ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM HANDBOOK

~~JANUARY~~ May 2018

Whilst this publication has been prepared by the Financial Services Authority, it is not a legal document and should not be relied upon in respect of points of law. Reference for that purpose should be made to the appropriate statutory provisions.

Contact:
AML Unit, Enforcement Division
Financial Services Authority
PO Box 58,
Finch Hill House,
Bucks Road, Douglas
Isle of Man
IM99 1DT

Tel: 01624 646000 Fax: 01624 646001
Website: www.iomfsa.im Email: aml@iomfsa.im

Part 4 – Customer Due Diligence 35

Part 5 – Specified Non-profit Organisations 75

Part 6 – Simplified Customer Due Diligence 77

Part 7 – Unusual and Suspicious Activity 101

Part 9 – Miscellaneous 157

Glossary & Acronyms 161

Appendices

Sector Specific Guidance

Separate guidance documents can be found on the IOMFSA’s website for the sectors listed below. These documents are to be read in conjunction with this master document.

Trust Service Providers and Corporate Service Providers
Banking
Funds / Investment Businesses
Money Services Businesses
Isle of Man Post Office
Payroll Agents
Advocates and Registered Legal Practitioners
Accountants and Tax Advisors
Estate Agents
Money Lenders
Specified Non-Profit Organisations
High Value Goods Dealers

Part 1 – Introductory

1.1 Foreword

This document is designed to provide guidance to those businesses licensed under the Financial Services Act 2008[1], or registered under the Designated Businesses (Registration and Oversight) Act 2015. These persons, which are businesses in the regulated sector as defined by Schedule 4 to the Proceeds of Crime Act 2008 ("POCA") are referred to throughout this document as "relevant persons". Other persons included in Schedule 4 to POCA may also use this guidance as a reference tool if they wish.

The Isle of Man has a reputation as a sound and well regulated jurisdiction. This is confirmed by the IMF report of August 2009,the MONEYVAL 2013 follow up report, and the MONEYVAL Onsite Assessment 2016 . It is essential for the Island to maintain this reputation in order to continue attracting legitimate investors with funds and assets that are clean and untainted by criminality. Anyone in the Isle of Man that assists in laundering the proceeds of crime or is involved in the financing of terrorism or proliferation[2], whether knowingly, unintentionally, or without regard to what it may be facilitating through the provision of its products or services, could face law enforcement investigation, the loss of reputation and the possibility of regulatory sanctions or criminal proceedings. Involvement of a relevant person with criminal or terrorist property will also damage the reputation of the Isle of Man as a whole.

The Isle of Man legislative framework for anti-money laundering and countering the financing of terrorism ("AML/CFT") has been in place and effective since 1990[3]. This legislation has been regularly updated to deal with new threats that have emerged and has strengthened the Isle of Man's defences against all crimes money laundering and international terrorism. In addition to the legislation being in place, the continued

[1] If a fiduciary is part of a group which is subject to AML/CFT guidance issued under the Insurance Act and / or the Retirement Benefits Schemes Act 2000 the fiduciary may follow that guidance as long as the business can demonstrate compliance with the Code.
[2] Note that where money laundering and the financing of terrorism (ML/FT) is stated this also refers to proliferation.
[3] Criminal Justice Act 1990 and Prevention of Terrorism Act 1990.

vigilance and co-operation of the financial sector and designated non-financial businesses and professions ("DNFBPs") is vital to maintain these defences.

The Island's current anti-money laundering requirements are detailed in the Anti-Money Laundering and Countering the Financing of Terrorism Code 2015 ("the Code") which applies to all relevant persons. The Code is made under Section 157 of POCA

The Island's anti-terrorism legislation can be found in the Anti-Terrorism and Crime Act 2003 ("ATCA"), the Anti-Terrorism and Crime (Amendment) Act 2011 and the Terrorism and Other Crimes (Financial Restrictions) Act 2014. Section 68 of the Terrorism and Other Crimes (Financial Restrictions) Act 2014 requires the DHA to publish a Code for the purposes of preventing and detecting the financing of terrorism ("FT") and proliferation. The Code also has provisions in relation to this area.

The Island's National Risk Assessment ("NRA") has now been completed. The document can be found here.

1.2 Status of Guidance

Section 12 of the Financial Services Act 2008 and Section 32 of the Designated Businesses (Registration and Oversight) Act 2015 state that the Authority may issue and publish guidance as it considers appropriate.

The Authority issues guidance for various purposes including to illustrate best practice, to assist relevant persons in complying with legislation and to provide examples or illustrations. The guidance in this Handbook is not law, however it is persuasive. Where a person follows guidance this would tend to indicate compliance with the legislative provisions, and vice versa.

This Handbook is written to supplement the Code and assist relevant persons in their compliance with the legislation. The main body of the Handbook, which consists of Parts 1 to 9, applies to all businesses. Additional guidance which is specific to different industries will be published separately on the Authority's website, this is referred to in this document as "sector specific guidance".

The sector specific sections build on the core document for each business sector and should not be read in isolation. The sector specific sections help those sectors identify risk areas unique to that sector or provide refined guidance in respect of due diligence measures where a one-size fits all approach may not work. Finally these areas are illustrated with case studies to assist in providing context to these threats and vulnerabilities.

If a relevant person has any particular areas that they would like to see included in the Handbook or the sector specific guidance the Authority would welcome feedback on this.

1.3 Purpose of the Handbook

1. The purpose of this Handbook is to assist relevant persons in understanding their obligations and to enable the Island to maintain and further its high standards;

2. summarise and explain the requirements of the primary and secondary AML/CFT legislation in the Isle of Man;
3. assist relevant persons to comply with the requirements of POCA, ATCA, the Terrorism and Other Crimes (Financial Restrictions) Act 2014 and the Code by specifying best practice;
4. set the minimum criteria to be followed by all relevant persons in the Isle of Man where there is knowledge, suspicion or reasonable grounds to suspect ML and/or FT;
5. promote the use of a proportionate, risk-based approach to Customer Due Diligence ("CDD") and Enhanced Due Diligence ("EDD") measures;
6. ensure compliance with international standards by the Isle of Man; and
7. emphasise the particular ML/FT risks of certain of the services and products offered by relevant persons in the Isle of Man.

This Handbook does not aim to prescribe an exhaustive list of recommended AML/CFT practices. A reasonable, proportionate and intelligent risk-based approach is required. Each relevant person must consider its own particular circumstances. This includes additional measures that may be necessary to prevent its exploitation and that of its products and services by persons seeking to launder criminal property or to finance terrorism.

The Authority recognises that relevant persons may have systems and procedures in place which, whilst not identical to those outlined in the Handbook, nevertheless impose controls and procedures which are at least equal to if not higher than those contained in the Handbook. This will be taken into account by the Authority when assessing the adequacy of a business's systems and controls.

1.4 Failure to Comply with the AML/CFT Code

Paragraph 41 of the Code sets out the offences for contravening the requirements of the Code:

1. on summary conviction, breach of a provision of the Code carries a maximum custody period of twelve months or a fine not exceeding £5,000, or both.
2. on conviction on information, breach of a provision of the Code carries a maximum custody period of 2 years or a fine, or both.

Paragraph 41(2) of the Code states that a court **may** take account of any relevant supervisory or regulatory guidance given by a competent authority that applies to that person.

The Authority will take account of this Handbook in assessing the level of compliance with the Code when conducting its supervisory or oversight visits / meetings. The level of compliance of a relevant person will therefore be directly relevant to its licensed or registered status and any assessment of the fitness and propriety of its owners or other key persons where appropriate. Failure to comply with the minimum requirements of the Code may be regarded by the Authority as an indication of:

1. conduct that is not in the best economic interests of, or which damages the reputation of the Isle of Man; and/or
2. lack of fitness and propriety;

This may therefore result in regulatory action at the discretion of the Authority and in certain cases, it may result in revocation of a licence or de-registering of a business.

1.5 FATF Recommendations

The Financial Action Task Force ("the FATF") is an independent inter-governmental body that develops and promotes policies to protect the global financial system against ML, FT and the financing of the proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global standards in respect of AML/CFT.

In June 2012 the Council of Ministers issued a strong commitment to following international standards in combating ML, FT and proliferation of weapons of mass destruction. In May 2017 the Isle of Man Government published A Progress Report on Anti-Money Laundering and Combatting the Financing of Terrorism Matters In the Isle of Man Government issued its AML/CFT National Strategy for 2017 - 2020. The document can be found here.

A link to the 2012 FATF 40 Recommendations, upon which our legislation and this guidance is based, can be found here.

In October 2012, the Island joined the MONEYVAL mutual evaluation process. MONEYVAL is a FATF style regional body. The aim of MONEYVAL is to ensure that its member states have in place effective systems to counter ML and FT and comply with the relevant international standards in these fields.

MONEYVAL assesses its members' compliance with all relevant international standards in the legal, financial and law enforcement sectors through a peer review process of mutual evaluations. Its reports provide recommended actions on ways to improve the effectiveness of domestic regimes to combat ML and FT and the capacity of its members to co-operate internationally in these areas. MONEYVAL also publishes typologies and procedures to assist jurisdictions in compliance with the international standards.

1.6 Compliance Culture

The Authority expects relevant persons to give due priority to establishing and maintaining an effective compliance regime and culture. The Authority recognises that effective AML/CFT policies and procedures can only be delivered through partnership with the industry and, accordingly, expects all relevant persons to ensure that they establish an open and positive approach to compliance and AML/CFT issues amongst all employees.

The board and senior management have a responsibility to ensure that a relevant person's systems and controls are appropriately designed and implemented, and are effectively operated to reduce the risk of the business being used in connection with ML/FT.

The board or senior management of a relevant person must establish documented systems and controls which:

1. undertake risk assessments of its business and its customers[4];
2. determine the true identity of customers and any beneficial owners and controllers;
3. determine the nature of the business that the customer expects to conduct and the commercial rationale for the business relationship;
4. require identification information to be accurate and relevant (relevant persons are not automatically required to replace identity documents simply because they have expired since first being obtained);
5. require business relationships and transactions to be effectively monitored on an ongoing basis with particular attention to transactions which are complex, both large and unusual, or an unusual pattern of transactions which have no apparent economic or lawful purpose;
6. compare expected activity of a customer against actual activity;
7. apply increased vigilance to transactions and relationships posing higher risks of ML/FT;
8. ensure adequate resources are given to the Money Laundering Reporting Officer ("MLRO") and the compliance function to enable the standards within this Handbook to be adequately implemented and periodically monitored and tested;
9. ensure procedures are established and maintained which allow the MLRO and any other designated person to have access to all relevant information, which may be of assistance to them in considering suspicious activity reports ("SARs");
10. require a disclosure to the Financial Intelligence Unit ("FIU") when there is knowledge or suspicion or reasonable grounds for knowing or suspecting ML and/or FT, including attempted ML and/or FT; and;
11. maintain records for the prescribed periods of time.

