
SECTION 3

KNOW YOUR CUSTOMER AND CUSTOMER DUE DILIGENCE

3.1

INTRODUCTION

The term "know your customer" ("KYC") has been in use since the 1980s. Increasingly the term "customer due diligence" ("CDD"), drawn from the Basel Committee on Banking Supervision paper of October 2001 "Customer Due Diligence for Banks", is also used. CDD is defined in the Proceeds of Crime (Money Laundering) Code 2010 ("AML Code") and the Prevention of Terrorist Financing Code 2011 ("CFT Code") (together referred to as "the Codes") as meaning the measures specified in paragraphs 5 to 7 and 9 to 15 of the Codes. Essentially, the term CDD is being used to represent the same concepts as reflected throughout the Handbook.

CDD measures involve:

- (a) Identifying a customer and verifying a customer's identity using reliable, independent source documents, data or information;
- (b) Identifying the beneficial ownership and control of the customer and taking reasonable measures to verify the identity of the beneficial owners and controllers such that a financial service business is satisfied that it knows who the beneficial owners and controllers are;
- (c) Obtaining information on the nature of the customer's business and the customer's economic circumstances;
- (d) Obtaining information on the purpose and intended nature of the business relationship;
- (e) Obtaining information on the type, volume and value of the activity that can be expected within the relationship;
- (f) Obtaining information on the source of funds and, subject to the risk assessment, obtaining information on the source of wealth;
- (g) Monitoring activity and transactions undertaken within the relationship to ensure that the activity or transaction being conducted is consistent with the licenceholder's knowledge of the customer; and
- (h) Keeping the information relevant and up to date. Sound CDD procedures are vital for all licenceholders because they:
 - (i) Help protect the licenceholder and the integrity of the Isle of Man financial sector by reducing the likelihood of licenceholders becoming a vehicle for, or victim of, financial crime;
 - (j) Assist law enforcement by providing available information on customers or activities, funds and transactions being investigated;
 - (k) Constitute an essential part of sound risk management e.g. by providing the basis for identifying, limiting and controlling risk exposures in assets and liabilities, including assets under management; and
 - (l) Help to guard against identity theft.

Inadequacy or absent satisfactory CDD standards and controls can subject a licenceholder to serious customer and counterparty risks, especially reputational, operational, legal and concentration risks, which can result in significant financial cost to the business.

CDD information is also a vital tool for employees in recognising whether there are grounds for knowledge or suspicion of money laundering or where there are reasonable grounds to suspect terrorist financing. The information is also essential for the MLRO in assessing whether an internal report has foundation. It is only through knowledge of what constitutes normal activity for a customer that unusual activity can be recognised and, from the unusual that suspicious transactions or activity can be determined.

In relation to CDD, the Commission believes that to properly understand and manage the money laundering and terrorist financing risk (and other risks) that a customer may represent, it is prudent practice for licenceholders to be clear about the risk that individual customers or categories of customers represent. The criteria used in assessing customer risk will vary from licenceholder to licenceholder, based on each institution's operations.

Licenceholders therefore should have clear, documented customer acceptance policies and procedures which are based on their assessment of risk.

Licenceholders should apply a graduated customer acceptance policy which requires more extensive CDD procedures to be undertaken on customers who represent higher risk. Where an applicant for business poses a higher risk of money laundering or terrorist financing, paragraph 3(4) of the AML Code requires licenceholders to carry out enhanced CDD. Where customers pose a higher risk of terrorist financing, paragraph 3(4) of the CFT Code requires licenceholders to either undertake enhanced CDD or conduct an adequate investigation. However, because the AML Code requires licenceholders to undertake enhanced CDD where there is a higher risk of terrorist financing, it could be a breach of the AML Code should a licenceholder choose to undertake an adequate investigation instead of enhanced CDD. Therefore where there is a higher risk of money laundering or terrorist financing, licenceholders must undertake enhanced CDD procedures.

In addition, certain concessions contained within the Codes do not apply where an applicant for business poses a higher risk. These include the Acceptable Applicant and Eligible Introducer concessions.

However, even where a customer is considered to represent a lower risk of money laundering, the minimum standard of due diligence procedures in the Handbook must always be applied.

