limited partnership, customers will include the limited partners of the partnership (see section 13.3.4).

25. In the case of a *relevant person* that carries on trust company business and is to provide a service, e.g. registered office, in respect of a limited partnership, the customer will be the general partner acting for the limited partnership – a third party (see section 4.4.3 of Part 1 of the *AML/CFT Handbook*).

26. In the case of a *relevant person* that carries on trust company business and is to provide a service to a company, the customer will be the company (see section 4.5.1 of Part 1 of the *AML/CFT Handbook*).

27. In the case of a *relevant person* that carries on trust company business and is to provide a service to a foundation, the customer will be the foundation (see section 4.5.3 of Part 1 of the *AML/CFT Handbook*).

28. In the case of a *relevant person* that carries on trust company business and is to provide a service to a separate limited partnership, incorporated limited partnership or limited liability partnership, the customer will be the partnership (see section 4.5.5 of Part 1 of the *AML/CFT Handbook*).

29. In the case of a *relevant person* that carries on trust company business and is to form a company, partnership or foundation, the customer will be the persons who are to be the beneficial owners and controllers of the legal person (see section 4.3.1 and 4.5 of Part 1 of the *AML/CFT Handbook*).

13.3.1 Finding Out Identity – legal arrangement that is a trust

Guidance notes

30. A *relevant person* that is to act as trustee of an express trust may demonstrate that it has applied *identification measures* under Article 3(2)(a) of the *Money Laundering Order* to its customer, where it applies those measures to:

- the settlor (including any person subsequently settling funds into the trust) (except if deceased) and any person who directly or indirectly provides trust property or makes a testamentary disposition on trust or to the trust.
- any co-trustee;
- any protector;
- any beneficiary with a vested right;
- any other beneficiary or person who is the object of a power and that has been identified as presenting a higher risk; and
- any other person exercising ultimate effective control over the trust.

31. In any case where a settlor, protector, beneficiary, object of a power or other person referred to in paragraph 30 (the "**person**") is not an individual, a *relevant person* may demonstrate that it has identified each individual who is the person's beneficial owner or controller under Article 3(2)(c)(iii) of the *Money Laundering Order* where it has identified:

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

- To the extent that there is doubt as to whether the individuals exercising control through ownership are beneficial owners, or where no individual exerts control through ownership, any other individual exercising **control** of the person **through other means**.
- Where no individual is otherwise identified under this section, individuals who **exercise control** of the person **through positions held** (who have and exercise strategic decision-taking powers or have and exercise executive control through senior management positions).

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

13.3.2 Finding Out Identity – legal arrangement that is a charitable trust (capital markets)

Guidance notes

33. A *relevant person* that is to act as the trustee of a charitable trust which is established to hold an investment in a security-issuing vehicle, or to hold security (as bare trustee for security-holders) over assets held within such a vehicle, may demonstrate that it has applied *identification measures* under Article 3(2)(a) of the *Money Laundering Order* to its customer, where it applies those measures to:

- the originator or instigator of the capital market transaction; and
- each security-holder that is able to exercise effective control over the underlying security-issuing vehicle.

13.3.3 Obtaining Evidence of Identity - legal arrangement that is a trust

Overview

34. 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.

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

AML/CFT Codes of Practice

36. 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 of the *Commission*.

13.3.4 Finding Out Identity – legal arrangement that is a limited partnership

Guidance notes

37. A *relevant person* that is to act as the general partner of a limited partnership may demonstrate that it has applied *identification measures* under Article 3(2)(a) of the *Money Laundering Order* to its customer where it applies those measures to limited partners holding a **material controlling ownership interest** in the capital of the partnership (through holdings of interests or voting rights) or any other person exercising **control through other ownership**

means, e.g. partnership agreements, power to appoint senior management, or any outstanding debt that is convertible into voting rights.

38. 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 *relevant person* that is to act as the general partner of a limited partnership may demonstrate that it has applied *identification measures* under Article 3(2)(a) of the *Money Laundering Order* to its customer where it applies those measures to any other person exercising **control** over the partnership **through other means**, e.g. those who exert control through personal connections, by participating in financing, because of close and intimate family relationships, historical or contractual associations or as a result of default on certain payments.

39. Where no person is identified under this section, a *relevant person* that is to act as the general partner of a limited partnership may demonstrate that it has applied *identification measures* under Article 3(2)(a) of the *Money Laundering Order* to its customer where it applies those measures to persons who exercise **control through positions held** (who have or exercise strategic decision-taking powers or have or exercise executive control through senior management positions, e.g. general partner or limited partner that participates in management).

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

- Each individual with a **material controlling ownership interest** in the capital of the partnership (through direct or indirect holdings of interests or voting rights) or who exerts **control through other ownership means**.
- To the extent that there is doubt as to whether the individuals exercising control through ownership are beneficial owners, or where no individual exerts control through ownership, any other individual exercising **control over the partnership through other means**.
- Where no individual is otherwise identified under this section, individuals who exercise **control** of the partnership **through positions held** (who have and exercise strategic decision-taking powers or have or exercise executive control through senior management positions).

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

13.3.5 Obtaining Evidence of Identity - legal arrangement that is a limited partnership

Overview

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

AML/CFT Codes of Practice

43. 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 of the *Commission*.

13.3.6 Finding out Identity - legal person that is a protected cell company

Note: This section must be read in conjunction with, and is supplemental to, sections 4.5.1 and 4.5.2 of Part 1 of the *AML/CFT Handbook*.

Overview

44. Under Article 127YDA(1) of the *Companies Law*, in the case of both *PCCs* and *ICCs*, a cell shall have the same registered office and secretary as the cell company, and the registered office must be in Jersey.

45. Where a *relevant person* carrying on trust company business provides a registered office or secretary to a *PCC*; **it will also do so for each cell of that *PCC***. Because the cell of a *PCC* does not have the ability to enter into arrangements or contract in its own name, for the purposes of Article 3 of the *Money Laundering Order*, the *PCC* will be taken to be a customer acting for a third party and each cell will be taken to be a third party that is a person other than an individual. It follows that *identification measures* must be applied under Article 13 of the *Money Laundering Order* to the *PCC* (the customer) and **each cell** of the *PCC* (a third party).

13.3.7 Finding Out Identity - legal person that is a private trust company

Overview

46. Schedule 2 of the *Proceeds of Crime Law* provides that a private trust company (a "**PTC**") - a company the purpose of which is to provide trust company business services in respect of a specific trust or trusts or foundation or foundations, that does not solicit from or provide trust company business services to the public, and the administration of which is carried out by a person that is registered to carry on trust company business - is not subject to the *Money Laundering Order*.

47. The basis for this concession is that *CDD* measures will be applied by the person that is registered to carry on trust company business (a *relevant person*) to the specific trust or trusts that are serviced by the PTC - in line with Article 13 of the *Money Laundering Order* - since the PTC is administered by the *relevant person*.

48. A *relevant person* will consider the PTC to be its customer and each of the trusts to be third parties (which are not a person).

AML/CFT Codes of Practice

49. A *relevant person* that administers a PTC must apply *CDD* measures, record-keeping and reporting requirements to that PTC in line with the *Money Laundering Order*.

13.4 Timing of Identification Measures

Note: This section must be read in conjunction with, and is supplemental to, section 4.7 of Part 1 of the *AML/CFT Handbook*.

Overview

50. In line with Article 13(8) of the *Money Laundering Order*, a *relevant person* that is to act as trustee may delay obtaining evidence of the identity of a customer after the time that a business relationship is established so long as:

- 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 *financing of terrorism* occurring as a result of obtaining evidence after entitlement is conferred.

51. Similar provisions should apply in a case where the customer of a *relevant person* that is a trustee changes during a business relationship.

Guidance notes

52. During a business relationship, a *relevant person* that is the trustee of an express trust may demonstrate that it has obtained evidence that is reasonably capable of verifying the identity of each beneficiary with a vested right where:

› it 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 *financing of terrorism* occurring as a result of obtaining evidence after entitlement is conferred.

53. During a business relationship, a *relevant person* that is the trustee of an express trust may demonstrate that it has obtained evidence that is reasonably capable of verifying the identity of a beneficiary or person who is the object of a trust power where it does so at the time that the person is identified as presenting a higher risk.

13.5 Failure to Complete Identification Measures

Note: This section must be read in conjunction with, and is supplemental to, section 4.8 of Part 1 of the *AML/CFT Handbook*.

Overview

54. Under Article 14 of the *Money Laundering Order*, if a *relevant person* is unable to apply *identification measures* when required to do so then it must terminate that relationship and consider whether to make a *SAR* to the *JFCU*.

55. Such a requirement can be problematic in the case of a *relevant person* that is a trustee where its customer is the beneficiary or object of a power of a trust and where:

› the relationship between a *relevant person* and its customer is governed by other legislation - e.g. the Trusts (Jersey) Law 1984; and

› the termination of a relationship with a customer (a beneficiary or object of a power) may have a prejudicial effect on the interests of other customers.