Relevant persons must adopt a robust approach and not refrain from asking their customers "awkward" questions in circumstances of unusual activity. Any reluctance or failure by the customer to provide credible and verifiable answers should lead the relevant person to consider the reason for this reluctance, consider if this makes them suspicious and then take appropriate action.

A hierarchical approach within a business may hinder an effective system of AML/CFT control. Relevant persons need to recognise and address this. The human element is very important in this context in that policies and procedures only work if they are understood, followed and enforced by those required to comply with them. The inter-relationships between different employees within a relevant person and between employees and customers, can result in the following damaging barriers:

1. senior management being unwilling to lead on the concept of the need for sound corporate ethics;

[4] It should be noted that the Code defines a customer of a relevant person (excluding SNPOs) as a person seeking to form a business relationship or to carry out an occasional transaction, or carrying on a business relationship, or carrying out an occasional transaction. Where the term 'customer' is used in this Handbook it should also be considered that it also refers to the 'beneficial owner'; which is the natural person owning or controlling the customer on or on whose behalf a transaction or activity is being conducted.

2. more junior employees assuming that their concerns or suspicions are not significant;
3. employees being unwilling to subject high value (therefore important) customers to effective CDD checks;
4. management or customer relationship managers outside the Isle of Man pressurising employees in the Isle of Man to transact without obtaining all relevant CDD and business relationship information;
5. employees being unable to understand the commercial rationale for customer relationships and the use of certain products / services, so that potentially suspicious activity is not identified;
6. lack of time and/or resources to address concerns generating a tendency for line managers to discourage employees from raising concerns; and
7. conflict between the desire on the part of employees to provide a confidential and efficient customer service and the requirement for employee vigilance in respect of prevention and detection of ML/FT.

1.7 Risk Based Approach

The FATF Recommendations state that AML/CFT requirements must allow a business to adopt a risk-based approach towards the prevention and detection of ML/FT. Provision for using a risk based approach in meeting the AML/CFT requirements is made in the Code.

It is very important to note that POCA, ATCA and the Code do not prohibit or prevent any streams of business, any customers or systems, unless they are undertaking ML/FT. The legislation requires only that the risks posed by customers, products and systems are identified, mitigated and the mitigating factors/controls are documented and reviewed periodically.

This Handbook suggests ways in which the relevant person can comply with the requirements of the AML/CFT legislation. The application of a risk based approach provides a strategy for managing potential risks by enabling relevant persons to subject customers to proportionate controls and oversight. Relevant persons will always have to make their own determination as to the risks based on their respective circumstances and should always avoid a “tick box” approach. An assessment of risk should always be documented, reasonably and objectively justifiable and sufficiently robust so as to demonstrate that the business acted reasonably. Finally, while a risk based approach grants a wide degree of discretion, parameters set by law or regulation may limit that discretion.

1.7.1 What is risk?

Risk can be seen as a function of three factors and ideally, a risk assessment involves making judgments about all three of these elements:

- **THREAT** - person or group of people, an object or an activity with the potential to cause harm.
- **VULNERABILITY** - those things that can be exploited by the threat or that may support or facilitate its activities.

- **CONSEQUENCE** - the impact or harm that ML or FT may cause.

1.7.2 What is mitigation?

Relevant persons must then take appropriate steps to mitigate any risks that have been identified. This will involve determining the necessary controls or procedures that need to be in place in relation to a particular part of the business in order to reduce the risk identified. The documented risk assessments that are required to be undertaken by the Code will assist the business to develop a risk based approach.

A risk based approach:

1. recognises that the ML/FT threat to a relevant person varies across customers, jurisdictions, products and delivery channels;
2. allows a relevant person to be flexible in relation to the AML/CFT requirements in a way that matches the risk profile of the business itself and the customers of that business;
3. allows a relevant person to apply its own approach to procedures, systems and controls and arrangements in particular circumstances; and
4. helps to produce a more cost effective system by applying resources to where the risks are assessed as greatest.

Systems and controls may not always prevent and detect all ML/FT. A risk-based approach will, however, serve to balance the cost burden placed on relevant persons and on their customers with a realistic assessment of the threat of a business being used in connection with ML/FT. It focuses effort where it is needed and has most impact.

1.8 Assessing Compliance with Risk Based Approach

Relevant persons should avoid rigid internal systems of control as these can encourage the development of a 'tick box' mentality that can be counter-productive. Internal systems should require employees to think about the risks posed by individual customers and relationships and to mitigate appropriately and document their thought processes. The Authority, or its delegates, must be able to see clear, documented rationale of how risks have been assessed and then how these risks have been mitigated or controlled.

Any risk assessment systems used by the relevant person should be reviewed regularly to check the system is effective and action should be taken to remedy any identified deficiencies.

Part 2 – General Requirements

2.1 General Requirements

The Code requires relevant persons to have certain procedures in place. This Handbook is designed to aid relevant persons in the establishment and operation of those procedures. Paragraph 4 of the Code requires a relevant person to:

1. establish, maintain and operate procedures in relation to the following —

   (a) risk assessment;
   (b) ongoing monitoring;
   (c) CDD;
   (d) record keeping and compliance;
   (e) staff appointment and training;
   (f) appropriate reporting and disclosures; and
   (g) any other internal controls and communication procedures that are appropriate for the purposes of preventing and detecting ML/FT.

2. take appropriate measures for the purpose of making employees and workers aware of —

   (a) the procedures established, maintained and operated above; and
   (b) the AML/CFT requirements;

3. monitor and test compliance with the Code in accordance with paragraph 29;

4. provide education and training to its staff in accordance with paragraph 31; and

5. comply with paragraphs 38 and 40 which is the use of Shell Banks and fictitious/anonymous/numbered accounts respectively.

These procedures and controls must be approved by the senior management of the relevant person and evidence of this approval should be made available to competent authorities upon request. Examples of such evidence include board minutes or similar documentary evidence.

It is a criminal offence for a relevant person to fail to establish, maintain and operate the procedures listed above. Where such an offence is committed with the consent or connivance of, or is attributable to neglect on the part of an officer of the business, he too shall be deemed to have committed a criminal offence. The definition of “officer” includes a director, manager, board member or secretary and a person purporting to act as such.

Part 3 – Risk Assessment and Ongoing Monitoring

3.1 Business Risk Assessment

A relevant person must, under paragraph 6 of the Code, undertake a business risk assessment to estimate the risk of ML/FT on the part of the relevant business and its customers. As explained at section 1.7.1 of this Handbook, a risk assessment involves making a judgement of a number of elements including threat, vulnerability and consequence.

It should also consider the extent of its exposure to risk by reference to a number of additional factors which are explained in this section. The examples provided are not exhaustive and other factors may need to be considered depending on the nature of the business and its activities.

The relevant person must record and document its risk assessment in order to be able to demonstrate its basis. The assessment must be undertaken as soon as reasonably practicable after the relevant person commences business and regularly reviewed and

amended to keep it up to date. It is expected that this risk assessment is reviewed at least annually and this review should be documented to evidence that an appropriate review has taken place.

Any risks that have been identified should be properly mitigated by policies, procedures and controls. The relevant person should also document the mitigating factors and controls put in place to provide an audit trail of how the assessed risks have been mitigated.

Note that relevant persons who are licensed under the Financial Services Act 2008 ("FSA") are under a further obligation to conduct a business risk assessment under Rule 8.6 of the Financial Services Rule Book ("FSRB"). It is acceptable for a relevant person to cover the requirement of both paragraph 6 of the Code and Rule 8.6 in one assessment, however the overall AML/CFT score/assessment must not be impacted by non-AML factors. The Authority suggests that a relevant person may wish to have an overall risk score and a separate AML/CFT score

Paragraph 6(3) of the Code requires businesses to assess 5 key areas when undertaking the business risk assessment:

(a) the nature, scale and complexity of the relevant person's activities;
(b) the products and services provided by the relevant person;
(c) the persons to whom, and the manner in which the products and services are provided;
(d) reliance on third parties for elements of the CDD process; and
(e) technological developments.

Businesses should also consider the findings of the NRA in their business risk assessment.

Each of the areas specified by the Code, and examples of what factors a business should consider as a part of assessing these areas, are detailed in the following sections.

3.1.1 The nature, scale and complexity of its activities

- Consider the services provided by the business and how those services might be abused for ML/FT.
- Actively involve all members of senior management in determining the risks (threats and vulnerabilities) posed by ML/FT within those areas for which they have responsibility.
- Consider any organisational factors that may increase exposure to the risk of ML/FT e.g. business volumes and outsourcing aspects of regulated activities or compliance functions.
- Consider the nature, scale and complexity of its business including the diversity of its operations, the volume and size of its transactions, and the degree of risk associated with each area of its operation.
- Consider the jurisdictions in which the business operates, any particular threats from those jurisdictions, any particular vulnerabilities within the

organisation in those jurisdictions.Consider the scale on which the services are provided and linked to this, any vulnerabilities in the level of compliance resources available.
- Consider whether the business model provides for complex structures and what risks this poses to the business.
- Consider the findings of the NRA in relation to the business sector.

3.1.2 Its customers, products and services

- Consider the threats posed by the types of customers the business markets to. Some examples include, politically exposed persons ("PEPs"); high net worth individuals, those from or operating in a higher risk jurisdiction; the use of bearer instruments; and non face-to-face business.
- Consider the vulnerabilities of the services or products offered and how they could be abused for ML/FT.
- Consider jurisdictional factors such as high levels of organised crime, increased vulnerabilities to corruption and inadequate frameworks to prevent and detect ML/FT in countries where it may have customers such as, though not exclusively, the countries and territories on Appendices D(a) and D(b) will affect the risk.
- Whether the customer base has any involvement in those businesses which are likely to be most vulnerable to corruption such as oil, construction or arms sales.
- Certain characteristics of the products and whether there are any increased vulnerabilities such as high volumes of cash, bearer instruments, virtual currencies or other untraceable/anonymous medium.