It is important to distinguish between the identification and verification of identity procedures on the one hand, and the wider CDD procedures which entail much more than the identification of a customer, whether a legal or natural person. The general CDD requirements and the nature of the information to be collected for each different customer type are covered in this Section of the Handbook. The persons for whom information is to be obtained and the identification and verification of identity procedures which the Commission expects licenceholders to apply are detailed in Section 4 of the Handbook. Exemptions and concessions from the identification requirements are also contained within Section 4.

CDD requirements apply at the outset of a customer relationship or one-off transaction. They also apply, in relation to existing and continuing business relationships, as per paragraph 7 of the Codes, when there is/are:

- (a) A transaction that is suspected may be related to money laundering or terrorist financing.
- (b) A pattern of behaviour that causes a licenceholder to know or suspect that the behaviour is or may be related to money laundering or terrorist financing.
- (c) Transactions or patterns of transactions that are complex or unusually large and which have no apparent economic or visible lawful purpose.
- (d) The licenceholder becomes aware of anything which causes them to doubt the identity of the person who, in relation to the formation of the business relationship, was the applicant for business.
- (e) The licenceholder becomes aware of anything which causes them to doubt the veracity or adequacy of CDD information and documentation already produced.
- (f) A suspicion of money laundering or terrorist financing in respect of a person for whom identification evidence is not already held.
- (g) A change in identification information of a customer.
- (h) A change in underlying principals or third parties on whose behalf a customer acts.
- (i) A change in the beneficial ownership and/or control of a customer.
- (j) An absence of meaningful originator information on wire transfers (see Section 5.3 for more specific information on the requirements relating to wire transfers).

(k) In respect of wire transfers, where a one-off payment in excess of Euro 1000 is to be made at the request of a non-account holding customer.

3.2

A RISK-BASED APPROACH TO CDD

A risk-based approach to CDD is one that takes a number of discrete steps in assessing the most effective and proportionate way to manage the money laundering and terrorist financing risks faced by a licenceholder.

The risk assessment of a particular customer will determine:

- (a) the extent of identification information to be sought;
- (b) any additional information that needs to be requested;
- (c) how that information will be verified and for whom; and
- (d) the extent to which the relationship will be monitored.

It will also help to guard against identity theft.

Care has to be exercised under a risk-based approach. Being identified as carrying a higher risk of money laundering or terrorist financing 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 terrorist financing does not mean that the customer presents no risk at all.

There are five stages within a risk-based approach to CDD requirements.

3.2.1 Stage 1- Collection of relevant information

CDD information comprises both identification and relationship information. To enable a customer profile to be prepared, licenceholders must collect relevant CDD information on a risk sensitive basis to determine how and how far this should be done on the following:

- (a) The customer;
- (b) The beneficial ownership and control of the customer;
- (c) The nature of the customer's business and the customer's economic circumstances;
- (d) The anticipated relationship with the licenceholder; and
- (e) The source of funds.

A customer will be one of the following:

- (a) An individual.
- (b) The trustee of an express trust or other similar legal arrangements where they are acting on behalf of these entities.
- (c) A legal person - bodies corporate, foundations (including those established under the Foundations Act 2011), anstalts, partnerships, associations, or any similar bodies that can establish a permanent customer relationship with a licenceholder or otherwise own property.

Underlying principals of a customer are the individuals who ultimately own or control a relationship, and/or the individuals on whose behalf the relationship is being conducted. The individuals considered to be the underlying principals for each customer type are described in Sections 4.6 and 4.7 and mainly refer to legal arrangements such as trusts and legal persons such as companies.

The Isle of Man Government considers it vitally important for the international standing and economic well-being of the Island that it conforms to established international standards for combating money laundering and terrorist financing. The FATF Recommendations and the Basel CDD principles both state the importance of knowing the identity of the beneficial owner and/or underlying principals and of not operating anonymous accounts.

Except where specific circumstances allow licenceholders must, in all cases, know the identity of underlying principals and/or beneficial owners at the outset of a business relationship. This is irrespective of the geographical origin of the client, or of any introducer or fiduciary, or of the complexity of a legal structure.

As per paragraph 25 of the Codes, licenceholders must not keep anonymous accounts or accounts in fictitious names for any new or existing customer.

Where numbered accounts exist, licenceholders must maintain them in such a way that full compliance can be achieved with the Codes, the Rule Book and this Handbook. Licenceholders must properly identify and verify the identity of the customer in accordance with the Handbook

In all cases, whether the relationship involves numbered accounts or not, the customer identification and verification records should be available to the Compliance Officer, MLRO, other appropriate staff and competent authorities.