56. Such a requirement can also be problematic in the case of a *relevant person* that is a council member where its customer is a foundation and the foundation is governed by the *Foundations Law*. In particular, under Article 12(3) of the *Foundations Law*, the retirement or removal of the qualified member of a foundation does not take effect until immediately before the appointment of a new qualified person to be the qualified member of the council has taken effect.

57. In order to address such tension, termination of a business relationship may be **delayed** until such time as compliance with Article 14 of the *Money Laundering Order* does not conflict with another legal requirement, and/or does not have any prejudicial effect on the interests of other customers, so long as the risk of *money laundering* or *financing of terrorism* is effectively managed.

14. FUNDS AND FUND OPERATORS

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 through the use of italic text. The Glossary is available from the JFSC website.

14.1 Overview of section- scope

1. This section must be read in conjunction with, and is supplemental to the other sections of the *AML/CFT Handbook*[1]. All references to Articles are to Articles of the *Money Laundering Order* unless otherwise stated.

2. The purpose of this section is to assist with the application of customer due diligence, the conduct of Risk Assessments and additional *AML/CFT* requirements by funds and fund operators. The definition of *financial services business* in the *Proceeds of Crime Law* means that both regulated and prudentially supervised funds and fund operators are subject to the same statutory requirements in the *Money Laundering Order* as unregulated funds and fund operators. To be clear this section applies to funds and fund operators as set out below:

3. **Funds**

Type of Fund[2]	**Proceeds of Crime Law Schedule 2**
Recognized funds under the *CIF(J) Law*	Part A paragraph 3(1)(b)
Unclassified funds (not just Jersey Certified Funds but also non domiciled funds that are *relevant persons*) under the *CIF(J) Law*	Part A paragraph 3(1)(c)
Unregulated funds under the Collective Investment Funds (Unregulated Funds) (Jersey) Order 2008	Part B paragraph 6
CoBO funds (meaning CoBO-Only funds, Private Placement Funds (**PPFs**), Jersey Private Funds and very private funds) all under the Control of Borrowing (Jersey) Order 1958 (**CoBO**) (not just Jersey CoBO funds but also non domiciled funds that are *relevant persons*)	Part B paragraphs 7(1)(h) and (n)

For the purposes of the above table and this section:

---

1 All Guidance applies to *relevant persons* whether they are regulated or not as per Part 1: Section 1.3, particularly paragraph 27.

2 There are no statutory exemptions for Funds, except (and subject to certain requirements) a non-domiciled company that is a Collective Investment Fund. See the *AML/CFT Handbook* Part 4 Section 1 Proceeds of Crime Schedule 2

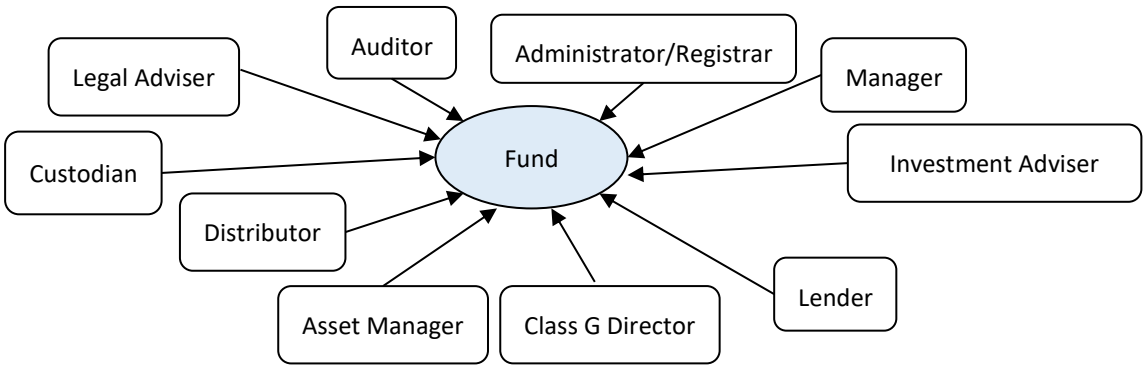
- References to a Fund include all sub funds and constituent parts of the Fund, e.g., those constituent parts of a fund referred to in a Certificate issued to the Jersey Certified Fund.
- An example of a non-domiciled public fund that will be issued with a Certified Fund certificate and that is also a *relevant person* is a non-Jersey company with an established place of business in Jersey.

4. **Fund Operators**

Type of Fund Operator[3]	**Proceeds of Crime Law Schedule 2**
Functionary of recognized fund under the *CIF(J) Law*	Part A paragraph 3(1)(a)
Fund Services Business under the *FS(J) Law*	Part A paragraph 4
Those providing services related to CoBO funds (meaning CoBO-Only funds, PPFs), Jersey Private Funds and very private funds)	Part A paragraph 4 – such as carrying on: › trust company business i.e. acting as partner/trustee or providing a director › investment business Part B paragraphs 7(1)(h), (k), (l), (m) or (n)
Guidance will also be relevant for other entities providing services to a fund that fall within the activities listed in Schedule 2. See paragraph 6 below.	

5. Every *relevant person* has obligations pursuant to the *Money Laundering Order*. Where there are a number of different Fund Operators involved in a Fund structure their respective *CDD* obligations and subsequent *CDD* measures applied may differ. The differences may be attributable to different roles, risk appetites and risk assessments, which will determine how they fulfil their *AML/CFT* obligations.

6. The reference to *financial services businesses* in the *Proceeds of Crime Law* means *relevant persons* under the *Money Laundering Order* includes more entities than those entities defined as financial service businesses in the *FS(J) Law*. Fund Operators can include all those entities and activities listed in Schedule 2 Part A and Part B of the *Proceeds of Crime Law*. The diagram below shows an example of some of the entities (there are others) that may be *relevant persons* with the Fund as their customer:



[3] There are some statutory exemptions for activities that would otherwise be *Fund Operators.* See the AML/CFT Handbook Part 4 Section 1 Proceeds of Crime Schedule 2

7. Natural Persons such as Class G Directors regulated under the *FS(J) Law* are *relevant persons* and will also have *AML/CFT* obligations. The *Commission* has produced the guidance note "Natural Persons carrying on a Single Class of Trust Company Business"[4].

8. An entity that is a Managed Entity[5] has the same *AML/CFT* obligations as any other Fund Operator.

9. Funds and Fund Operators may have different *AML/CFT* obligations. For example, any one of the Fund Operators in the diagram above may be neither a Jersey body corporate nor carrying on business in or from within Jersey and so will not be a *relevant person* and will not be subject to Jersey *AML/CFT* obligations. A Fund and/or Fund Operator that is not a *relevant person* may have *AML/CFT* obligations in another jurisdiction. A Non Jersey Fund Operator that is not subject to Jersey *AML/CFT* obligations may act for a Jersey Fund, such as a Jersey Fund Company, that does have Jersey *AML/CFT* obligations.

14.2 AML/CFT risk assessments

14.2.1 Overview: obligation to conduct risk assessments

Note: This section must be read in conjunction with, and is supplemental to Part 1: Section 2.3 of the *AML/CFT Handbook* regarding Business Risk Assessments and Part 1: Section 3.3.2 regarding Customer Risk Assessments.

10. A *relevant person* (see table below for example) must prepare an assessment of its exposure to *money laundering* and *financing of terrorism* risk – "the *Business Risk Assessment*" (*BRA*) and an assessment of the risk that a business relationship or one-off transaction will involve *money laundering* or *financing of terrorism* risk – "the *Customer Risk Assessment*" (*CRA*) for each of its customers. References to *CRA* and *BRA* in this section are to those prepared to meet *AML/CFT* obligations. It is important to make the distinction between a *BRA* and a *CRA* as they are separate statutory requirements. For example:

relevant person	BRA[6]	CRA[7]
Administrator	Administrator's Business	Funds for which the administrator acts
Fund	Fund itself	Investors

11. All the *financial services businesses* defined by the *Proceeds of Crime Law* that are *relevant persons* under the *Money Laundering Order* must conduct a *BRA* and individual *CRAs*. Where

[4] Available from the *Commission* website at: https://www.jerseyfsc.org/industry/guidance-and-policy/natural-persons-carrying-on-a-single-class-of-trust-company-business/

[5] Means an entity that is managed by a Manager of a Managed Entity with class ZK of Fund Services Business as described in Guidance Note for a Manager of a Managed Entity (a "MoME") and Certain Managed Entities (as may be amended by the *Commission*, from time to time). https://www.jerseyfsc.org/industry/guidance-and-policy/manager-of-a-managed-entity-and-certain-managed-entities/

[6] Article 11(1)(f) of the *Money Laundering Order*. (Handbook Part 1: Section 2.3: Corporate Governance).

[7] Articles 13 and 3(5) of the *Money Laundering Order*. (Handbook Part 1: Section 3.3.2 Identification Measures).

the conducting of a *BRA*/*CRA* is outsourced to an external party, the *relevant person* must take adequate steps to ensure the *BRA* and *CRA* are properly conducted and documented.