3.1.3 The manner in which it provides these products and services to its customers

- Relevant persons should consider how they deliver products and services to their customers and the extent to which this might increase the risk. Risks are likely to be greater when relationships can be established remotely ("non-face-to-face"), or when they may be controlled remotely by the customer ("straight–through" processing of transactions).
- The type of product should be considered, the higher risk products or services are more likely to be those with high values and volumes; where unlimited third party funds can be freely received and those where funds can regularly be paid to third parties without CDD on the third parties being obtained.
- The speed with which products and services can be delivered or transactions undertaken.

3.1.4 The reliance which is placed on any third parties for elements of the CDD collected

- Consider how reliance on third parties is prompted and agreed on.
- Consider who these third parties are on which reliance is placed, including any reputational issues, the quality of relationships with such third parties and previous experiences.
- Consider the extent and type of any reliance placed or to be placed on third parties.
- Consider the extent of the information being provided by the third party and who has actually met the customer face-to-face (chains of information).
- Consider any jurisdictional issues in connection with reliance placed on third parties.
- Consider the results of any testing undertaken on the third party's procedures and the responses to any previous requests for documentation.
- Consider the extent of any outsourcing undertaken.
- Consider the quality of the provider for any outsourced functions including any reputational issues, previous experiences with the provider, results of any audits, assessments or inspections where the material generated as a result of outsourcing has been reviewed.

3.2 Technological Developments Risk Assessment

Under paragraph 8 of the Code, a relevant person is required to undertake and document a risk assessment prior to the launch or implementation of new products, new business practices or delivery methods including new delivery systems. The outcome of a technological risk assessment must also be considered as a part of the business risk assessment detailed in paragraph 6 of the Code and part 3.1 of this Handbook.

The relevant person should assess the use of developing technologies for both new and pre-existing products such as:

- digital information storage including cloud computing;
- digital or electronic documentation storage;
- electronic verification of documentation;
- data and transaction screening systems; or
- the use of virtual or digital currencies.

For completeness, the assessment should consider the operational risks, reputational risks and legal risks posed by the use of new technologies in the context of ML/FT. Appropriate action should be taken to mitigate the risks that have been identified.

3.2.1 Operational risks

Operational risks arise from the potential loss that could be incurred due to significant deficiencies in system reliability or integrity. Operational risk will also increase in proportion to the amount of reliance placed on outside service providers and external experts to implement, operate, and support portions of electronic systems.

Also, the rapid pace of technological change carries risk in itself. For example, staff may not fully understand the nature of new technology, resulting in operational problems with new or updated systems. Channels for distributing software updates could pose risks in that criminal or malicious individuals could intercept and modify the software.

It will have to be considered whether any of the factors above would have any impact in relation to the relevant person continuing to meet the AML/CFT requirements.

3.2.2 Reputational risks

Reputational risk may arise when systems or products do not work as expected and cause negative public reaction. The event of this happening would have to be assessed by the relevant person and any risk should be mitigated. In particular, if this affected systems that were involved with the collection or maintenance of customer information this may lead to serious reputational concerns.

3.2.3 Legal risks

Legal risks arise from violations or non-compliance with legislation such as the Code. Electronic money systems may be attractive to money launderers or those financing terrorism if the systems offer liberal balance and transaction limits, but provide for limited auditability of transactions. Relevant persons may also face increased difficulty in applying traditional crime prevention and detection methods because of the remote access by customers of the systems.

It is recognised that where relevant persons may be part of a larger group, the parent may introduce new products, systems or procedures without input from the Isle of Man based branch. It is important to note that this paragraph of the Code requires that the business identifies and mitigates any risks arising from the proposed system rather than places a moratorium on new technologies.

3.3 Customer Risk Assessment

Paragraph 7 of the Code requires that a customer risk assessment estimating the risk of ML/TF must be undertaken prior to the establishment of a business relationship or carrying out an occasional transaction, with or for, that customer. This risk assessment

must be documented in order to be able to demonstrate its basis. The customer risk assessment may have to take into account that not all CDD and relationship information might have been collected yet, it should be a living document that is revisited and reviewed as more information about the customer and relationship obtained.

The initial risk assessment of a particular customer will help determine:

- the extent of identification information to be sought;
- any additional information that needs to be requested;
- how that information will be verified; and
- the extent to which the relationship will be monitored on an ongoing basis.

Care has to be exercised under a risk-based approach. Being identified as carrying a higher risk of ML/FT 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 ML/FT does not mean that the customer presents no risk at all.

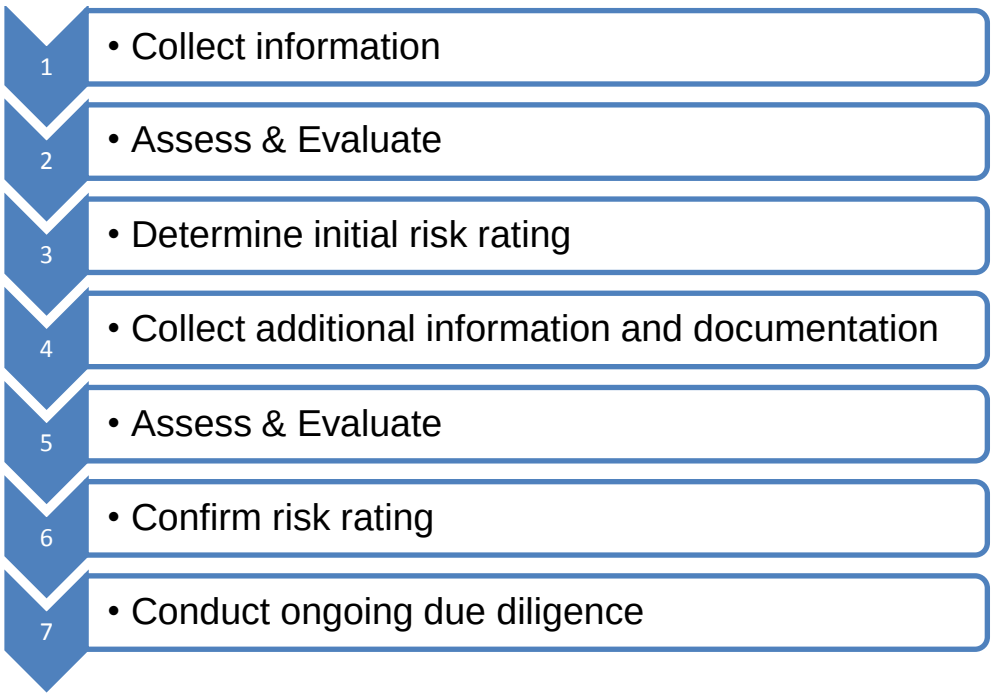
In order to complete a meaningful risk assessment, it is recommended that information should be gathered prior to the assessment, although this may not always be possible. Upon completion of the risk assessment any additional information, evidence or clarification should be sought in the event that circumstances remain unclear.

It should be noted that the Authority has no objection to a relevant person having higher risk customers, provided that they have been adequately risk assessed and any mitigating factors have been documented. If the customer is assessed as presenting a higher risk EDD must be obtained. Also, it should be noted that where a customer is assessed as posing a higher risk certain concessions within the Code no longer apply. This is explained further in Part 6 of this Handbook.

Paragraph 7 of the Code states that the customer risk assessment should have regard to all risk factors including:

(a) the business risk assessment carried out under paragraph 6 of the Code;
(b) the nature, scale, complexity and location of the customer's activities;
(c) the persons to whom and the manner in which the products and services are provided; and
(d) reliance on third parties for elements of the CDD process.

The following diagram sets out the basic risk assessment process:



When assessing the risks posed by a customer, the relevant person should consider all risk factors that are known and ensure that all of these factors are included into the customer's risk profile taking care that any mitigating factors are fully documented. A relevant person must be able to objectively and reasonably justify a risk assessment classification and document those justifications. The relevant person should also ensure that its internal sign off procedure in relation to customer risk assessments is appropriate.

The Authority would expect relevant persons to avoid a tick box approach when assessing risks and consider each customer on a case by case basis, looking at any risks they pose along with any mitigating factors. These factors should be documented and details provided of how any risks identified are then mitigated. The Authority would have no objection to templates or forms being used during the risk assessment, however it should be carefully considered how these work, what the scoring system is and how the score is reviewed / overridden. It should also be ensured that the score only takes into account factors relevant to ML/FT.

As with business risk assessments, customer risk assessments must be reviewed on a regular basis to ensure they remain up to date and to assess any changes of the risk profile due to changes in the customer's circumstances. It is expected that the review of the risk assessment is documented to evidence that an appropriate review has taken place. Regarding frequency of the reviews, customer risk assessments should be reviewed:

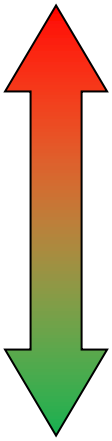
- at least annually for higher risk customers;
- at least every 3 years for standard risk customers subject to sector specific guidance; and;
- at the point of a material change in the customer's circumstances, for example establishing connections with a higher risk jurisdiction or engaging in a higher risk business.

Where a customer has been identified as posing a higher risk of ML/FT and the relevant person is not satisfied that it is able to effectively mitigate those risks, the relevant person may consider the prospective customer to be of 'unacceptable risk' and decline from entering into a business relationship with or carrying out an occasional transaction for that customer. Where such risks give rise to a suspicion of ML/FT then an internal disclosure must be made.

Relevant persons are encouraged to make decisions on 'unacceptable risk' customers on a case by case basis and to avoid implementing policies that support the wholesale de-risking of business segments. Further information on the subject of de-risking can be found in an FATF typology document available at the following link: FATF De-Risking Guidance.

Suggested Risk Classifications:

Relevant persons may use their own categories of risk classifications provided that they are able to demonstrate a correlation between their own categories and those listed below.