3.2.1.1 Profiling customers

Certain types of product or service may provide an opportunity to build generic templates that predict expected patterns of activity. More complex products or services will require individual customer profiles.

It is important that customer profiles are kept up to date to reflect changing circumstances (see Section 5).

The customer profile must contain sufficient information on the rationale for the relationship and the nature of the business that the customer expects to undertake in order for a licenceholder to be able to:

- (a) predict a pattern of expected business activity within each customer relationship;
- (b) Identify unusual complex or higher risk activity that may indicate money laundering or terrorist financing. Identification information and the relationship information to be collected for each of the above customer types are described in the following Sections.

The following situations 1 to 4 will apply to all licenceholders:

Situation 1: Where the customer is a natural person

- (a) Obtain identification information on the natural person.

Situation 2: Where the customer is a legal person

- (a) Obtain identification information on the legal person.
- (b) Obtain identification information on the underlying principals i.e. persons exercising control over the management of the legal person, any person(s) having power to direct the activities of the legal person. This will include directors and account signatories or persons in equivalent roles such as, in respect of foundations, council members, enforcer(s), person(s) appointed under the foundation rules (or equivalent in non-Isle of Man established foundations).
- (c) Obtain identification information on any person(s) purporting to act on behalf of the legal person or by whom binding obligations may be imposed on the legal person. This will include persons holding powers of attorney.
- (d) Obtain identification information on the beneficial owners i.e. any individual who ultimately owns or controls the customer, or on whose behalf a transaction or activity is being conducted. For legal persons not listed on a recognised stock exchange, this includes (but is not restricted to) any individual who ultimately owns or controls (whether directly or indirectly) 25% or more of the shares or voting rights in the legal person. For all legal

persons this includes any individual who otherwise exercises control over the management of the legal person e.g. persons with less than 25% of the shares or voting rights but who nevertheless hold a controlling interest.

For a stock exchange to be considered as "recognised" the entities listed on it must be subject to appropriate disclosure requirements. For entities listed within Europe, this means regulated markets within the meaning of the Directive on Markets in Financial Instruments 2004/39/EC. For entities listed outside Europe, this means regulated markets subject to disclosure requirements consistent with the aforementioned Directive.

For example, in the context of the London Stock Exchange, this would include the Main Market but would not include the Alternative Investment Market.

(e) In respect of foundations, which are legal persons but which resemble trusts in many ways, licenceholders must also obtain identification information on the registered agent, founder(s), dedicator(s), assignee(s), all known beneficiaries and potential beneficiaries presenting a higher risk (or equivalent in non-Isle of Man established foundations). It is also necessary to obtain identification information on any other person(s) with a sufficient interest, including a person who in the view of the High Court, can reasonably claim to speak on behalf of an object or purpose of the foundation and a person who the High Court determines to be a person with a sufficient interest under section 51(3) of the Foundations Act 2011 (or equivalent in non-Isle of Man established foundations).

Situation 3: Where the customer is a trustee of an express trust

- (a) Obtain identification information on the customer i.e. the trustee(s) or other persons controlling the applicant.
- (b) Obtain identification information on the trust
- (c) Obtain identification information on the underlying principals i.e. the settlor(s) or other persons by whom the arrangement is made, protector(s), any other person having power to direct the activities of the applicant, any person(s) whose wishes the trustee may be expected to take into account, known beneficiaries and potential beneficiaries presenting a higher risk.
- (d) Obtain identification information on any person(s) purporting to act on behalf of the trustee(s) or by whom binding obligations may be imposed on the trustee(s).

Situation 4: Where the customer is acting other than as principal (except as trustee)

- (a) Obtain identification information on the customer.
- (b) Obtain identification information on the underlying principals (natural person, legal person or trustee of an express trust) on whose behalf the applicant is acting.
- (c) Obtain information concerning the relationship between the customer and the underlying principals.

In all of the above situations, relationship information must be obtained (for express trusts, the relationship information to be obtained is on the express trust). Relationship information to be collected is outlined at Section 3.3.

The identification information that must be collected in respect of each type of customer is contained in Section 4.