Guidance Notes

12. For Fund Operators who are subject to a relevant regulatory code of practice[8] there is also an obligation for a wider, operational business risk assessment to be conducted. When preparing a *BRA* or *CRA*, factors in this operational business risk assessment may be relevant. Therefore, a combined *BRA* and operational business risk assessment may be appropriate.

13. Risks that are not normally considered to be specific *AML/CFT* risks may also be relevant to a *BRA*; for example, credit risk, tax risk, investor eligibility risk, cyber security etc.

14. It is common practice for a Fund to outsource the conduct of its *BRA* to an administrator. In such circumstances, the administrator will also need to conduct a *CRA* on the Fund (its customer) as it has two separate roles - acting both for itself (conducting a *BRA* on itself and *CRA* on the Fund) and as delegate for the Fund (conducting a *BRA* and *CRA* on behalf of the Fund). Although there may be similar factors considered in the *BRA* and the *CRA*, separate assessments will need to be conducted and documented.

15. It is likely that the *BRA* will be conducted by the *relevant person* prior to any *CRA*. When *CRA's* are prepared the *BRA* may need to be updated (for example, to take into account new risk factors or the Board's changing risk tolerance/appetite). The Board may demonstrate that its *BRA* is kept up to date where it is reviewed when events (internal and external) occur that may materially change the *money laundering* and *financing of terrorism* risk.

16. Risk should not simply be "averaged out" (e.g. two low risk factors and one high risk factor does not necessarily lead to a medium risk rating). Each identified risk should be appropriately identified, assessed and mitigated. Similarly, the mitigation of risk does not necessarily lead to a low risk rating.

17. Where high risk elements are present in a collection of lower risk elements, care should be taken that all risks are appropriately dealt with. There may be individual higher risk elements within a lower/medium risk customer - in such circumstances care should be taken that there is sufficient mitigation in place for the higher risk element.

18. *BRAs* and *CRAs* should also consider the cumulative effect of risks identified, which may exceed the sum of each individual risk element.

14.2.2 Business Risk Assessment

Note: This section must be read in conjunction with, and is supplemental to Part 1: Section 2.3 of the *AML/CFT Handbook* regarding *BRAs*.

Overview

19. The purpose of the *BRA* is to consider a *relevant person's* exposure to *money laundering* and *financing of terrorism* risk and to enable the *relevant person* to put in place *policies and procedures* to deal with those risks.

[8] means, collectively, the, Code of Practice for Deposit-taking Business, the Code of Practice for Fund Services Business, the Code of Practice for General Insurance Mediation Business, the Code of Practice for Insurance Business; the Code of Practice for Investment Business; the Code of Practice for Money Service Business and the Code of Practice for Trust Company Business.

Guidance Notes

20. When conducting a *BRA* care should be taken not to focus on any single factor. All factors (including any identified by a National Risk Assessment or similar), as well as the wider picture (and cumulative risk) should be considered. There may be a number of parties involved in the creation of a Fund and the conduct of the fund business – in such circumstances, the *AML/CFT* risks arising from the involvement of all parties will need to be considered. Below are some potential factors[9] in a Fund *BRA* that could be considered, this list is not exhaustive and the *relevant person* needs to consider the risks relevant to them.

21. *Money laundering* is defined in Part 1: Section 1. Has sufficient information been obtained in relation to a fund structure to fully understand the structure and manage the risk of being involved with the proceeds of criminal conduct? This may include the fund itself being set up for a fraudulent purpose or the fund being used to facilitate *money laundering*. Not all of these potential factors will be applicable in every case (e.g. there may be no external finance).

22. Potential factors to consider when conducting a Fund *BRA*:

Fund	
Type of Fund	› Open/closed › Public/private › Regulated/unregulated › Listed/ unlisted › Asset Class - Private equity / venture capital / property / hedge fund / fund of funds
Rationale for Fund	› Does fund proposal make sense in light of the objective? › Capital accumulation / income producing / both
Jurisdiction/Domicile of Fund	› Local / Non-domiciled
Fund Structure	› Legal Structure: Limited partnership / company / unit trust / incorporated cell company / protected cell company / incorporated limited partnership / separate limited partnership? › Separate governing body i.e. general partner/trustee › Complex / Simple › Special Purpose Vehicles (*SPVs*) to hold assets › Part of Fund Manager's Platform › Umbrella
Conflicts of Interest	› Promoter v Fund investors › Fund Operators v Fund investors › Related parties v Fund Investors › Between Investors (Evidenced in some cases by Side Letters) › Between Fund Operators

[9] In this Section of the *AML/CFT Handbook* a Risk Factor is a circumstance, fact or influence to take into consideration which may contribute to the assessment of risk.

Fund	
Unusual Features	› Lock ins › Asset holding arrangements › In specie contributions
Influential Persons	› The entities named in the diagram at paragraph 6 › Promoter › Investment Committee – powers, composition, independence › Consultants –value for money, related? › Valuers – independent? › Suppliers › *SPV* level suppliers › Letting agents › Asset managers › Developers › Legal advisers › Tax advisers › Auditors › Co-investors › Key investors/Seed investors
Risk Indicators	› *PEP*s › High Risk Jurisdictions › Sanctions- check the lists
Cash flow	› In specie payments/redemptions permitted › Third party payments permitted › Early redemptions permitted › Budgetary and payment controls of monies flowing out of fund

23.

Investors / Target Market	
Type	› Retail › Professional / Sophisticated › Institutional › Co-investors at fund level or at investment level (see paragraph 30 below)
Method of Distribution/ Solicitation.	› Word of mouth / club arrangement / reverse solicitation / private distribution / public distribution › Control of raising money and distribution of securities › Distributor employed › Promoter distributes › In house fund (i.e. Bank for high net worth clients)

Investors / Target Market	
	› Investment Adviser distributes › Subject to local marketing requirements e.g. AIFMD?
Investor's Holding Method	› Via intermediaries › Via nominee › Directly/indirectly › Complexity of holding structure › Rationale for holding structure
Investor information	› *Source of funds* › *Source of wealth* › Rationale

24.

Investments	
Type / Asset Class	› Property / private equity / hedge fund / fund of funds / Infrastructure etc › Liquid/illiquid assets
Listed / Unlisted	› Recognised market?
Risks associated with that Asset Class	› Diamonds / gold / luxury goods – higher *AML/CFT* risk › Have Fund and Fund Operators sufficient knowledge and competence to deal with the asset class?
Valuation	› Listed assets easier to value › Specialist assets may be difficult to value › Independent Valuer - Experts linked already to the fund?
In Specie receipt/payment	› Valuation › Title transfer effective? › Liquid/ illiquid › Related party transferring the asset?
Sanctions	› Check the lists

25.

Common to *Fund Operators *Governing Body *Finance Provider * Investors / Target Market *Instigator / Promoter / Creator	
Stature	› Public / Private › Newly established / long established › Listed / unlisted › Global / local / number of jurisdictions / number of offices

Common to *Fund Operators *Governing Body *Finance Provider * Investors / Target Market *Instigator / Promoter / Creator	
Legal Form	› Legal person / legal arrangement
Ownership and Control	› Wide spread of ownership / control or sole ownership › Dominant directors / shareholders
Regulatory Status	› Regulated / unregulated
Reputation	› Subject to regulatory or other disciplinary actions › Subject to legal action › International / national reputation › Held in high regard in business community
Track Record	› Relevant experience particularly in the case of specialist funds or those perceived to be high risk, for example, futures and options funds.
Jurisdiction	› Local / non-domiciled › Multiple jurisdictional operations › Multiple branches / regional office
Solvency	› Insolvency proceedings › Judgements › Issues with accounts (Audit) › Lack of liquidity
Risk Indicators	› *PEPs* - Are there are any? › Sanctions - Have they been checked? › High Risk Jurisdictions – are there links?

26.

Instigator / Promoter / Creator	
Control of Fund	› Participation in structure – owns management shares, owns governing body, is investment manager /adviser/ directors on board of governing body

27.