Unacceptable Risk:	If a relevant person is not satisfied that the risks identified can be effectively managed the business should be declined.
Higher Risk:	CDD must be undertaken and also EDD applies to all higher risk customers. (Note there maybe some further requirements where a PEP is involved).
Standard Risk:	CDD must be undertaken and in some cases simplified due diligence may be acceptable. Note there maybe some further requirements where a PEP is involved (Code paragraph 14).
Lower Risk:	Lower risk is likely to be used in exceptional circumstances only. See section 3.3.1 below. Lower risk customers face the same CDD requirements under the Code as standard risk customers, but the Authority will accept that methods of verification of identification may be less robust.

3.3.1 Lower risk

The Code makes reference to both those customers presenting a higher risk of ML/FT and to those customers that have not been identified as posing a higher risk which are referred to in this Handbook as "standard risk" customers. The Authority recognises that there may be exceptional circumstances where a relevant person considers a particular customer as presenting a lower risk of ML/FT than those customers assessed as standard risk.

Where a customer presents a lower risk of ML/FT, certain concessions in relation to verification of identity, detailed at sections 4.6.1, 4.7.1 and 4.7.2 of this Handbook, may be made available. Presenting a lower risk of ML/FT does not remove the requirement to undertake CDD or to conduct risk assessments.

Lower risk should be limited to customers who do not present any high risk factors (whether mitigated or not). Only customers that comply with all of the following factors may be considered lower risk for the purposes of these verification concessions:

- Natural person;
- Local, resident and conducting business face-to-face;
- Not High Net Worth;
- Only dealing with low value transactions which would be described as standard retail financial services;
- No foreign business or personal interests;
- Not cash based;
- Not complex – no legal persons or arrangements such as trusts as asset holding vehicles or part of more complex structures; and
- No intermediary / introducer / agency involvement.

However, a customer's compliance with all of the above factors does not necessarily mean that a customer should be treated as lower risk. Where a relevant person considers a customer to be a lower risk it must be able to objectively justify that the customer presents a much lower than standard risk of ML/FT. This should be considered on a case by case basis and should not be applied on a general basis (e.g. blanket risk assessing all IOM resident customers or all children's bank accounts as lower risk).

If a relevant person wishes to classify a customer as lower risk for purposes other than use of the verification concessions referred to above a customer risk assessment must be undertaken as per paragraph 7 of the Code taking into account all relevant factors. The requirements in the list above need not necessarily be met in such circumstances.

It should be noted that in this Handbook where a customer is referred to as standard risk this includes both standard and lower risk customers unless this is otherwise specified.

3.3.2 The business risk assessment

A relevant person should consider its findings from its own business risk assessment conducted under paragraph 6 of the Code. Any risk factors which are identified by the business should be applied to the profile of the customer.

3.3.3 The nature, scale, complexity and location of the customer's activities

Relevant persons should understand and consider risks inherent in the nature of the activity of its customer and the customer's business activities including factors such as the location of the activities, volume and size of transactions, use of complex structures etc. This also includes considering the customer's activities outside of the business relationship such as whether they are a PEP or if the nature of their business puts them at a higher risk of bribery, corruption or other criminal activity.

As an example, the arms trade and the financing of the arms trade are activities that pose multiple risks, such as:

- corruption risks arising from procurement contracts;
- politically exposed person (PEP) risks; and
- terrorism and terrorist financing / supplying risks.

The relevant person should compare the jurisdiction that the customer:

- is resident in;
- is located in; and
- or is conducting business activity related to the lists below:

List A – High risk list
List B – May be high risk list
List C – Equivalent jurisdiction list
→ See section 3.5

Sanctions lists
→ See section 7.3.5

A relevant person should also consider the ML/FT risks posed by jurisdictions not included in the lists mentioned above as there may be additional jurisdictions that pose a higher risk to their particular sector or customer type. Relevant persons should take into consideration typology reports for their business sector and their own experience in the industry.

3.3.4 The type of customers, products and services

In addition to considering and understanding the type/nature of customer (such as a natural person, legal person, legal arrangement or unincorporated association), relevant persons should also consider and understand the characteristics of the products and services they are providing to their customer and the manner in which they are being provided.

Consideration should be made as to the rationale of the customer requesting a particular product or service and whether this is consistent with their business profile / customer risk assessment.

Relevant persons should consider how the product will be delivered to the customer and the extent to which this might increase the risk. Risks are likely to be greater when the relationship has been established remotely ("non-face-

to-face"), or when it has been controlled remotely by the customer ("straight-through" processing of transactions).

The highest risk products or services are those with high values and volumes; those where significant or unlimited third party funds can be freely received; or those where funds can regularly be paid to third parties without CDD on the third parties being obtained.

All of this information should be used in determining and understanding the extent to which the products and services being provided are vulnerable to ML/FT abuse.

Generally, any form of legal entity or related service that enables individuals to divest themselves of ownership of property whilst retaining an element of control over it, is vulnerable. Some examples include, but are not limited to the following:

1. companies that can be incorporated without the identity of the ultimate owners or controllers being disclosed through the use of nominees;
2. certain forms of trusts or foundations including blind trusts, revocable trusts, dummy settlor trusts and settlor directed trusts where knowledge of the identity of the true underlying owners or controllers cannot be guaranteed;
3. the provision of nominee shareholders or nominee members;
4. companies issuing bearer shares or other bearer instruments;
5. correspondent banking relationships - a correspondent account can be used to transfer funds on behalf of unidentified third parties;
6. banking services for higher risk accounts or high-net worth individuals such as those offered by private banks;
7. wire transfers due to the speed and ease of transmission across jurisdictions;
8. any financial service or product that is capable of being provided on a non-face-to-face basis or controlled by a customer remotely;
9. business which is by its nature highly cash intensive or has a high turnover of near cash products (such as traveller's cheques); or
10. any service / product that involves the frequent use of high denominations of currency such as £50 or €500 notes.

3.3.5 The reliance which is placed on any third parties for elements of the CDD collected

Where reliance is placed on a third party for elements of CDD, for example an eligible introducer relationship, the relevant person must ensure that the identification information sought from the introducer (or other third party) is adequate and accurate. Relevant persons should consider the extent of the information being provided by the third party and also whether the third party has met the customer face to face.

A customer risk assessment must be undertaken on the introduced customer by the relevant person. The relevant person must not rely on a risk

assessment undertaken by the eligible introducer. The introducer must also be risk assessed in its own right. If the introducer or the introduced customer poses a higher risk of ML/FT, then the eligible introducer concession at 23(5) of the Code must not be used.

Please refer to Part 6 of the Handbook for further details

3.4 Ongoing Monitoring

Paragraph 9 of the Code requires relevant persons to monitor the conduct and activities of any business relationship. This covers the entire relationship including information held and transactions undertaken by the customer.

CDD information in respect of all customers should be reviewed periodically to ensure that it is accurate, and up to date. However, to be most effective, resources should be targeted towards monitoring those relationships presenting a higher risk of ML/FT. Part 3.4.4 of this Handbook explains the frequency of ongoing monitoring further.

3.4.1 Transaction monitoring

In relation to monitoring of transactions paragraphs 9(1)(b) and (c) of the Code state that relevant persons must:

9(1)(b) undertake appropriate scrutiny of transactions and other activities paying particular attention to suspicious and unusual activity; and

9(1)(c) appropriate scrutiny of transactions to ensure they are consistent with -

(i) the relevant person's knowledge of the customer, the customer's[5] business and risk profile and, if necessary, the source of funds for the transaction;
(ii) the business risk assessment carried out under paragraph 6;
(iii) the customer risk assessment carried out under paragraph 7; and
(iv) any relevant technological developments risk assessment carried out under paragraph 8."

In order to undertake such scrutiny a relevant person will need to know the anticipated type, volume and value of activities prior to the business relationship proceeding in order to be able to monitor for differences and fluctuations. These records relating to the customers should be kept up to date.

A relevant person should pay particular attention to transactions which are complex, large and unusual, or unusual patterns of transactions which have no apparent economic or lawful purpose. A relevant person should make

[5] Please note this is a typographical error in the Code and should state the customer's business and risk profile rather than the relevant person's business and risk profile.

appropriate enquiries and investigate these transactions to identify whether there may be a knowledge or suspicion of ML/FT.

Wherever possible, transaction monitoring should be carried out by a separate function to that which is responsible for sales or transaction processing to minimise any conflicts of interest. Please see Part 7 of the Handbook for further information on how to scrutinise unusual activity.

Any enquiries undertaken, and the results, should be properly documented and be available to any competent authority or auditor who requests it. Where there is any knowledge or suspicion of ML/FT, an appropriate report must be made to the FIU. Please see Part 7 of the Handbook for further details in relation to dealing with suspicious activity.

Relevant persons must be vigilant for changes in the nature of the relationship with the customer over time. This may be where:

- new products or services are entered into;
- new corporate or trust structures are created;
- a change in a customer's employment or other circumstances takes place;
- the stated activity or turnover of a customer increases; or
- the nature, volume or size of transactions increases etc.

Possible areas to monitor could be:

- the nature and type of the transaction;
- the frequency and nature of a series or pattern of transactions;
- the amount of any transactions, paying particular attention to particularly large transactions;
- the geographical origin/destination of a transaction; or
- the parties concerned with a view to ensuring that there are no payments to or from a person on a sanctions list or relating to any restricted activities.

Where the basis of the business relationship changes significantly, a relevant person should undertake a new assessment to reassess the customer's risk profile to ensure that the revised risk and basis of the relationship is fully understood, this could include further CDD procedures where necessary.

3.4.2 Due diligence monitoring

Paragraph 9 of the Code states that a relevant person must perform ongoing and effective monitoring of any business relationship, including -

9(1)(a) a review of information held for the purpose of CDD to ensure that it is up-to-date and appropriate (in particular where the relationship poses a higher risk of ML/FT).

This should include considering the customer's location in relation to the higher risk jurisdiction lists and sanctions list. Ongoing monitoring of a customer's activities will allow a relevant person to continue to build a profile of the customer, and will entail the ongoing collection of CDD information.

This review must take account of the CDD and EDD obtained on the customer, whether there have been any changes to the customer's activity / circumstances. Where the basis of a relationship has changed the relevant person should consider whether the risk rating of the customer needs amending and carry out further CDD procedures to ensure that the revised risk rating and basis of the relationship is fully understood. Ongoing monitoring procedures must take account of these changes. If the risk changes significantly it should be remembered that EDD may be required.

Relevant persons must ensure that any updated CDD information obtained through meetings, discussions, or other methods of communication with the customer is recorded and retained with the customer's records. That information must be available to the MLRO.