3.2.2 Stage 2 - Assess and evaluate relevant information

On the basis of the information collected at Stage 1, or on the basis of the nature of the relationship, licenceholders must evaluate the information against the risk areas identified by the risk assessment required by Paragraph 3 of the Codes. Consideration must then be given to whether it is appropriate to collect further information on the applicant for business, on any underlying principals and on the relationship to be established.

In respect of any proposed relationship, licenceholders must always ensure they understand:

- (a) why an applicant for business has requested a particular product or service;

(b) details of any existing relationships with the licenceholder; (c) the nature and frequency of the customer's expected activity paying due regard to any linked accounts or other activity;

(d) the ownership and control structure of legal persons and arrangements.

- For legal persons this would include identifying the underlying principals, beneficial owners etc as outlined at Section 3.2.1.1;

- For legal arrangements this would include identifying the Settlor or other person by whom the arrangement is made, the Trustee or other person(s) controlling the applicant, any other person whose wishes the trustee may be expected to take into account and the beneficiaries;

(e) the various relationships between signatories and underlying principals;

(f) the nature of a customer's business activities or occupation;

(g) the source of the funds for the product or transaction in question; and

(h) where relevant, the source of income or wealth of the customer (see Section 3.4).

For many simple retail savings or investment products, the reasons for a relationship may be self evident. However, for more complex products they may not be e.g. corporate accounts, private banking accounts, investment banking, fund management and discretionary trusts and corporate services. Not all customers, products or services carry the same money laundering and terrorist financing risk and a risk-based and proportionate approach should be adopted in determining the amount of CDD information required in each case.

The following suggested risk factors are not meant to be exhaustive.

Country Risk

Residence in or connection with high risk countries for example:

(a) those that have been classified by the FATF as non-cooperative countries or territories;

(b) countries whose senior political or public figures are included on an internationally recognised sanctions list;

(c) those with inadequate safeguards in place against money laundering or terrorist financing including those jurisdictions listed in Appendices [G\(a\)](#) and [G\(b\)](#);

(d) countries with high levels of organised crime or which are vulnerable to corruption;

(e) those countries that are believed to have strong links to terrorist activities.

In assessing country risk, regard should be given to data available from bodies such as the IMF, FATF, US Department of State (International Narcotics Control Strategy Report) and US Treasury (OFAC).

Customer Risk

(a) Type of customer. E.g. a politically exposed person, a high net worth individual, or a non-quoted legal person will potentially present a higher risk.

(b) Complexity of the relationship, including unexplained use of corporate structures and express trusts and the use of nominee and bearer shares.

(c) Delegation of authority (e.g. power of attorney, mixed boards and representative offices).

(d) Request to use numbered accounts.

(e) Request to use "hold mail" or mail/email forwarding facilities.

- (f) The public profile of the customer or involvement with, or connection to, politically exposed persons.
- (g) Any linked accounts or business partners.
- (h) Value and frequency of cash transactions including a business that generates significant amounts of cash.
- (i) Value of funds involved in the relationship.
- (j) Nature, scope and location of business activities generating the funds/assets in a relationship, having regard to sensitive activities.
- (k) Reputation of the customer. E.g. a well-known, reputable company, with long histories in its industry and with abundant independent information about it and its beneficial owners and controllers are likely to present a lower risk.
- (l) Behaviour of the customer. E.g. where there is no commercial rationale for a customer buying the products that he seeks, where there are requests for undue levels of secrecy, or where it appears that a relationship or transaction is being made unnecessarily complex.
- (m) Express trusts: relationship of the known beneficiaries and potential beneficiaries to the settlor(s) (or equivalent in respect of foundations).
- (n) Express trusts: the nature of classes of beneficiaries and classes within an expression of wishes for which it is not reasonable to identify specific persons within that class (e.g. a trust established for the benefit of all pupils within a specified school) (or equivalent in respect of foundations).

Product or service risk

- (a) Ability to make payments to, or receive payments from, third parties.
- (b) Ability to migrate from one product to another.
- (c) Facilities for cash transactions within the product.
- (d) Ability to pool underlying customers/funds.
- (e) Ability to use hold mail or mail/email forwarding facilities.
- (f) Ability to hold boxes, parcels or sealed envelopes in safe custody.

Delivery Risk

- (a) Indirect relationship with the customer - use of introducers and pooled accounts.
- (b) Non-face to face relationships - products or services delivered by post, telephone, internet etc.
- (c) Availability for "straight-through" processing of customer transactions.