Fund Operators	
General	› Risks in relation to fund operator role or that particular fund operator › Sub outsourcing

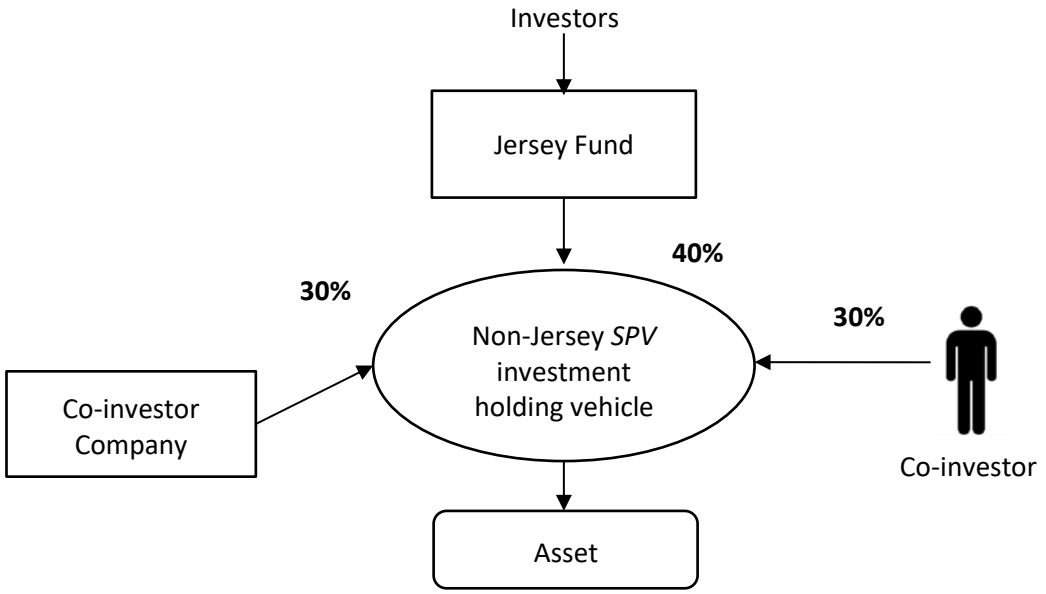
28.

Governing Body	
Control	› Independent / equal / proportionate / dominant individuals › Bank Account Mandates
Corporate Governance	› Compliance Culture, compliance monitoring policy › Frequency that Policy and Procedures are updated

29.

Finance	
Source of borrowing	› Regulated Bank / credit institution › Private finance – where are funds from? › Layers of borrowing- how many lenders? › Related party?
Structure	› Loan › Bond › Ring fencing › Priority
Security	› Secured/unsecured › Collateral › Limited recourse › Guarantor › Take title › Can lender deal with the asset it is holding as security?.
Level of borrowing	› Fund › *SPV*
Rationale	› Make sense? › Normal commercial terms? › Unusual features?
Onward Lending	› Why? › Who to? › Benefit to the Fund?

30. An example of a factor to consider in a Fund *BRA* is the existence of Co-investors, see below:



31. The non-Jersey *SPV* investment holding vehicle is not a *relevant person* so has no Jersey *AML/CFT* obligations.

32. The Fund's *BRA* should consider the *AML/CFT* risks arising from the existence of the Co-investors in the structure. This may include (and this list is not exhaustive) connections to a jurisdiction listed on Appendix D2 or whether the Co-investor or the ultimate beneficial owner of the Co-investor company is a *PEP*. Sufficient information should be obtained to assess the *AML/CFT* risks in this aspect of the business.

14.2.3 Customer Risk Assessment – risk indicators

Note: This section must be read in conjunction with, and is supplemental to Part 1: Section 3.3.4 of the *AML/CFT Handbook*.

33. The lists below are indicators only and are not exhaustive. The results of any National Risk Assessment or similar must also be taken into account. The presence of one or more low or high risk indicators does not necessarily mean a customer is low or high risk and their rating needs to be assessed on a case by case basis. Risk will be assessed on initial take-on of a customer but will also need to be reviewed to ensure the risk rating remains appropriate.

34. Potential Higher Risk Indicators[10] on take-on of a customer (Fund or investor)[11].

Where the customer:

› has provided information/documentation that cannot be verified

[10] In this Section of the *AML/CFT Handbook* a Higher Risk Indicator may indicate *money laundering* or *financing of terrorism* based on a *relevant person's* understanding of its business, its products and its customers (i.e. the outcome of its business risk assessment – Part 1: Section 2.3.1) and may contribute to the risk rating.

[11] Consideration may also need to be given as to whether it is appropriate to take-on the Customer at all and whether a *SAR* should be submitted.

- has links to a *PEP*
- has links to a higher risk jurisdiction[12]
- is evasive / inconsistent when additional information is requested such as regarding identity of beneficial owners / *source of funds* / purpose and expected transactions
- has a complex structure, for example, operates via layers of representatives making identification difficult
- is revealed to have money problems (i.e. debt judgements)
- is the subject of regulatory or criminal actions or has associates with these characteristics
- acts as a nominee and there is an unwillingness to identify the underlying third party
- is a Non-Profit Organisation / Charity that might be susceptible to abuse regarding terrorist activities such as medical and emergency relief charities with an unlimited global scope. Or where a Non-Profit Organisation / Charity operates in a specific geographical area but then transfers monies to a country / territory / jurisdiction not within the specific geographical area
- is a Fund and:
    a. is aiming to invest in products that may be susceptible to *money laundering*, for example diamonds and gold.
    b. has a one off minimum investment amount so that it operates below AML reporting threshold amounts.
    c. is a highly liquid open-ended Fund (the customer) with the possibility of frequent subscriptions and redemptions.
    d. uses unregulated fund operators
    e. outsources functions without any valid reasons provided
    f. has a complex structure so it is difficult to ascertain who the underlying beneficiary is, for example using many *SPV*s and intermediaries

35. Potential Higher Risk Indicators that may be flagged during ongoing monitoring of the customer (Fund or investor).

    Where the Fund:

- has entered or intends to enter into finance arrangements that are either at a higher rate or lower rate than usual with no rationale provided
- has or intends to purchase assets without independent valuations (particularly from connected persons)
- receives or sends monies to related or unrelated third parties that do not fit the pattern of transactions expected for the Fund and no acceptable rationale is provided
- transfers monies to *SPV*s which the Fund customer appears to have no control over
- purchases assets without proof of title from the seller and title to the assets is not clearly transferred to the Fund customer

[12] Appendix D2:
https://www.jerseyfsc.org/industry/financial-crime/aml-cft-handbooks/aml-cft-handbook-for-regulated-financial-services-business/

- engages consultants who add little benefit and receive high fees (particularly in countries associated with a higher risk of corruption)
- enters into a promise to purchase agreements for which monies are paid where transactions are regularly aborted, resulting in forfeiture of the monies
- is investing with no obvious commercial rationale and is inconsistent with the Fund customer profile
- regularly pays fees, commissions and costs to source and investigate transactions, but no transactions are executed
- exhibits transaction activity that does not follow the expected pattern or changes substantively with no rational explanation
- displays endemic conflicts of interest
- regularly changes bank accounts and uses different Fund Operators in different jurisdictions

Where the investor:

- requires a high level of liquidity and indicates funds may need to be withdrawn / moved at short notice
- is proposing an investment of an unexpected large amount

14.2.4 Risk assessments for SPV governing bodies

36. An *SPV* Governing Body is a vehicle established for the specific purpose of acting as the governing body of a Fund. Common examples are a company established to act as the general partner of a limited partnership Fund or a trustee of a unit trust Fund.

37. A unit trust or a limited partnership has no separate legal personality, so the *SPV* Governing Body is considered to be the "customer" of the Fund Operator (Article 3(2)(a) and (c)). However, trustees and general partners are also Fund Operators. Effectively they have two capacities - they are both Fund Operator and Fund governing body. For the purposes of this section if a trustee or general partner provides services to **more than one** Fund it will not be regarded as an *SPV* but will be regarded as a Fund Operator.

38. In these circumstances, its *BRA* and *CRA* (as Fund Operator) and the *BRA* it conducts in its capacity as *SPV* Governing Body of the Fund are likely to significantly overlap. In order to avoid duplication of effort, it may be appropriate to consolidate these 3 Risk Assessments, provided that all relevant risks (i.e. of all 3 risk assessments) are appropriately considered.

39. This has no effect on the separate obligation of the Fund to conduct a *CRA* on each of its customers, i.e. the investors.

<table>
<tr><th>Entity</th><th>BRA</th><th>CRA</th><th>Entity</th><th>BRA</th><th>CRA</th></tr>
<tr><td>Non SPV Trustee of Unit Trust Funds</td><td>Self</td><td>Fund</td><td>SPV Trustee of one Unit Trust Fund</td><td colspan="2" rowspan="2">Consolidated Risk Assessment
Combined BRA/CRA for Trustee and Fund BRA as SPV Trustee is intrinsically part of the Fund.</td></tr>
<tr><td>Unit Trust</td><td>Self</td><td>Investors</td><td>Unit Trust</td><td>Investors</td></tr>
</table>

14.2.5 Documenting risk assessments

Note: This section must be read in conjunction with, and is supplemental to Part 1: Section 3, paragraph 23 and Part 1: Section 2 paragraph 10 of the *AML/CFT Handbook.*

Overview

40. *BRAs* and *CRAs* must be properly documented.

Guidance Notes

41. Comprehensive subscription agreements / investor questionnaires may assist in obtaining information on a Fund's investors and provide sufficient detail to enable the Fund to carry out a *CRA*. However, a subscription agreement / investor questionnaire is not a *CRA*.