During this review if it is identified that CDD needs to be renewed, the procedures under paragraph 11 of the Code should be used. Please see part 4.3.3 of the Handbook below for further details.

Relevant persons are not automatically required to replace identification documents simply because they have expired since first being obtained. However, it is expected that identification information must be accurate, relevant and up to date. Relevant persons, must therefore review CDD information and satisfy themselves that the information on file meets these criteria. Where identification information previously obtained has changed, such as a name or residential address, the revised information must be obtained and verification of this information should be sought on a risk based approach. Consideration should be given as to whether this change may impact on the customer risk assessment undertaken under paragraph 7 of the Code. Please see part 4.7.2.1 of the AML/CFT Handbook for further details in relation to re-verification of address.

Failure to adequately monitor customers' activities could expose a business to potential abuse by criminals and may call into question the adequacy of systems and controls, or the prudence and integrity or fitness and properness of the management of the business. A failure to adequately monitor customers' activities would constitute a breach of the requirements under the Code. Please see part 1.4 for details regarding failure to comply with the Code.

3.4.3 Customer screening

When obtaining CDD or carrying on ongoing monitoring, it is likely that a relevant person will perform searches against its customer's name, and in the case of non-personal customers, against the names of the beneficial

owners, controllers, beneficiaries etc. These searches can be performed using a wide variety of risk management systems or public domain searches.

When conducting searches against the name of an individual or entity, relevant persons should consider "negative press" in addition to whether the individual or entity is named on a sanctions or PEP list.

Negative press is the term given to any negative information, whether alleged or factual. This could be anything from an allegation of fraud by a disgruntled former customer to an article in a newspaper relating to a criminal investigation.

Consideration should be given to the credibility of the information source, the severity of the negative press, how recent the information is and the potential impact the negative press would have on the business relationship with that customer.

The Authority would expect the relevant person to document:

- the source and date of the search;
- actions taken to confirm or discount any potential match;
- details of the negative press;
- any actions taken to verify or disprove the claims ; and
- any additional actions taken as a result of this information such as treating the customer as high risk and/or seeking proof of source of wealth/funds etc.

3.4.4 Frequency of ongoing monitoring

CDD information in respect of all customers must be reviewed periodically. The extent of monitoring will be linked to the risk profile of the customer which has been determined through the risk assessment required by paragraph 7 of the Code. To be most effective, resources should be allocated towards relationships posing a higher risk of ML/FT.

The Authority considers that to meet the requirements of ongoing monitoring provisions in paragraph 9 of the Code the following monitoring frequencies could be used:

- standard risk customers' CDD information should be reviewed at least every three years;
- high risk relationships require more frequent intensive monitoring. CDD information for higher risk customers should be reviewed at least annually.

All reviews should be completed in a timely manner.

Under paragraph 14 of the Code relevant persons are required to perform ongoing and effective enhanced monitoring of the business relationship with

foreign PEPs and higher risk domestic PEPs. Part 4 of this Handbook explains the concept of "enhanced monitoring".

Under paragraph 15 of the Code relevant persons must carry out EDD on business relationships with customers that have been identified as posing a higher risk of ML/FT. EDD includes giving consideration to what on-going monitoring should be carried on.

For PEP and higher risk customers, relevant persons must consider:

- whether it has adequate procedures or management information systems in place to provide relationship managers and reporting officers with timely information, including information on any connected accounts or relationships;
- how it will monitor the sources of funds, wealth and income and how any changes in circumstances will be recorded; and
- conducting an annual independent review of CDD information, activity and transactions.

3.4.5 Considering unreasonable customer instructions

Relevant persons must remain conscious that under the Code they have an obligation to prevent and detect ML/FT.

A customer who is, or may be, attempting to launder money may frequently structure his instructions in such a way that the economic or lawful purpose of the instruction is not apparent or is absent entirely. When asked to explain circumstances or transactions, the customer may be evasive or may give explanations which do not stand up to reasonable scrutiny.

Where a relevant person is suspicious, or has knowledge of, money laundering or terrorist financing, it should not unquestioningly carry out instructions as issued by the customer.

If a relevant person unquestioningly carries out unreasonable instructions in this manner, it may mean that it is failing in its duty to prevent and detect ML/FT.

When faced with unreasonable customer instructions that lead the relevant person to know or suspect ML/FT, the relevant person must make a disclosure and also consider taking legal advice. The relevant person must also contact the FIU prior to undertaking any such transactions for the customer. Please see Part 7 of the Handbook for further information on obtaining consent from the FIU and making a disclosure.

3.4.6 Handling cash transactions

The use of cash, monetary instruments or bearer negotiable instruments ("BNIs") as a means of payment or method to transfer funds can pose a

higher risk of ML/FT than other means, such as wire transfer, cheques or illiquid securities. Unlike many other financial products with cash, monetary instruments and BNIs there will likely be no clear audit trail and it may be unclear where the funds have originated from.

Therefore, where cash, monetary instruments or BNIs transactions are being proposed by customers, and such requests are not in accordance with the customer's known reasonable practice, relevant persons must approach such situations with caution and make relevant further enquiries.

In relation to cash transactions, the relevant person should consider factors such as the amount of cash, currency, denominations and the age of the notes in determining whether the activity is 'normal' for the customer along with a comparison with the customer's expected activity.

Relevant persons should be especially robust when dealing with requests for frequent or unusually large amounts of cash, monetary instrument or BNI by customers, especially where the customer is resident in jurisdictions where tax evasion is a known problem. Relevant persons should be vigilant for explanations given by customers which do not stand up to scrutiny.

Where the relevant person has been unable to satisfy itself that the transaction is legitimate activity, and therefore considers it suspicious, an internal disclosure must be made.

3.5 Jurisdiction Lists

The Code makes reference to three risk lists which are to be used in assessing customer's risk.

A relevant person should also consider the ML/FT risks posed by jurisdictions not included in the lists detailed below as there may be additional jurisdictions that pose a higher risk to their particular sector or customer type. Relevant persons should take into consideration typology reports for their business sector and their own experience in the industry.

LIST A – "the High Risk List" (a copy is provided at Appendix D(a))
List A specifies jurisdictions regarding which the FATF (or a FATF-style regional body) has made a call on its members and other jurisdictions to apply countermeasures to protect the international financial system from the on-going and substantial risks of ML/FT emanating from the jurisdiction.

Any customer resident in, located in, or engaged in business activity in a jurisdiction listed in List A must be treated as higher risk.

Other connections to a List A jurisdiction, such as nationality or source of wealth, should be considered as a higher risk factor but would not automatically deem the customer a higher risk customer.

LIST B – "the May-Be High Risk List" (a copy is provided at Appendix D(b))
List B specifies jurisdictions with strategic AML/CFT deficiencies or those considered to pose a higher risk of ML/FT.

Any customer resident in, located in or engaged in activity involving a List B jurisdiction may pose a higher risk of ML/FT. This means that the customer does not have to be considered higher risk but the Authority would expect the relevant person to be able to demonstrate why this higher risk factor did not result in the customer being classified as higher risk.

LIST C – "the Equivalent Jurisdiction List" (a copy is provided at Appendix C)
List C specifies jurisdictions which are considered to operate AML/CFT laws equivalent to those of the Isle of Man.

Relevant persons may be able to use certain concessions in relation to CDD requirements as detailed in Part 6 of the Handbook in respect of customers or introducers resident, or located in, jurisdictions listed in List C.

Part 4 – Customer Due Diligence

4.1 Introduction

4.1.1 Definitions

For ease of reference some of the key terms from this part of the Handbook are explained in this introductory section.

Know Your Customer ("KYC")

KYC is a term used to describe the process of obtaining, retaining and using information and documents about a customer to verify that they are who they say they are.

Customer Due Diligence ("CDD")

CDD encompasses KYC but it goes further than knowing who your customer is. It involves obtaining, documenting and using a broad range of information relating to a customer relationship or an occasional transaction. Areas to be considered include identity, address, source of funds and expected business or transactional activity. Certain elements of this information must also be verified. The term CDD also incorporates the ongoing monitoring of a business relationship, including the due diligence information obtained, to ensure it remains up to date and that the relationship is operating as expected for that customer. CDD is required for all new or continuing business relationships or occasional transactions.

Identification and Verification ("ID&V")

ID&V refers to establishing a customer's identity and verifying that customer's identity. Verification refers to the verification of elements of the identification information by using independent reliable sources, such sources may include material obtained from the customer such as a passport to verify the customer's name. It is essentially the concept of the relevant person satisfying themself that their customer is who they say they are.

Enhanced Due Diligence ("EDD")

EDD goes further than obtaining CDD. This involves considering whether additional identification information needs to be obtained, considering whether additional verification of identity is required, taking reasonable measures to establish source of wealth (in addition to source of funds) of the customer and beneficial owner and considering what ongoing monitoring of this information should be undertaken. EDD is to be undertaken when a new business relationship, occasional transaction, or a continuing business relationship is assessed as posing a higher risk of ML/FT, or when unusual activity is identified. When a suspicious activity is detected EDD should be considered.

Enhanced Monitoring

Enhanced monitoring should examine all aspects of the business relationship including the CDD / any EDD obtained and the customer's activity. In particular it should focus on any changes in transactional activity or transactional activity that is not in line with the customer's expected activity, these transactions should be scrutinised more thoroughly. Appropriate screening for negative press should also be undertaken. In relation to any foreign PEP, and higher risk domestic PEPs, the Code requires that enhanced monitoring is undertaken of the business relationship.

4.1.2 Background to CDD

The term KYC has been in use since the 1980s. Increasingly, the term CDD, drawn from the Basel Committee on Banking Supervision paper of October 2001 "Customer Due Diligence for Banks" is also used. In recent times the term CDD has tended to be used in place of KYC as this concept covers wider aspects of the customer relationship than KYC does. For the purpose of this Handbook we use the term CDD rather than KYC.

CDD is defined in the Code as meaning the measures specified in Paragraphs 9 to 14, 17 to 24, 37 and 39 of the Code. The CDD requirements apply at the outset of a business relationship or occasional transaction (paragraphs 10 and 12 of the Code). They also apply in relation to continuing business relationships (paragraph 11 of the Code). Also, in certain circumstances EDD may be required, EDD is explained further in part 4.3.5 of this Handbook.