3.2.3 Stage 3 - Determine initial risk profile

On the basis of Stages 1 and 2, licenceholders must determine and record a risk profile for the relationship. This should show whether the customer is to be treated as standard risk or where additional CDD is required. It will determine which underlying principals' identity needs to be verified, how identity is to be verified and the ongoing CDD to be conducted throughout the course of the relationship. For higher risk relationships, enhanced CDD must be performed.

Licenceholders should consider whether inconsistencies between the CDD information obtained, specific information concerning source of funds or source of wealth, and the nature of transactions increases the customer's risk classification.

The risk profile should be reviewed and updated throughout the relationship.

3.2.4 Stage 4 - Verify the identity of the customer and any underlying principals

Licenceholders must satisfactorily verify the identity of the customer and the identity of any underlying principals.

Requirements for verifying identity are set out in Section 4.

3.2.5 Stage 5 - Conduct ongoing due diligence

Licenceholders should review the CDD information held in relation to all customers on a periodic basis, and for higher risk customers at least annually. The opening of a new account, purchase of a further product, or a meeting with the customer may provide an opportunity to confirm or update the information held in respect of that customer.

Further detailed guidance is contained in Section 5.

Procedures should ensure that up-to-date CDD information is readily accessible to the MLRO (and any designated person), and to the Commission and the FCU on request.

3.3

COLLECTING RELATIONSHIP INFORMATION

Unless it is obvious from the product being provided, the following must be established:

3.3.1 In all situations

- (a) Purpose and intended nature of relationship.
- (b) Expected type, volume and value of activity.
- (c) Expected geographical sphere of the activity.
- (d) Activity providing the source of funds for the relationship and geographical sphere of the activity.
- (e) Details of any existing relationships with product/service provider.

3.3.2 Express Trusts - Additional information

- (a) Type of trust (e.g. fixed interest, discretionary, testamentary).
- (b) Structure of any underlying legal persons (if applicable) and nature of activities undertaken by the trust and any underlying entities (having regard for sensitive activities and trading activities).
- (c) Classes of beneficiaries, including charitable causes named in the trust deed.
- (d) Name of trustee's regulator, if applicable.

3.3.3 Legal Persons - Additional information

- (a) If applicable, group ownership and structure enough to understand the ownership and control structure as per Paragraph 5(3)(h) of the Codes.
- (b) Nature of activities undertaken (having regard for sensitive activities and trading activities).
- (c) Geographical sphere of the legal person's activities and assets. (d) Name of regulator, if applicable.

SOURCE OF FUNDS, INCOME AND WEALTH - TAKING A RISK BASED APPROACH (STAGES 1 AND 2)

A licenceholder must as per paragraphs 6(4)(d), 7(4)(b), 9(3)(d) and 11(4) of the Codes take reasonable steps to establish the source of funds for all applicants for business when entering a new relationship, carrying out a one-off transaction or in the circumstances specified at paragraph 7(2) of the Codes. Licenceholders must take reasonable steps to establish the source of income or wealth for higher risk applicants as per paragraph 8(3)(c) of the Codes.

Source of funds includes the immediate source of funds from which property has derived i.e. a bank account. Knowing who provided the funds and the account or product from which they have derived is necessary in every case. Source of funds will sometimes be a bank account that can be related directly to the customer. Where this is not the case, for example when third party funding is involved, licenceholders may take a risk based approach and where appropriate make further enquiries about the relationship between the ultimate underlying principal of the funds and the account holder. In addition, consideration must be given to verifying the identity of the ultimate underlying principal, i.e. the provider of the funds.

Source of wealth is distinct from source of funds and describes the origins of a customer's financial standing or total net worth i.e. those activities which have generated a customer's funds and property. Information sufficient to establish the source of income or wealth should be obtained for all higher risk relationships and all other relationships where the type of product or service being offered makes it appropriate to do so because of its risk profile. This will also include where the product or service is not consistent with information held on the customer.

POLITICALLY EXPOSED PERSONS ("PEPs")

Much international attention has been paid in recent years to "politically exposed person" ("PEP") risk, the term given to the risk associated with providing financial and business services to those with a high political profile or who hold public office. PEP status itself does not automatically mean that the individual is corrupt nor that they have been incriminated in any corruption. However, their office and position can leave them vulnerable to corruption. The risks increase when the person concerned is from a country with widely-known problems of bribery, corruption and financial irregularity within their governments and society. This risk is even more acute where such countries do not have adequate AML/CFT standards, or where these do not meet international financial transparency standards.