42. For certain types of products or services, standard customer profiles may assist the *CRA* process. In such cases, the *relevant person* will need documented procedures which consider:

- whether the intention is to only accept investors who fit the standard customer profile
- if not, how will exceptions to the standard customer profile be managed; either at the outset or subsequently?
- whether (for instance) individual *CRAs* will be conducted with respect to any customers that do not fit the standard customer profile.

43. The *relevant person* always remains ultimately responsible for its Risk Assessments regardless of whether they outsource the conduct of them.

14.3 Customer identification measures

Overview

44. Part 1: Section 3 of the *AML/CFT Handbook* describes the stages of the identification process and provides guidance in relation to each stage. Customer due diligence is not limited to finding out the identity of the customer and obtaining verification (e.g. taking their personal details and copies of their passport and driving licence). The table below summarises *CDD* requirements:

<table>
<tr><td rowspan="8">*CDD*</td><td rowspan="6">*Identification measures*</td><td colspan="3">Risk assessment</td></tr>
<tr><td colspan="3">ID customer</td></tr>
<tr><td colspan="3">ID Third parties</td></tr>
<tr><td colspan="2">ID person acting for customer</td><td>Verify authority to act</td></tr>
<tr><td rowspan="2">Where customer not individual:</td><td colspan="2">Understand Ownership / control structure</td></tr>
<tr><td colspan="2">ID Beneficial Owners / Controllers</td></tr>
<tr><td colspan="3">Obtain information on purpose / nature</td></tr>
<tr><td rowspan="2">On-going monitoring</td><td colspan="3">Scrutinising transactions / activity</td></tr>
<tr><td colspan="3">Keep documents / information up-to-date</td></tr>
</table>

45. The following sections provide guidance on the identification of customers, ultimate beneficial owners and third parties. These sections must be read in conjunction with relevant sections of the *AML/CFT Handbook*.

14.3.1 Obligation to apply identification measures.

Overview- Fund

46. Part 1: Section 3.1 paragraph 5 of the *AML/CFT Handbook* states a customer may be an individual (or a group of individuals) or a legal person. Further guidance on finding out of identity and obtaining evidence of identity is provided as follows:

AML/CFT Handbook Section	Type of Customer	Fund Structure
4.3	Individual / Group of Individuals.	
4.5	Legal Person	› Company, › Limited Liability Partnership, › Separate Limited Partnership, › Incorporated Cell
4.4	Individual or legal person acting for a legal arrangement.	› Trustee on behalf of a Unit Trust › General Partner on behalf of a Limited Partnership

47. For the purposes of this section, company, limited partnership and unit trust will be used as practical examples, as these are the most common Fund structures.

48. Each of the Fund's investors are its customers. The investors may take a variety of legal forms and Article 3 specifies how *identification measures* are applied to each.

Fund Structure	relevant person re each Fund structure	Customer/Investor
Company	Company	› Article 3(2)(a) individual › Article 3(2)(aa) any person acting on behalf of the customer › Article 3(2)(b) acting for a third party (legal arrangement) › Article 3(2)(c) not an individual but legal person. To Legal Persons / Arrangements apply the Three Tier Test[13].
Limited Partnership	General Partner on behalf of the Limited Partnership	
Unit Trust	Trustee on behalf of the Unit Trust	

[13] 1 The Three Tier Test refers to the process by which a *relevant person* may demonstrate that it has identified each individual who is a beneficial owner or controller: See Part 1: Section 4 page 10 onwards.

2. The Three Tier Test is often summarised as control through 1) ownership means and 2) other means; or 3) through positions held. When applying the Three Tier Test, if no one is identified at Tiers 1 and / or 2 then consider Tier 3. There may be more than 1 individual identified at Tiers 1 and/or 2.

49. The table at Part 1: Section 3.3 paragraph 23 sets out the identification process, of which identifying the customer is only a part. A *relevant person* must also understand the ownership and control of the customer and identify:

- any beneficial owners and controllers of the customer;
- those third parties for whom the customer acts indirectly/directly (e.g. legal arrangement); and
- others listed in Article 3(2) (which links to Article 3(7) e.g. settlor/protector).

50. The starting point is that the *relevant person* has to determine who everyone detailed in paragraph 49 above is as part of *identification measures*.

Guidance Notes- Fund

51. Responsibility for applying *CDD* measures (which includes *identification measures* and monitoring) rests with the governing body of the Fund.

Type of Fund Entity	Responsibility
Company	Directors
Limited Partnership/ Unit Trust	Directors of the general partner / trustee of the limited partnership / unit trust where the general partner / trustee is a company
Protected Cell	Directors of the protected cell company (*PCC*) not each of the protected cells although the directors of the protected cells may assist with compliance
Incorporated Cell	Directors of each of the incorporated cells

14.3.2 Guidance Notes – Fund Operators

52. A number of Fund Operators are likely to provide services to the Fund. Each will be a *relevant person*, with the Fund as their customer. Each will have their own *CDD* obligations pursuant to the *Money Laundering Order*.

53. Even where a Fund Operator is not providing investor facing services and only provides services to the Fund they should ensure when conducting their *CRA* (of their customer - the Fund) that they obtain sufficient information on investors (e.g. *source of funds*) and controllers of the Fund. Rather than gathering this information themselves in a low risk scenario the Fund may be able to provide a list of its investors with holdings of 25% and *source of funds* information provided to the Fund via investors via subscription agreements/investor questionnaires (see also paragraph 127).

54. The first step for a *relevant person* is to determine the nature of their customer and determine the customer's potential beneficial owners and controllers, any third parties on whose behalf the customer acts (and any third party's beneficial owners and controllers) and others listed in Article 3(2). It may not always be necessary to verify all of them.

55. The application of Article 3 differs depending on the legal form of the Fund. In the examples in the two tables below it is assumed that both the general partner and trustee are companies.

Application of Article 3 where the Fund Operator's customer is a:

Legal Person i.e. a Company			
Customer	Third Party	Owners / Investors of the Fund	Governing Body
Company Article 3(2)(a), (aa) and (c)	n/a	Shareholder(s) (owns customer) Article 3(2)(c)(iii)	Directors of Company Re customer Article 3(2)(aa), c(ii) and c(iii)
Legal Arrangement i.e. a Limited Partnership/Unit Trust			
General Partner / Trustee (Company) Article 3(2)(a),(aa) and (c)	Limited Partnership / Unit Trust Article 3(2)(b)(iii)	Limited Partner(s) / Unit Holder(s) (owns Third Party) Article 3(2)(b)(iii)(A), (B) and (C) (Note the requirements of Article 3(7))	Directors / Shareholders of General Partner / Trustee Re customer Article 3(2)(aa), c(ii) and c(iii) Re Third Party Article 3(2)(aa), (b)(iii)(A), (B) and (C)

56. Once a *relevant person* fully understands the ownership and control structure of a customer the *relevant person* can determine the beneficial owners and controllers pursuant to the Three Tier Test (see footnote 13 above*)* and then apply the necessary *identification measures*.

57. The Three Tier Test is applied on a case by case basis and the table below indicates potential beneficial owners or controllers in different scenarios where the ***relevant person*** **is Fund Operator and the Fund is a**:

Legal person i.e. a company		
Customer	Third Party	Beneficial Owners/Controllers
Company Article 3(2)(a), (aa) and (c)	n/a	Apply the Three Tier Test (see footnote 13 above) Shareholder(s) Article 3(2)(c)(iii) - Potentially Tier 1 Promoters/Instigators Article 3(c)(ii) - Potentially Tier 2 Directors of Company - Potentially Tier 3 Article 3(2)(aa), (c)(ii) and (c)(iii)
Legal arrangement i.e. Unit Trust/Limited Partnership		
General Partner for Limited Partnership / Trustee for Unit Trust (Company) Article 3(2)(a), (aa) and (c)	Limited Partnership/ Unit Trust Article 3(2)(b)(iii)	Apply the Three Tier Test to the customer and the Third Party: customer – General Partner /Trustee Article 3(2)(aa) and (c) Third Party- Limited Partnership / Trust Articles 3(2)(b) and 3(7)

58. More detailed guidance on how to determine and identify beneficial owners and controllers is contained in the following sections of the *AML/CFT Handbook*.

Entity	Finding out identity	Obtaining evidence
Limited Partnership	4.4.3	4.4.4
Trust (not Unit Trust)	4.4.1	4.4.2
Company	4.5.1	4.5.2

14.3.3 Guidance Notes - Unit Trusts

59. Unit trusts differ from traditional private trusts. For example, with a private family trust there is normally a settlor who not only establishes the trust but also provides the initial funds and ongoing funding to the trust. Beneficiaries may be expressly referred to or may form part of a class and may not have a vested right to the trust assets.

60. In a unit trust the promoter or instigator may fund the establishment of the unit trust and may fund the initial investment, thus being considered a settlor. While the individual investors are not considered to be settlors for the purposes of Article 3(7)(a), each of the unit holders will be customers of the Fund (unit trust) investing their money into the unit trust. This may include the promoter as an investor.