Robust CDD procedures are vital for all relevant persons because they:

- help protect the relevant person and the integrity of the Isle of Man financial and designated business sectors by reducing the likelihood of relevant persons becoming a vehicle for, or victim of, financial crime;
- assist law enforcement by providing available information on customers or activities, funds or transactions being investigated;
- constitute an essential part of sound risk management e.g. by providing the basis for identifying, limiting and controlling risk exposures; and
- help to guard against identity theft.

Inadequate CDD standards and controls can result in serious customer and counterparty risks for relevant persons. Particularly in relation to reputational, operational, legal and concentration risks, which can result in significant financial cost to the business and potentially legal action being taken against the relevant person.

CDD information is also a vital tool for employees in recognising unusual or suspicious activity and therefore the CDD information held should be utilised when monitoring business relationships and transactions. The ongoing

monitoring requirements are explained further in paragraph 9 of the Code and part 3.4 of this Handbook.

4.2 Key Principles of CDD

1. Cumulative approach:

CDD is generally a cumulative process with more than one document or data source being required to verify all of the necessary components. The extent of documentation and data which is required to be collected varies depending on the customer's risk rating. Relevant persons will need to be prepared to accept a range of documents and data. However, relevant persons should be aware that some documents are more easily forged than others.

2. Foreign documents:

Relevant persons should ensure that any key documents obtained as part of the CDD process which are in a foreign language are adequately translated into English, so that the true significance of the document can be appreciated. This should be considered on a case by case basis as it may be obvious in certain instances what a document is and what it means, however in other cases it may not. If the decision is made not to translate a foreign document the relevant person should document why it has not been translated and include a summary of what they believe the document is. This should be appropriately signed off by a staff member of appropriate seniority.

Where customers put forward documents with which the relevant person is unfamiliar, either because of origin, format or language, the relevant person should take reasonable steps to verify that the document is indeed genuine. This may include contacting the relevant authorities. Consideration should be given to the importance of the detail of the document. A copy of the translation of the document should be obtained and kept with the original or copy document as evidence.

3. Sanctions:

Relevant persons should check a customer's (including beneficial owners and controllers where appropriate) nationality, residency, expected activities and source of funds to ensure that they are not subject to any relevant financial sanctions at the outset of the relationship but also on an ongoing basis. More information on sanctions can be found within part 7 of this Handbook.

4. Document verification and certification:

Where CDD documentation is obtained by hard copy, this must be certified by a suitable certifier. For identity documents the certifier must have seen the original document and met the individual face-to-face. Where CDD documentation is obtained electronically the authenticity of this document must be appropriately verified.

5. Photographs and signatures:

Any photocopies showing photographs and signatures should be plainly legible. In face-to-face situations, relevant persons should check that the photograph represents a good likeness of the customer.

6. Signatories and attorneys:

In circumstances where a customer appoints another person as an account signatory e.g. an expatriate appointing a member of his family, or company directors appointing a non-director as a signatory, or granting power of attorney in favour of an individual, full CDD procedures should also be carried out on the new account signatory or attorney.

7. Doubts over information or documentation:

Irrespective of the type of business relationship or transaction, or whether the customer is a natural or legal person, where any doubt arises as to the CDD information or verification of that information, this constitutes unusual activity. In this case the relevant person must undertake EDD and perform appropriate scrutiny of the activity. The relevant person must also consider whether an internal disclosure is appropriate. Further information regarding unusual/suspicious activity can be found at part 7 of this Handbook.

8. Unable to obtain satisfactory CDD:

Where any of the required information or documentation cannot be obtained, the business relationship or transaction must proceed no further, the relationship must be terminated and the relevant person must consider making an internal disclosure. In such circumstances, all documentation that has been obtained should be retained for at least 5 years from the relevant date. Further information regarding reporting requirements can be found at part 7 of this Handbook and the record keeping provisions are explained at part 8 of this Handbook.

9. Reporting suspicions:

Where a relevant person identifies any suspicious activity, or has reasonable cause to suspect ML/FT by a prospective customer and the business relationship has not proceeded, an internal disclosure must be made. The requirement is irrespective of the type of prospective customer. Further information regarding reporting requirements can be found at part 7 of this Handbook.

4.3 Code Requirements

It should be noted that paragraphs 10 – 12 and 13(5) of the Code do not apply to Specified Non-Profit Organisations. All other relevant persons must comply with these paragraphs. Relevant persons should apply a graduated customer acceptance policy

which requires EDD to be undertaken on those customers who are assessed as representing a higher risk of ML/FT. However, even when a customer is considered to represent a lower risk of ML/FT, the minimum standard of CDD procedures in the Handbook must be applied, as allowed for at section 4.6.1, 4.7.1 and 4.7.2.

Part 6 of the Handbook provides further detail on other Simplified CDD Measures which may be permitted in certain circumstances.

There are additional Code requirements for any customer who is a Foreign PEP (regardless of risk rating), or a domestic PEP who has been identified as posing a higher risk of ML/FT. Information regarding the Code requirements for PEPs and how to identify them is at section 4.16 of this Handbook.

4.3.1 Minimum standards table

The table overleaf is intended to provide a very high level summary of the minimum CDD requirements by the risk category of customer. This should be used in conjunction with the relevant parts of Handbook which cover this in greater detail.

	Lower and Standard Risk (CDD)	**Higher Risk (EDD)**	**Foreign PEPs & Higher Risk Domestic PEPs** (as per Code para 14 in addition to EDD where applicable)
Identification information (Customer)	Required before or during the formation of the relationship	Consider additional information and verification in addition to standard CDD requirements.	As per standard or higher risk as determined by risk rating
Verification of that information (Customer)	May be undertaken following the establishment of the business relationship in **very limited circumstances**		
Identification information (Underlying customer, persons acting on behalf of, beneficial owners)	Required before or during the formation of the relationship		
Verification of that information (Underlying customer, persons acting on behalf of, beneficial owners, legal status)	Reasonable measures May be undertaken following the establishment of the business relationship in **very limited circumstances**		
Purpose / intended nature of relationship	Required before or during the formation of the relationship	Required before or during the formation of the relationship	
Source of Funds	Reasonable measures to establish	Reasonable measures to establish	
Source of Wealth	No legislative requirement – best practice only.	Reasonable measures to establish	Reasonable measures to establish
Obtain senior management approval to take on business	No legislative requirement	No legislative requirement	Required before relationship is established
Ongoing monitoring	Ongoing and effective monitoring	Ongoing and effective monitoring, also consider additional ongoing monitoring	Must perform ongoing and effective enhanced monitoring

4.3.2 New business relationships and occasional transactions

Paragraphs 10 and 12 of the Code require the relevant person to establish, maintain and operate procedures in respect of new customers or occasional transactions to:

(a) **identify the customer**;
(b) **verify the identity of the customer** using reliable, independent source documents;
(c) obtain (and understand) information on the **purpose and intended nature of the business relationship**; and
(d) take reasonable measures to establish the **source of funds**.

Consideration should be given to additional procedures, explained later in this part of the Handbook where the customer is assessed as posing a higher risk or is a foreign PEP (or higher risk domestic PEP).

All CDD procedures must be undertaken before or during the formation of that relationship. In exceptional circumstances only, the verification of identity may be undertaken following the formation of that relationship provided that certain conditions are met, see Part 4.4 of this Handbook for further details relating to this concession.

Please see Part 6 of the Handbook for details of exempted occasional transactions to which the requirements of paragraph 12 of the Code do not apply.

If sufficient CDD is not obtained, the business relationship and transaction is to proceed no further and the relevant person should consider making an internal disclosure.

4.3.3 Continuing business relationships

Paragraph 11 of the Code requires the relevant person to establish, maintain and operate procedures in respect of continuing business relationships (existing relationships established under a previous Code or requirements) to:

(a) examine the **background and purpose** of the transactions or activity;
(b) take measures that will **require the production of information, if evidence of identity was not produced after the relationship was established**;
(c) take measures to **determine if the evidence of identity previously obtained remains satisfactory**; and
(d) if the evidence of identity is **not satisfactory**, obtain satisfactory evidence.

Continuing business covers the scenario where new Code requirements are introduced for existing sectors already subject to the Code requirements, and also includes any business relationships held prior to AML/CFT requirements

coming in for a particular business sector. It is anticipated this will only affect a small number of relevant persons.

The requirements at paragraph 11 of the Code must be undertaken during a business relationship as soon as reasonably practicable. Part 4.4 of the Handbook sets out further details relating to the timing of CDD.

As per paragraph 11, if CDD has not already been obtained, or that which was obtained is unsatisfactory (for example, because the CDD requirements have been changed / enhanced since the original evidence was collected), relevant persons must take steps to obtain satisfactory CDD. Where CDD documentation obtained previously has subsequently expired a relevant person does not automatically have to update this documentation.

The relevant person must keep records of any examination, steps, measures or determination made and must, on request, make such findings available to their competent authority or auditor.

If sufficient CDD is not obtained, the business relationship or occasional transaction is to proceed no further and the relevant person should consider making an internal disclosure.

Ongoing Monitoring provisions at Paragraph 9 of the Code:

The ongoing monitoring requirements for customers where satisfactory CDD was undertaken at the outset of the business relationship or transaction are explained in paragraph 9 of the Code. See part 3 of the Handbook for further details regarding to ongoing monitoring of business relationships.

For these continuing relationships, whether CDD needs to be undertaken will depend upon whether the relevant person already obtained the relevant information and documentation at the beginning or during the course of the relationship previously and whether, if it has been obtained, it is satisfactory and complies with current standards.

Relevant persons will therefore need to examine the information and documentation they already hold to determine whether it is necessary to collect additional CDD or make further enquiries either from the customer concerned or from other sources. If during this review it is identified that CDD needs to be renewed as it is not up-to-date and/or appropriate, the procedures under paragraph 11 of the Code should be used.