PEPs are defined in the Codes and include natural persons, resident outside the Isle of Man, entrusted with prominent public functions and their immediate family members, and close associates. This definition would include royal families as persons entrusted with prominent public functions.

Prominent publicfunctions include:

- (i) a head of state, head of government, minister or deputy or assistant minister;
- (ii) a senior government official;
- (iii) a member of parliament;
- (iv) a senior politician;
- (v) an important political party official;
- (vi) a senior judicial official;
- (vii) a member of a court of auditors or the board of a central bank;
- (viii) an ambassador, charg d'affaires or other high-ranking officer in a diplomatic service;
- (ix) a high-ranking officer in an armed force; and
- (x) a senior member of an administrative, management or supervisory body of a State-owned enterprise;

(xi) a senior official of an international entity or organisation; and

(xii) an honorary consul.

Immediate family members include:

(i) a spouse;

(ii) a partner considered by national law as equivalent to a spouse;

(iii) a child or the spouse or partner of a child;

(iv) a brother or sister (including a half-brother or half-sister);

(v) a parent;

(vi) a parent-in-law;

(vi) a grandparent; and

(vii) a grandchild.

Close associate includes any natural person:

(i) who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with such a person;

(ii) who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of such a person;

(iii) who is known to be a beneficiary of a legal arrangement of which such a person is a beneficial owner or beneficiary; and

(iv) who is in a position to conduct substantial financial transactions on behalf of such a person.

Licenceholders that handle the proceeds of corruption, or handle illegally diverted government, supranational or aid funds, face the risk of severe reputational damage and the possibility of criminal charges for having assisted in laundering the proceeds of crime. Licenceholders also face the risk of constructive trust suits in such situations.

The Isle of Man as a jurisdiction faces considerable reputational damage should any of its licenceholders have a business relationship with customers of this nature involving the proceeds of foreign corruption.

Licenceholders can reduce risk by conducting detailed CDD at the outset of the relationship and on an ongoing basis where they know or suspect that the business relationship is with a PEP.

All licenceholders must assess which countries with which they have financial relationships are most vulnerable to corruption. Licenceholders that are part of an international group might also use the group network as another source of information.

Where licenceholders do have business in countries vulnerable to corruption, they must establish who are the senior political figures in that country and, must seek to determine whether or not their customer has any connections with such individuals (e.g. they are immediate family or close associates). Licenceholders should note the risk that individuals may acquire such connections after the business relationship has been established.

Licenceholders should be most vigilant where their customers are involved in those businesses which appear to be most vulnerable to corruption, such as, but not limited to, oil, construction or arms sales.

Paragraphs 8, 10 and 15 of the Codes require licenceholders to have in place enhanced CDD measures to address PEP risk.

In particular, enhanced CDD must include:

(a) Appropriate procedures to determine, as far as reasonably practicable, whether an applicant for business, a customer, any natural person having power to direct the activities of an applicant for business or a customer, a beneficial owner or a known beneficiary of a legal arrangement is a PEP.

(b) Close scrutiny of any complex structures (e.g. involving legal persons, legal arrangements and multiple jurisdictions) so as to establish that there is a clear and legitimate reason for using such structures and a financial centre such as the Isle of Man. It should be borne in mind that most legitimate political figures would expect their personal affairs to be undertaken in a more than usually open manner, rather than the reverse.

(c) Every effort to establish the source of income/wealth (including the economic activity that created the wealth) as well as the source of funds involved in the relationship, establishing that these are legitimate, both at the outset of the relationship and on an ongoing basis.

(d) Approval of senior management before commencing the business relationship and regular review, on at least an annual basis, of the development of the relationship.

(e) Close scrutiny of any unusual features, such as very large transactions, the use of government or central bank accounts, particular demands for secrecy, the use of cash or bearer bonds or other instruments which break an audit trail, the use of small and unknown financial institutions in secrecy jurisdictions and regular transactions involving sums just below a typical reporting amount.

