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*.