4.3.4 Beneficial ownership and control

Paragraph 3 of the Code defines beneficial owner as:

the natural person who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted and includes but is not restricted to:

1. in the case of a legal person other than a company whose securities are listed on a recognised stock exchange, a natural person who ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings) 25% or more of the shares or voting rights in the legal person;
2. in the case of any legal person, a natural person who otherwise exercises ultimate effective control over the management of the legal person;
3. in the case of a legal arrangement, the trustee or other person who exercises ultimate effective control over the legal arrangement; and
4. in the case of a foundation, a natural person who otherwise exercises ultimate effective control over the foundation;

Please note that the definition of beneficial owner in the Code differs from the definition in the Beneficial Ownership Act 2017. The Beneficial Ownership Act 2017 can be found here. The Authority has issued guidance regarding the Beneficial Ownership Act 2017, which can be found here. This part of the Handbook further explains some of the persons associated with the customer that should be identified and their identity verified where necessary. A relevant person must be satisfied it knows who the beneficial owner of its customer is. Therefore where a person identified is not an individual, it would be necessary to look through to the natural person(s) that ultimately owns or exercises ultimate effective control of the customer.

The relevant person should consider whether any persons associated with the customer that need to be ID&Vd would result in a higher risk rating for that customer. This in turn may impact on the appropriateness of utilising any simplified CDD measures for the customer and its associated persons as explained in part 6 of the Handbook.

Where there is a change in any of the parties who are acting on behalf of a customer or there is a change in beneficial ownership and control of a customer, relevant persons should treat these persons as new relationships and CDD requirements must be applied as required by paragraphs 10 and 13 of the Code.

Paragraph 13 of the Code states that where a customer is not a natural person the relevant person must identify the beneficial owner(s) of its customer. It should take reasonable measures to ID&V any beneficial owner of the customer.

Paragraph 13(2)(c) of the Code is relevant for **any** customer. It requires a relevant person to:

> **Determine whether the customer is acting on behalf of another person, and if so identify that other person and take reasonable measures to verify that other person's identity.**

This is intended to ensure that any persons who your customer is acting for, or on behalf of, are appropriately ID&Vd.

In order to determine whether the customer is acting for another person, the relevant person should consider:

1. who the customer instructions come from;
2. the source of funds;
3. the destination of funds;
4. payment references or rationale that does not appear to relate to the purported customer; and
5. an unusual delay in answering questions (due to having to refer to a third party).

For example, if a Bank were to open a sole current account for Mr X but the expected activity was 'receipt of salary in from Mr Y's employer and transfers to Mr Y' then it would appear that the customer, Mr X, is acting on behalf of Mr Y and therefore the Bank should identify and verify Mr Y. The relevant person should also know and understand the rationale for this arrangement and why Mr Y did not seek to form his own customer relationship.

The relevant person may be able to make use of certain simplified CDD concessions detailed in Part 6 of this Handbook provided that the relevant conditions are met.

In the case of a customer that is a legal person or a person who acts in relation to legal arrangement paragraph 13(3) of the Code requires the relevant person to:

(a) verify that any person purporting to act on behalf of the customer is authorised to do so;

This is intended to ensure that any person acting on behalf of the customer is authorised to act in this capacity. This must be determined prior to any instructions being accepted by that person. The relevant person should also know and understand the rationale for this arrangement.

(b) identify that person and take reasonable measures to verify the identity of that person, using reliable, independent source documents;

This is intended to ensure that any person acting on behalf of the customer is identified and reasonable measures have been taken to verify their identity.

(c) in the case of a legal arrangement, identify the trustees or any other controlling party, any known beneficiaries; and the settlor or

other person by whom the legal arrangement is made or on whose instructions the legal arrangement is formed;

This includes protectors (or similar), co-trustees or other third parties (including the settlor) where significant powers are retained or delegated. Where a blind trust or dummy settlor is used, this places an obligation on the relevant person to identify the individual who gave the instructions to form the legal arrangement and any person funding the establishment of the arrangement. Relevant persons should also obtain information regarding classes of beneficiaries to enable them to have the capacity to establish the identity of a beneficiary in future and appropriately risk assess the relationship.

(d) in the case of a foundation, identify the council members (or equivalent), any known beneficiaries, the founder and any other dedicator;

In respect of foundations, which are legal persons but which resemble trusts in many ways, relevant persons must identify the persons referred to above. 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). Relevant persons should also obtain information regarding classes of beneficiaries to enable the relevant person to have the capacity to establish the beneficiary in the future and appropriately risk assess the relationship.

(e) obtain information concerning the names and addresses of any natural persons having power to direct the customer's activities and take reasonable measures to verify that information;

(f)

Persons exercising control over the management and having power to direct the activities of a customer that may not deemed to be a controller, or one of the parties referred to in (c) or (d) of this list such as any remaining directors, persons with Powers of Attorney or account signatories.

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 legal arrangement, this includes persons whose instructions or requests the trustees are accustomed to acting on, for the avoidance of doubt, this includes where those instructions are not binding.

Methods to verify this information may include obtaining a copy of signatory lists, the most recent annual return, third party authority signing mandate or a register of directors.

(g) obtain information concerning the person by whom, and the method by which, binding obligations may be imposed on the customer;

This includes taking reasonable measures to obtain information regarding the roles and powers of any persons as described above and obtaining copies of authority such as Memorandums and Articles of Associations, Power of Attorney, a signatory list plus a copy of a board resolution relating to the signatory list. The Authority expects a relevant person to take a risk based approach in this regard and consider verifying the identity of persons able to exercise a high level of control over the customer or where other high risk factors are present.

(h) obtain information to understand the ownership and control structure of the customer;

This may include structure charts and lists detailing the persons as described above plus details of the group's structure and any connected entities as appropriate.

(i) Paragraph 13(5) of the Code requires that the relevant person must not, in the case of a customer that is a legal person or legal arrangement, make any payment or loan to a beneficial owner of that person or beneficiary of that arrangement unless it has identified the recipient of the payment or loan, and taken a risk based approach to verifying the identity of the recipient[6];

Where a payment such as a distribution or loan is made to an unconnected third party on behalf of a beneficiary or beneficial owner, that third party must be identified (the extent of identification information obtained by the relevant person could be determined on a risk based approach) and the relevant person must consider verifying the identity of this party on a risk based approach

For example, in the case of making a payment for a routine repair to a property or school fees, a check to satisfy yourself that a payee exists and appears to be legitimate would be sufficient. However, where a

[6] For the purposes of this paragraph "arrangement" is a collective terms which refers to a loan, distribution, payment or similar transfer to a beneficiary. A "beneficiary" means the person who will benefit from the arrangement in question rather than to the beneficiary of a legal arrangement.

payment is being made to an unknown third party, more substantive checks should be undertaken.

The relevant person must be satisfied with the CDD obtained before making a payment to a third party. Instances include, but are not limited to:

- making a loan to a third party;
- repaying a liability or loan on behalf of a beneficiary or beneficial owner; or
- paying an invoice on behalf of a beneficiary or beneficial owner.

For the avoidance of doubt, this sub-paragraph applies to any type of payment including a partial revocation of a trust.

4.3.5 Enhanced due diligence

Where a new business relationship, a continuing business relationship, or occasional transaction is assessed as posing a higher risk of ML/FT, paragraph 15 of the Code states that EDD must be carried out to enable further appropriate scrutiny of the relationship to take place.

Also, in the event of an unusual activity, EDD must be carried out to allow further scrutiny of the activity, and if appropriate consideration given to making an internal disclosure.

If suspicious activity is identified an internal disclosure must be made and EDD must be considered by the relevant person.

EDD is defined in the Code as meaning steps additional to the measures detailed in paragraphs 9 to 14, 17 to 24, 37 and 39 and consists of –

(a) **considering** whether **additional identification information** needs to be obtained;
(b) **considering** whether **additional aspects of the identity need to be verified**;
(c) the taking of **reasonable measures** to establish **source of wealth** of the customer and any beneficial owner; and
(d) **considering** what **on-going monitoring** should be carried out.

In considering what EDD is appropriate, it is necessary to recognise that the information requirements for identifying and reporting suspected FT may be different from those for ML. ML involves the proceeds of crimes which have already taken place. FT may also involve the proceeds of crime, but equally it may involve completely clean funds. In FT situations, it is the destination of funds which is of primary importance as they may be used to finance future terrorist attacks, organisations, resources and support networks.
In undertaking EDD where there is a higher risk of FT, relevant persons should have particular regard to their customer's relationships and the destination of funds which will, or have, formed part of the relevant person's relationship with its customer.

It is necessary for relevant persons to document their deliberations and rationale when deciding what additional measures are required in order to demonstrate that the EDD requirements in the Code have been met.

EDD procedures for new customers that are assessed as posing a higher risk or ML/FT must be undertaken before or during the formation of that relationship. There is no concession to delay the timing of obtaining the identity information and verification of this.

If sufficient CDD and / or EDD is not obtained, the business relationship and transaction is to proceed no further and the relevant person should consider making an internal disclosure.

4.4 Timing of ID&V of Identity and Failure to Complete ID&V

In respect of any new business relationships, or an occasional transaction, relevant persons must obtain CDD, which includes ID&V, before a business relationship (or transaction) is entered into, or during the formation of that business relationship.

However, very exceptionally, where there is little risk of ML/FT occurring, the Code allows at paragraph 10(4) for the verification of identification to be carried out after the formation of a business relationship (this does not apply to an occasional transaction) provided that:

(a) it occurs as soon as reasonably practical;

(b) it is essential not to interrupt the normal course of business; (e.g. securities transactions where companies may be required to perform transactions very rapidly, according to the market conditions at the time that the customer is contacting them, and the performance of the transaction may be required before the verification of identity is completed);

(c) the customer has not been identified as posing a higher risk of ML/FT and the risks of ML/FT are effectively managed;

(d) the relevant person has not identified any suspicious activity;

(e) senior management approval is obtained to establish the relationship and for any subsequent activity until adequate verification of identity is received; senior management is defined in the Code as the "...Isle of Man resident directors or key persons who are nominated to ensure the relevant person is effectively controlled on a day-to-day basis and who have responsibility for overseeing the relevant person's proper conduct. For Licenceholders licensed under the FSA and subject to the FSRB this equates to the nominated resident officers of a Licenceholder and those deputising for the nominated resident officers in accordance with Rule 8.25 of the FSRB. It does not include the MLRO, Deputy MLRO or the Compliance Officer of a Licenceholder; and,

(f) the relevant person must appropriately limit and monitor transactions; such procedures must include a set of measures such as a limitation on the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside of norms for that type of relationship. As an absolute minimum we would not expect a relevant person to repay funds to the customer or a third party until the identification has been verified.