There should be full documentation of the information collected in line with the above. Given the above safeguards, the Commission would not necessarily expect licenceholders to avoid or close relationships with PEPs. If the risks are understood and properly addressed, then the acceptance of such persons becomes a commercial decision as with all other types of customer.

New and existing customers may not initially meet the definition of a PEP. Licenceholders should, as far as practicable, be alert to public information relating to possible changes in the status of its customers with regard to political exposure. Where an existing customer is subsequently found to be a PEP, senior management approval to continue the relationship must be sought.

Licenceholders should be aware of guidance from the United States of America on enhanced security for transactions that may involve the proceeds of foreign official corruption. This can be found on the Internet at www.federalreserve.gov.

Licenceholders may wish to make use of independent electronic data sources which can be of particular value in the context of business relationships with PEPs.

Licenceholders should not enter into or continue a business relationship where they know or have reasonable grounds to suspect that the funds derive from bribery, corruption or the misuse of national or supranational assets, without prejudice to any other obligation they may have under criminal law or other applicable laws. However, closing out any such relationship must be subject to preliminary discussion with the FCU.

3.6

Other high-risk customers

High risk customers may include high net worth individuals ("HNWI") particularly in connection with the provision of banking services. Reference to banking services within the Codes is not limited to deposit taking, but involves the whole range of private banking and wealth management services provided to high net worth individuals.

Although HNWI is a recognisable term used to define a certain class of customer, on the Isle of Man there is no legal definition and each licenceholder will have its own criteria for defining HNWIs. The affairs of HNWIs are on the whole more complex and varied than those of the average customer, and may involve for instance complex structures, multiple and interlinked products or services, and a high average value and volume of transactions.

The characteristics of HNWI relationships can represent an increased risk of money laundering, and licenceholders should ensure that they understand and manage the risk accordingly and make special provisions for HNWIs in their customer acceptance procedures and in their monitoring programmes.

High risk customers may also include legal persons with nominee shareholders or shares in bearer form and legal arrangements. The most significant feature from a money laundering and terrorist financing perspective with respect to legal persons and legal arrangements is the ability to hide the true beneficial ownership of the entity or the assets involved in the business relationship.

A legal person with nominee shareholders which is administered by a licensed fiduciary business in an equivalent jurisdiction which regulates fiduciary businesses for the prevention of money laundering and terrorist financing may present a lower risk than a legal person in a non-equivalent jurisdiction which does not regulate fiduciary businesses. This is because the fiduciary business administering the entity or arrangement should be subject to AML/CFT legislation requiring information and verification of the beneficial ownership and regulatory oversight to ensure that the requirements are complied with.

Whether or not a legal person with nominee shareholders or a legal arrangement presents a higher risk may depend upon the complexity of the structure that it forms a part of and the opportunities within the structure for obscuring the true beneficial ownership of the entity or assets.

Other high risk customers may also include:

- . persons or legal arrangements resident or located in jurisdictions with insufficient application of the FATF Recommendations;
- . persons who are the subject of a warning issued by a competent authority; or
- . a situation which by its nature presents a risk of money laundering or terrorist financing.

Enhanced CDD procedures should also be applied where a licenceholder has any reason to believe that an applicant for business has been refused banking or other financial services by other institutions.

These scenarios are not exhaustive, and a licenceholder's own risk assessment may highlight further instances where an applicant for business or persons connected with the applicant for business, such as underlying principles, directors and beneficial owners, may pose a higher risk.

Whether or not an applicant for business falling within one of the above categories or scenarios in fact presents a higher risk of money laundering or terrorist financing is dependent upon the specific circumstances pertaining to each particular applicant for business and the licenceholders' risk assessment.

Where an applicant for business falls within a scenario which may pose a higher risk, licenceholders must document their consideration of those persons and their decision as to whether or not to treat that applicant for business as higher risk. This must include clearly documenting the full rationale behind this decision.

Where the licenceholder knows or suspects money laundering or terrorist financing or where there is anything which causes the licenceholder to doubt the identity or bona fides of the applicant for business, or beneficial owner, enhanced CDD is required. In these circumstances, there is no discretion as to whether or not to apply enhanced CDD.

Enhanced CDD procedures must be applied to all customers, where there is a higher risk of money laundering or terrorist financing as per paragraph 8 of the AML Code. Where customers pose a higher risk of terrorist financing, paragraph 3(4) of the CFT Code requires licenceholders to either undertake enhanced CDD or conduct an adequate investigation. However, because the AML Code requires licenceholders to undertake enhanced CDD where there is a higher risk of terrorist financing, it could be a breach of the AML Code should a licenceholder choose to undertake an adequate investigation instead of enhanced CDD.