61. Statutory requirements relating to *identification measures* that apply to unit trusts are set out at Article 3(7).

14.3.4 Guidance Notes Fund Operators- Passive Investors

62. Identification of Investors in a Fund will be approached differently by the Fund and a Fund Operator.

63. The Fund has an obligation to identify each of its investors, as they are the Fund's customers. This obligation exists whether or not they are passive investors and don't exercise control over the Fund.

64. The Fund Operator, however, has an obligation to identify the beneficial owners and controllers of their customer (the Fund) and should apply the Three Tier Test (see footnote 13 above) to ascertain who the beneficial owners and controllers are. Where ownership of a Fund is distributed widely, it may be that none of the investors control the Fund through their ownership. In such a case, these "passive" investors are not beneficial owners at Tier 1 and, assuming they are not controllers via Tier 2 or 3, a Fund Operator need not apply *identification measures* to them.

65. It should be noted, however, that in order to demonstrate that sufficient information has been collected on *source of funds* for a customer relationship, it may still be necessary to consider the provenance of investors who have a material interest in a customer, but who do not also exercise control. The effect of this may still be to require information to be obtained on such passive investors (though it may not be necessary to also obtain evidence of identity).

66. For example, an investment advisor giving advice directly to a regulated Fund with passive investors will still need to obtain *source of funds* information in relation to those investors in order to understand the *AML/CFT* risk posed by its customer.

67. The extent of *source of funds* information collected will be proportionate to the risks identified and determined on a case by case basis. In a lower risk relationship, *source of funds* information should be obtained for all passive investors with a holding of 25% or more. Where there are no 25% holders, generic investor information on *source of funds* such as a generic client profile could be obtained. In a higher risk relationship, more stringent measures should be applied.

68. Similarly, in order to demonstrate that sufficient information has been collected to assess the *AML/CFT* risks posed by a customer, it may be necessary to consider the identity, nature, structure and location of investors who have a material interest in a customer, but who do not also exercise control. See Sections 3.3.2 and 3.3.4 for further detail.

14.3.5 Guidance Notes Fund Operators – Promoters

69. A *relevant person* may need to consider whether the promoter of a Fund is a beneficial owner or controller. For example, the promoter / instigator of the Fund may have direct control by owning the governing entity (i.e. the general partner or the trustee) or by owning management shares of a Fund company.

70. In addition, a promoter may also be a beneficial owner or controller when the Board of a Fund does not exercise sufficient effective control. For example, a promoter may be the investment adviser / investment manager or may have a significant presence on the investment committee (which may be "controlling by other means" – see Tier 2 of the Three Tier Test).

14.3.6 Guidance Notes - Multiple layers

Overview

71. Fund structures are often complicated by ultimate beneficial owners not entering into transactions directly and there may be multiple entities, such as holding companies or trusts, between the investment in the Fund and the individual who is the ultimate beneficial owner. The more complex the structure and/or the more use of nominees / intermediaries; the more difficult it may be to determine the beneficial owner and controller.

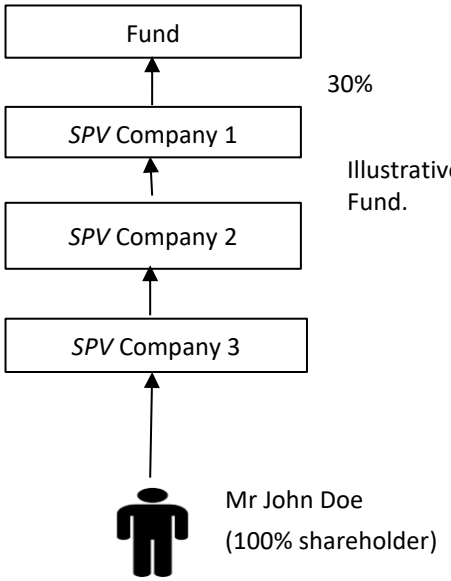
72. A *relevant person's* approach to a complex ownership and control structure will be informed by the risk rating allocated to that customer.

73. The following must always be identified:

- the customer;
- the ultimate beneficial owner/controller of the customer (as per the Three Tier Test (see footnote 13 above)); and
- any third parties for whom the customer acts.

Guidance Notes

74. In this example the Fund is the *relevant person*. The general rule is that you are trying to ascertain the ultimate individual(s) who control(s) the structure.



Customer

75. *SPV* Company 1 is the customer of the Fund.

76. The Fund is obliged to find out the identity and obtain evidence of identity of its customer. The *AML/CFT Handbook* provides guidance on *identification measures* to be applied to a legal person that is a company:

- Part 1: Section 4.5.1 finding out the identity of a legal person that is a company; and
- Part 1: Section 4.5.2 obtaining evidence of identity of a legal person that is company.

Beneficial Owner/Controller

77. *SPV* Company 1 is a legal person and the *relevant person* must understand the ownership and control structure of the customer. The Fund is obliged to find out the identity and obtain evidence of identity of its beneficial owners/controllers. The Three Tier Test is applied to ascertain who controls the customer:

- Control via ownership; and
- Control via other means; or
- Control through positions held (if no-one at Tiers 1 and/or 2)

78. Understanding a customer's ownership and control structure will allow a *relevant person* to determine the ultimate beneficial owner/controller. Article 2(2) of the *Money Laundering Order* states "…. *it is immaterial whether an individual's ultimate ownership or control is direct or indirect*".

79. In this example the structure is in place for the purpose of facilitating the investment of John Doe and he is exercising effective control. Therefore, regardless of the holding companies, John Doe is the ultimate beneficial owner/controller of the customer.

80. The *AML/CFT Handbook* provides guidance for individuals (in this case John Doe):

- Part 1: Section 4.3.1 finding out the identity of an individual
- Part 1: Section 4.3.2 obtaining evidence of identity of an individual

81. If none of the individuals with an ownership interest exercises control then they may not need to be identified (see passive investor Section 14.3.4).

"Layers"

82. In the scenario above understanding the ownership and control structure of the customer is likely to require some effort, but it may not be necessary to obtain detailed identity information and evidence in relation to each entity in the structure.

83. Verification of Identity may not be necessary in relation to *SPV* Company 2 and *SPV* Company 3– they are not customers, or beneficial owners/controllers, or third parties on whose behalf the customer is acting (see paragraph 73 above).The reason they are not controllers is because they are acting on the instructions of the ultimate controller Mr John Doe and are links in the control chain.

84. Whilst verification of identity may not be needed sufficient information will still need to be obtained in relation to these two entities in order to understand the ownership and control structure. The Information required will depend on the complexity of the structure and the overall risk of the customer relationship. However as a minimum for a low risk customer the following should be obtained:

- Name of the entity
- Evidence the entity exists
- Names of the directors
- Names of the shareholders or those with other interests
- Details of ownership and control of the entity (proportion of holdings, voting rights, decision-making authority, etc.)

14.3.7 Guidance Notes– Nominees / Investment Managers

Note: This section must be read in conjunction with, and is supplemental to Part 1: Section 7.13 of the *AML/CFT Handbook* regarding designated relationships and *pooled relationship*s.

85. There may be scenarios where the Fund's customer is representing others, for example as a nominee/investment manager.

86. In this scenario the normal obligations apply and the *relevant person* still has to identify:

- The customer
- The ultimate beneficial owner/controller of the customer (as per the Three Tier Test)
- Any third parties for whom the customer acts.

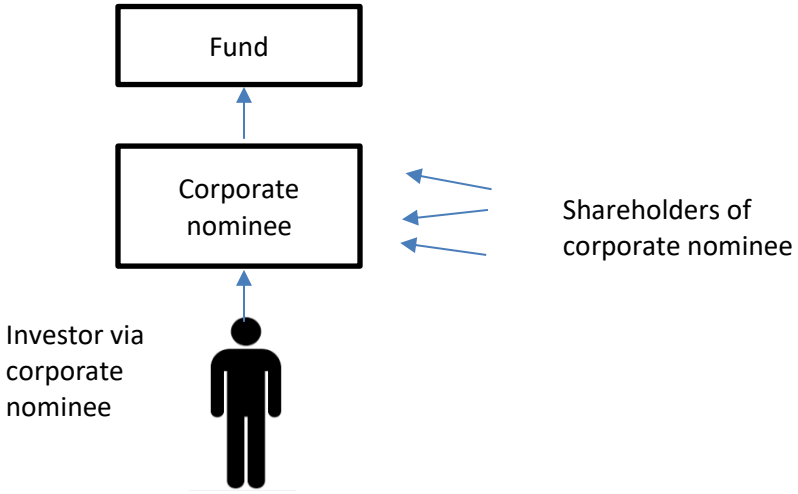
87. If the customer is a company then the *relevant person* would apply the guidance in paragraph 76 above.

88. The corporate nominee is the customer and it will be necessary to identify its beneficial owners and controllers. The Three Tier Test will need to be applied to determine the potential beneficial owner/controllers of the corporate nominee. In this scenario it will also be necessary to identify the third party for whom the corporate nominee is acting and determine the beneficial and ownership and control of that third party as per Article 3(2)(b).