Therefore, the Commission is of the view that in order to comply with both the AML Code and the CFT Code, it is necessary that where there is a higher risk of money laundering and / or terrorist financing, licenceholders must undertake enhanced CDD procedures.

In the Codes paragraph 8(3) outlines that enhanced CDD involves:

"(a) considering whether additional identification data needs to be obtained; Deleted: Anti-Money Laundering AML/CFT Handbook Customer due diligence Isle of Man Financial Supervision Commission January 2009 40

(b) considering whether additional aspects of the identity of the applicant for business need to be verified; and

(c) considering what ongoing monitoring should be carried out in accordance with paragraph 15."

In considering what enhanced CDD is appropriate, it is necessary to recognise that the information requirements for identifying and reporting suspected terrorist financing may be different from those of money laundering. Money laundering involves the proceeds of crimes which have already taken place. Terrorist financing may also involve the proceeds of crime, but equally it may involve completely clean funds. In terrorist financing situations, it is the destination of the funds which is of primary importance as they may be used to finance future terrorist acts, organisations, resources and support networks.

In undertaking enhanced CDD where there is higher risk of terrorist financing, licenceholders should therefore have particular regard to their customer's relationships and the destination of the funds which will, do or have formed part of the licenceholder's relationship with its customer.

Licenceholders must recognise that the value of funds involved in terrorist financing is different from money laundering. To undertake a terrorist act, does not necessarily involve large sums of money. Enhanced CDD should not therefore be limited to higher value transactions.

If, following consideration of whether additional information, verifications and ongoing monitoring are needed a licenceholder determines that there is value in obtaining further information or documentation, such information or documentation should be obtained.

Irrespective of whether a licenceholder ultimately determines that additional measures are appropriate, licenceholders must document their consideration and the full rationale behind the decision. It is necessary for licenceholders to be able to demonstrate their deliberations in order to demonstrate that the enhanced CDD requirements in the Code have been met.

3.7

Shell banks

A shell bank is a bank incorporated in a jurisdiction in which it has no physical presence and which is not affiliated with a financial services group which is subject to effective consolidated supervision. The jurisdiction is unlikely to be able to exercise adequate supervision over the shell bank's compliance with AML/CFT requirements. In addition, within some jurisdictions, the licensing requirements for shell banks have historically been weak, permitting some shell banks to be operated by, or controlled by, individuals who are not fit and proper to do so.

As required by paragraph 26 of the Codes, licenceholders must not enter into or continue relationships with shell banks. Licenceholders must also take adequate measures to ensure that they do not enter into or continue a relationship with a bank that permits its accounts to be used by a shell bank.

3.8

Correspondent banking services

Correspondent banking is the provision of banking services by a bank in one jurisdiction (the correspondent bank) to another bank in another jurisdiction (the respondent bank). Used by banks throughout the world, correspondent accounts enable banks to conduct business and provide services that the bank does not offer directly. There are similar arrangements in other areas of financial services.

Licenceholders must not enter into or continue correspondent banking relationships with shell banks. In addition, licenceholders must be satisfied that the respondent banks with which they have correspondent banking relationships do not permit their accounts to be used by shell banks.

Before entering into a business relationship or one-off transaction involving correspondent banking services or other similar arrangements, licenceholders must take steps additional to CDD requirements as per Paragraph 13 of the Codes as follows:

- (a) obtain sufficient information about the respondent bank to understand fully the nature of its business;
- (b) determine from publicly available information the respondent bank's reputation and quality of supervision including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;
- (c) assess the respondent bank's AML/CFT procedures and controls, and ascertain that they are adequate and effective;
- (d) obtain senior management approval, i.e. sign off before establishing new correspondent banking relationships; and
- (e) document the respective AML/CFT responsibilities of the licenceholder and the respondent bank.

Where correspondent banking services involve a payable-through account, a licenceholder must be satisfied that the respondent bank -

- (a) has taken steps complying with the requirements of Recommendation 5 (CDD and record keeping) of the FATF Recommendations with respect to every customer having direct access to the account; and
- (b) will provide relevant evidence of the customer's identity on request.