Illustrative Example of application of the Three Tier Test to

a corporate nominee (Article 3(2)(c))		
X	Control via ownership	There are number of owners and there is no majority shareholder.
X	Control via other means	There are no entities/persons that fall into this tier
√	Control through positions held	The board of directors control the corporate nominee

an individual whose interest is through the corporate nominee (Article 3(2)(b))		
√	Control via ownership	Here the principal is an individual
X	Control via other means	Tier 1 applies so no further need to determine potential persons in other Tiers.
X	Control through positions held	



89. In the scenario above the Fund is the *relevant person*, the corporate nominee is the customer and the individual is the third party for whom the customer is acting.

90. The relevant person must identify and verify its customer –here the corporate nominee as set out at paragraph 76. Control and ownership of the customer must be ascertained applying the three tier test (paragraph 88 above).

91. The third party for whom the customer is acting must also be identified and verified. In the diagram this will be the individual who is investing via the nominee. If the third party was not an individual then its beneficial owners and controllers must be identified and verified.

14.3.8 Guidance Notes Fund Operators– residual assets

92. On some occasions when a Fund is wound up the Fund Operator may hold residual and/or illiquid assets of the Fund for the benefit of the investors. In this scenario care has to be taken and the following matters should be considered:

- Have the investors now become the Fund Operator's customers?
- Does the Fund Operator hold sufficient *CDD* on its customers? For example, the Fund Operator may have taken comfort from the *identification measures* applied by the Fund but the Fund no longer exists.
- Has the Fund Operator updated its *CRA* and *BRA* to take into consideration its new role (whether or not the investors are its customers)?

14.4 Timing of identification measures

Note: This section must be read in conjunction with, and is supplemental to, Part 1: Sections 4.1 and 4.7 of the *AML/CFT Handbook.*

Overview

93. Article 13(4) of the *Money Laundering Order* provides a concession in relation to the timing of *identification measures*, permitting a delay in obtaining evidence in specific circumstances. In no circumstances can the obtaining of information be delayed.

Guidance Notes

94. Delaying the obtaining of evidence is permitted in certain circumstances but should not be common or standard practice. It should not be common practice that verification is deferred until after the first close of a Fund. On the rare occasions the provisions of Article 13(4) are relied upon to delay the obtaining of evidence of identity, additional measures are required, including effectively managing the associated risk by appropriate authorisation, monitoring and reporting.

95. The obtaining of evidence of identity "as soon as reasonably practicable" should in most cases be a matter of days rather than weeks or months.

14.5 Failure to complete identification measures

Note: This section must be read in conjunction with, and is supplemental to, Part 1: Section 4.8 of the *AML/CFT Handbook*.

Overview

96. Under Article 14 of the *Money Laundering Order*, if a *relevant person* is unable to apply *identification measures* when required to do so then it must terminate that relationship and consider whether to make a *SAR* to the JFCU.

97. Such a requirement can be problematic in the case of a *relevant person* that is a Fund where its customer is an investor and where:

- the relationship between the Fund and its investor is governed by other legislation or regulatory requirements - e.g. the *CIF(J) Law* and Code of Practice for Certified Funds; and
- the termination of a relationship with an investor may have a prejudicial effect on the interests of other investors (e.g. a closed-ended illiquid property fund).

Guidance Notes

98. In order to address such tension, termination of a business relationship may be **delayed** until such time as compliance with Article 14 of the *Money Laundering Order* does not conflict with another statutory or regulatory requirement, and/or does not have any prejudicial effect on the interests of other customers (investors), so long as the risk of *money laundering* or *financing of terrorism* is effectively managed.

14.6 Updating identification information

Note: This section must be read in conjunction with, and is supplemental to, Part 1: Sections 3.4 and 4.1 of the *AML/CFT Handbook*.

Guidance Notes

99. The *BRA* will enable a *relevant person* to establish procedures to undertake reviews of its customers on a risk sensitive basis. In addition to the established pattern of reviews there will be factors to consider or "trigger events" when it may be appropriate to consider whether the identity information and evidence held on a customer is relevant and up to date. These should include (in addition to those circumstances set out in Part 1: Section 3.4 of the *AML/CFT Handbook*):

- Receipt of significant additional funds to be invested where the delay between contributions is material (including drawdowns)
- Distributions being made
- Economic Merger of two Funds which results in the admission of new investors[14]

100. It may well be that when a customer's information and evidence is reviewed upon a trigger event it is clear that the information and evidence previously obtained, possibly pursuant to a recent scheduled review, is sufficient and no further updated information is needed.

14.7 On – going monitoring: scrutinising of transactions & activity

Note: This section must be read in conjunction with, and is supplemental to, Part 1: Section 6 of the *AML/CFT Handbook*.

Guidance Notes

101. The information about a customer obtained at the outset of the relationship as part of *identification measures* should permit a *relevant person* to monitor activity against an expected pattern of activity and transactions. For Funds this will include generic profiles of the expected target investors and the expected target investments. By way of example if the Fund's prospectus indicates that it is going to invest in UK real estate and then invests in pearls from the South China Sea this is not expected activity. Similarly, if the Fund is aiming for investment from European Banks and then receives investment from a Sub Saharan Non-Profit Organisation, this would not be expected activity.

102. It is not sufficient for an administrator/manager who has been delegated the responsibility for monitoring the Fund to simply facilitate the transaction - they are also required to monitor each transaction to determine whether it is inconsistent; complex/large; high risk or follows an unusual pattern. If, for example, the pattern does not match then the rationale for the deviation should be obtained and documented.

103. Expected activity may change over time if the target market or target investments change. This may also impact on the Fund's BRA and CRAs which may need to be updated.

14.8 Collation of customer due diligence

Overview

104. Every Fund and Fund Operator is obliged to comply with its own Customer Due Diligence requirements. However, there may be statutory or contractual provisions operating so that, should one entity in a Fund structure undertake sufficient customer due diligence, others in the structure may not need to duplicate certain aspects of customer due diligence themselves.

105. The following sections of the *AML/CFT Handbook* deal with specific provisions regarding scenarios where a *relevant person* may not undertake all of the *CDD* process themselves:

Exemptions from *Identification measures*	› Part 1: Section 7
Reliance on *obliged persons*	› Part 1: Section 5
Outsourcing	› Part 1: Section 2.4.4 › Part 1: Section 5 paragraph 12

[14] Also consider guidance on taking-on a new book of business at Part 1 Section 3.5 of the *AML/CFT Handbook*

106. Where a *relevant person* is not undertaking aspects of customer due diligence, including applying exemptions, it needs to document who is, on what basis and that the risks have been properly assessed and considered.

14.8.1 Exemptions from identification measures

Note: This section must be read in conjunction with, and is supplemental to, Part 1: Section 7 of the *AML/CFT Handbook*.

Overview

107. An assessment as to whether exemptions from *identification measures* are appropriate for customers and/or in relation to third parties must be conducted and documented. In doing so the statutory prohibitions, stating where exemptions cannot be applied, must be carefully considered in each case:

Circumstances in which exemptions under Part 3A do not apply (Article 17A)	
Exemptions under Articles 17 B-D	**Exemptions under Article 18**
› the *relevant person* suspects *money laundering*	› the *relevant person* suspects *money laundering*
› the *relevant person* considers that there is a higher risk of *money laundering,* including the risk of *money laundering* if fail to apply appropriate *identification measures* or keep records.	› the *relevant person* considers that there is a higher risk of *money laundering*
› the customer is resident in a country that is not compliant with the *FATF* recommendations	› the customer is resident in a country that is not compliant with the *FATF* recommendations
› the customer is a person in respect of whom Article 15(1)(c) applies [specified persons have a relevant connection to country/territory in relation to which *FATF* has called for enhanced customer due diligence]	› the customer is a person in respect of whom Article 15(1)(c) applies [specified persons have a relevant connection to country/territory in relation to which *FATF* has called for enhanced customer due diligence]
› the customer is a person in respect of whom Article 15B(1) applies [certain deposit taking businesses with a banking or similar relationship with an institution whose address for that purpose is outside Jersey]	

108. Exemptions from *identification measures* may only be applied in appropriate circumstances. Where specified, this will require an assessment of the risk of applying the exemption, in addition to a *CRA*.

Guidance Notes

109. Articles 18 and 17B-D can be applied to the same customer relationship, as they apply to separate identification requirements – Article 18 relates to identification of the customer and Articles 17B-D relate to identification of third parties on whose behalf the customer is acting.

110. However, there are some aspects of customer due diligence that the *relevant person* will always be obliged to undertake, see the table below:

	Always required.
	Articles 17B-D provide an exemption from this obligation
	Article 18 provides an exemption from this obligation (Note: does not apply to third parties)

CDD	*Identification measures*	Risk assessment		
		ID customer		
		ID Third parties		
		ID person acting for customer		Verify authority to act
		Where customer not individual:	Understand Ownership/control structure	
			ID Beneficial Owners/Controllers	
		Obtain information on purpose/nature		
	On-going monitoring	Scrutinising transactions / activity		
		Keep documents/information up-to-date		

111. Article 18 applies to the customer and does not extend to third parties. For example, Article 18 only applies to the general partner or the trustee and not to the limited partnerships or unit trust. Articles 17B-D do apply to third parties which would encompass the investors in a limited partnership or a unit trust.

112. Article 18(4)(b) refers to a customer that is a body corporate whose securities are listed on an IOSCO compliant exchange or on a regulated market. As part of the assessment whether SDD may be applied the *relevant person* should consider whether the exchange that the securities are listed on, is an IOSCO compliant exchange or a regulated market (Article 2(5)). The fact that the exchange is listed in a product guide (e.g. listed fund guide) or in an Order (e.g. Unregulated Funds Order) does not mean it necessarily qualifies. There are no lists of these exchanges available save for *EU* regulated markets: https://registers.esma.europa.eu/publication/searchRegister?core=esma_registers_mifid_rma#**.** Guidance is given on this point in Part 1: Section 7.16.3 of the *AML/CFT Handbook*.

14.8.2 Reliance on obliged persons

Note: This section must be read in conjunction with, and is supplemental to, Part 1: Section 5 of the *AML/CFT Handbook*.

Guidance Notes

113. Care should be taken when placing reliance on an administrator. An administrator may be acting in two capacities when undertaking customer due diligence; (i) for itself as Fund Operator and (ii) as a delegate on behalf of the Fund. In such a case, a *relevant person* seeking to rely on *CDD* undertaken by the administrator needs to be clear whether it is the administrator or the Fund that is the *obliged person*.

114. There are some key questions for the *relevant person* to ask:

- What *identification measures* do you need to apply?
- Who are you intending to rely upon?
- What identification information and evidence has the *obliged person* obtained?
- Does the information and evidence obtained by the *obliged person* being relied upon match your requirements?

115. Each Fund Operator will have its own risk appetite and its own *CRA* of the Fund and the risk ratings allocated by different Fund Operators may not be the same. Where a Fund Operator assesses the Fund as higher risk it may be insufficient to rely on information and evidence obtained by a Fund Operator rating the Fund as lower risk and additional information is likely to be required.

116. Importantly, chains of reliance are not permitted. A *relevant person* cannot rely on an *obliged person* who is in turn relying on someone else.

117. Reliance may be used where the Fund structure has higher *AML/CFT* risks or the Fund structure and Fund Operators are unregulated (where the Fund Operator cannot apply exemptions from *identification measures*).

118. There are aspects of Customer Due Diligence that, in the absence of other provisions, the *relevant person* must undertake itself, as below:

	Always required.
	Article 16(2) allows reliance upon an *obliged person*.

<table>
<tr><td rowspan="8">*CDD*</td><td rowspan="6">*Identification measures*</td><td colspan="3">Risk assessment</td></tr>
<tr><td colspan="3">ID customer</td></tr>
<tr><td colspan="3">ID Third parties</td></tr>
<tr><td colspan="2">ID person acting for customer</td><td>Verify authority to act</td></tr>
<tr><td rowspan="2">Where customer not individual:</td><td colspan="2">Understand Ownership/control structure</td></tr>
<tr><td colspan="2">ID Beneficial Owners/Controllers</td></tr>
<tr><td colspan="3">Obtain information on purpose/nature</td></tr>
<tr><td rowspan="2">On-going monitoring</td><td colspan="3">Scrutinising transactions / activity</td></tr>
<tr><td colspan="3">Keep documents/information up-to-date</td></tr>
</table>

14.8.3 Obtaining copy documentation from a regulated trust and company services provider in the Crown Dependencies

Note: This section must be read in conjunction with, and is supplemental to, Part 1: Section 4.4.5 and Part 1: Section 4.5.7.

Overview

119. In certain circumstances, it may be appropriate to obtain information from 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 in order to identify certain individuals.

120. It should be noted that such practice is restricted to a very narrow set of circumstances (e.g. only certain individuals; only certain documents) and is dependent on a number of conditions being met (e.g. specific risk assessment and obtaining specific confirmations from the trust and company service provider).

14.8.4 Outsourcing[15]

Note: This section must be read in conjunction with, and is supplemental to, Part 1: Section 2.4.4 and Section 5 paragraph 12.

Overview

121. Contractual arrangements may be put in place where another entity undertakes Customer Due Diligence for the *relevant person* as a delegate. This is likely to be the case where an administrator and/or manager is appointed to the Fund or where the governing body of the Fund such as a trustee or general partner is a managed entity and reliant on a manager of a managed entity. The *relevant person* always remains responsible for fulfilling its statutory obligations regardless of the activities it outsources to delegates.

122. Procedures and processes must be put in place so that the delegating party retains oversight of the outsourced activities. The *relevant person* needs to be provided with sufficient information by the delegate in order to adequately review and monitor the outsourced activities.

Guidance Notes

123. Outsourcing of specific functions to a Fund Operator may form part of the Fund Operator's service level agreement with the Fund. The *relevant person* would be expected to ensure that the terms are adequate to ensure a clear understanding of what activity the delegate is undertaking.

124. Given that the delegate carrying out the outsourced function is likely to have its own customer due diligence obligations it will be important to distinguish between measures applied on behalf of the delegating party and measures applied for itself. This will ensure the respective (and potentially differing) obligations are met and will assist if the delegating party moves to another Fund Operator and wishes to take its information/documentation /records with it.

	CDD is always the responsibility of the *relevant person*.
	These activities may be outsourced.

[15] Consideration will also need to be given as to whether the *Commission*'s Outsourcing Policy and Guidance Notes apply.
However, please note that the *Money Laundering Order* is described in that Policy as imposing additional legal or regulatory requirements which must still be complied with.

<table>
<tr><td rowspan="8">CDD</td><td rowspan="6">Identification measures</td><td colspan="3">Risk assessment</td></tr>
<tr><td colspan="3">ID customer</td></tr>
<tr><td colspan="3">ID Third parties</td></tr>
<tr><td colspan="2">ID person acting for customer</td><td>Verify authority to act</td></tr>
<tr><td rowspan="2">Where customer not individual:</td><td colspan="2">Understand Ownership/control structure</td></tr>
<tr><td colspan="2">ID Beneficial Owners/Controllers</td></tr>
<tr><td colspan="3">Obtain information on purpose/nature</td></tr>
<tr><td rowspan="2">On-going monitoring</td><td colspan="3">Scrutinising transactions/activity</td></tr>
<tr><td colspan="3">Keep documents/information up-to-date</td></tr>
</table>

125. Where *CDD* functions are outsourced, consideration will need to be given to the contractual arrangements between the Fund and its investors (customers), the Fund and its Fund Operators and any other entities. Below are some important matters to consider (this list is not exhaustive):

- "ownership" of the investor information
- permissions required from the investor for obtaining, holding and using the information for other purposes (data protection)
- the nature and scope of the obligations outsourced and provisions for monitoring, updating, retention and termination.

126. Where a Fund Operator assesses the risk of *AML/CFT* in relation to a Fund to be higher or the Fund/Fund Operators are not regulated the application of exemptions from *identification measures* is prohibited. Therefore, a Fund Operator providing services to a Fund with no direct relationship with investors may need to apply *identification measures* to investors. This may be in relation to the control of the Fund or *source of funds*. Rather than gathering this information themselves they will want access to this information which will normally already have been provided to the Fund by investors via subscription agreements/investor questionnaires.

127. Please note that specific provisions may be necessary in subscription agreements / investor questionnaires to enable the Fund to pass on information and evidence that it obtains to meet its own *AML/CFT* obligations to assist Fund Operators (present and future) involved in the Fund/Fund Structure to meet their *AML/CFT* obligations (subject to any data protection requirements).

14.9 Enhanced due Diligence – Non-Jersey Investors

Note: This section must be read in conjunction with, and is supplemental to, Part 1: Sections 7, 7.4 and 7.7 of the *AML/CFT Handbook*.

Overview

128. Funds with overseas investors will need to undertake enhanced due diligence on those investors (Article 15) as the investors will normally be:

- Non-resident customers; and/or
- Not physically present for identification purposes.

129. Enhanced due diligence measures must be applied to address the risk associated with the customer and Part 1: Section 7 of the *AML/CFT Handbook* provides guidance.

Guidance Notes

130. A requirement to apply enhanced due diligence does not automatically mean that the customer is higher risk. Some enhanced measures are required regardless of risk.

131. It may be possible for investor profiles/subscription agreements to address enhanced due diligence requirements by obtaining additional information if the investor meets certain criteria e.g. "Are you Jersey Resident? If the answer is no please provide the following additional information…"

132. On some occasions the rationale for non-Jersey investors looking to invest in Jersey may be determined without necessarily asking the customer (e.g. it may be obvious, i.e. the Fund is a Jersey Fund).