Relevant persons must satisfy themselves that the primary motive for the use of this concession is not for the circumvention of CDD procedures. The relevant person should document the justification for the use of this concession.

The CDD process (including the requirements of paragraphs 10, 12, 13 and 15), once begun, should be pursued through to conclusion within a reasonable timeframe. If a prospective customer does not pursue an application, or verification cannot be concluded within a reasonable timeframe and without adequate explanation, the business relationship shall not proceed any further and the relevant person must terminate that relationship and consider whether an internal disclosure should be made.

4.4.1 Timing in relation to continuing business relationships

Paragraph 11 of the Code refers to the CDD requirements for continuing business relationships. Continuing business is considered to be all customers including those customer relationships held by the relevant person prior to the Code coming into force for that particular business sector. Paragraph 11(3) of the Code requires that where evidence of identification (defined in paragraph 10(1) and covered in this Part) is not held or is insufficient, the relevant person must obtain that evidence.

The satisfactory evidence of identity should be provided in a reasonable period of time. The Authority considers that this information should be obtained within 3 months of the legislation coming into effect. There may be flexibility on this time scale (such as where a business has a particularly large customer base and 3 months is impractical). Where such a decision is made on the grounds of impracticality, the rationale behind this should be documented and the Authority should be informed of the relevant person's proposed timetable to remediate this.

In the event that a relevant person is unable to obtain satisfactory CDD within a reasonable period of time, paragraph 11(5) of the Code requires that the business must proceed no further and consideration should be given to the termination of that relationship and whether an internal disclosure should be made.

4.5 How to "Identify"

4.5.1 Natural persons

In order to "identify" a **natural person**, the following identification information should be established:

(a) legal name, any former names (e.g. maiden name) and any other names used;
(b) permanent residential address including post code if possible;
(c) date of birth;
(d) place of birth;
(e) nationality;
(f) gender;
(g) an official personal identification number or other unique identifiers contained in an un-expired official document; and
(h) identification information relating to any underlying customers or persons purporting to act on behalf of the customer.

The following may also be collected taking a risk-based approach:

(i) occupation and name of employer/source of income; and
(j) details of any public or high profile positions held.

4.5.2 Legal persons

In order to "identify" a **legal person**, the following identification information should be established:

(a) name of entity;
(b) type of legal person;
(c) any trading names;
(d) date and country of incorporation/registration/establishment;
(e) official identification number;
(f) whether listed and if so, where;
(g) registered office address and in respect of foundations the business address;
(h) principal place of business/operations (if different from registered office);
(i) mailing address (if different from registered office);
(j) name of regulator (if applicable); and
(k) identification information on the underlying customer, any person purporting to act on behalf of the legal person and the beneficial owners of the legal person.

4.5.3 Legal arrangements

In order to "identify" a **legal arrangement**, the following identification information should be established:

(a) name of trust;
(b) date of establishment;
(c) official identification number where applicable (e.g. tax identification number or registered charity number);
(d) identification information on any related natural persons to the legal arrangement including the beneficial owner, known beneficiaries, controlling parties including the trustee(s) or other persons controlling or having power to direct the activities of the customer in line with the guidance for natural and legal persons (this includes protectors, co-trustees, or other third parties (including the settlor) where significant powers are retained or delegated; and
(e) mailing address(es) of trustee(s) or other persons controlling or having power to control the customer (as above);

4.6 What to "Verify"

Whichever of the following methods is used for verifying identification information or address, in all cases, either an original document, electronic copy of a document or a certified copy of the relevant documentation should be retained on file to evidence that verification has been undertaken. Relevant persons should also confirm they are comfortable with the authenticity of the document. For further information on record keeping see part 4.10, 4.11 and 8.4 of this Handbook.

4.6.1 Natural persons

In the case of **natural persons,** verification of identity comprises:

1) Verification of identification information:

For all customers:
(i) name;
(ii) date of birth;

For standard and higher risk customers:
(iii) place of birth;
(iv) national identification number; and

For higher risk customers:
(v) nationality.[7]

2) Verification of address (including post code if applicable).

[7] The Authority would suggest that a risk based approach is taken and nationality is verified wherever it is practical to do so. Nationality should always verified in the case of a higher risk customer.

4.6.2 Legal persons

In the case of **legal persons,** verification of identity comprises:

1) Verification of identification information:
   (i) name;
   (ii) official identification number; and
   (iii) date and country of incorporation.

2) Verification of addresses:
   (i) registered office address/business address; and
   (ii) address of the principal place of business where this is different to the registered office/business address.

3) Verification of the identities of any natural persons associated with the legal person that are required to be ID&V'd.

4.6.3 Legal arrangements

In the case of **legal arrangements,** verification of identity comprises:

1) Verification of identification information:
   (i) name;
   (ii) date of establishment;
   (iii) official identification number; and
   (iv) legal status of the arrangement (i.e. satisfactory appointment of the trustee(s) nature of duties etc.

2) Verification of addresses:
   (i) the mailing address(es) of trustee(s) (or other person controlling the applicant)

3) Verification of the identities of any natural persons associated with the legal arrangement that are required to be ID&V'd.

4.6.4 ID&V requirements for multiple signatories / directors

In relation to signatories, it is acknowledged that there may be a large number of signatories at different levels. Relevant persons should take a pragmatic view in identifying the signatories of a legal person. The relevant person should take a risk based approach and form a view of which signatories are likely to be used to sign off transactions and are deemed to be acting on behalf of the customer. Also, the level of signing powers should be considered and a view taken on whether the signatory's power is deemed to be significant. This information would usually be determined following a discussion with the customer.

In both higher and standard risk cases it is also expected that the relevant person should obtain a list of (but not necessarily obtain full identification information on or verify the identity of) all directors. A copy of the register of directors would be sufficient for this. This information is important when conducting the customer's risk assessment in order to determine whether there are any higher risk persons or PEPs associated with the customer.

For standard risk businesses, we would expect to see that those persons with whom the relevant person has frequent interaction with or takes instructions from (be they directors or signatories) to be ID&Vd (subject to a minimum of 2 of the individuals).

In the case of a higher risk entity, we would usually expect a relevant person to ID&V all of the directors and the signatories. Where this may be impractical, for instance with a large multinational company, or a large international charity, the relevant person should use a risk based approach and should ID&V as many directors and signatories as is practical documenting the rationale behind not obtaining all of them. As a minimum it is expected that local directors and signatories or those from whom the relevant person is accustomed to receiving instructions should be ID&Vd.

In exceptional cases, where none of the fully ID&V'd third parties are available and in order not to disrupt essential business, another person from the list may act as a signatory, on condition that they are fully ID&V'd as soon as reasonably practical after the event, the customer has not been identified as posing a higher risk of ML/FT, the risks of ML/FT are effectively managed, the relevant person has not identified any suspicious activity, senior management approval is obtained for this activity until adequate verification of identity is received and the relevant person appropriately limits and monitors the transactions.

4.6.5 ID&V requirements for multiple 3rd parties

On occasion a customer may request a relevant person to allow a number of third parties to have limited control over their affairs such as a third party signing authority on a bank account. It is important that the relevant person understands and documents the rationale for such an arrangement and is comfortable with it from an AML/CFT point of view.

Where there are a large number of potential third parties, such as staff members at a certain company, the Authority would expect the relevant person to obtain a list of the names and accompanying signatures of all potential third parties and fully ID&V those third parties that are expected to exercise control.

In exceptional cases, where none of the fully ID&V'd third parties are available and in order not to disrupt essential business, another person from the list may act as third party, on condition that they are fully ID&V'd as soon as reasonably practical after the event, the customer has not been identified as posing a higher risk of ML/FT, the risks of ML/FT are effectively managed,

the relevant person has not identified any suspicious activity, senior management approval is obtained for this activity until adequate verification of identity is received and the relevant person appropriately limits and monitors the transactions.

4.6.6 ID&V requirements for clubs and associations

In the case of associations, clubs, societies, charities, church bodies, institutes, mutual and friendly societies, co-operative and provident societies, those with ultimate control will often include members of the governing body or committee plus executives. In the case of central and local government departments and agencies, this will include persons exercising control or significant influence over the department or agency.

When considering which natural persons need to be ID&V'd the entity concerned should be treated the same as a legal person. Also, relevant persons must obtain an appropriately certified copy of the board resolution or power of attorney (or other authority) that provides the individuals representing the corporate customer with the right to act on the institution's behalf.

Where there are significant numbers of individuals that need to be ID&Vd, please see the additional guidance in 4.6.3 or 4.6.4 of this Handbook in relation to the approach that can be taken.

In exceptional cases, where none of the fully ID&V'd third parties are available and in order not to disrupt essential business, another person from the list may act for the entity, on condition that they are fully ID&V'd as soon as reasonably practical after the event, the customer has not been identified as posing a higher risk of ML/FT, the risks of ML/FT are effectively managed, the relevant person has not identified any suspicious activity, senior management approval is obtained for this activity until adequate verification of identity is received and the relevant person appropriately limits and monitors the transactions.

4.7 Methods to Verify: Natural Persons

This section sets out the standard and alternative methods that can be used to verify the identity and address of natural persons. There are no alternative methods to verify identity, if one of the standard methods cannot be used the relevant person should adopt a case by case approach, there is further guidance in section 4.7.1 in relation to what to do in these circumstances.

Where hard copy documents are used these should be suitably certified for non-face-to-face customers, where electronic documents are submitted appropriate measures should be taken to verify their authenticity.

4.7.1 Acceptable methods to verify identity

At least one from this section		
Method		**Conditions**
1	Passport bearing a photograph of the individual	Current & valid Bearing photograph of the individual
2	Current valid national identity card bearing the photograph of the individual	
3	Provisional or full driving licence[8]	
4	Known employer ID card	Current & valid Bearing photograph of the individual Lower risk customers only
5	Birth certificates	Infants & minors only
6	Proof of age card	If unable to provide items 1-4
7	Use of independent data sources, including electronic sources.	Lower risk only MUST carry out additional check number 1 below
PLUS…on a risk based approach, consider the following additional checks…		
1	Require payment for the product or service to be drawn from an account in the customer's name at a credit institution in an equivalent jurisdiction	
2	Use independent data sources, including electronic sources	
When documentation cannot be provided…		
On occasion, a customer may not be able to provide any of the documentation listed in methods 1-6 or undertake the additional checks in options 1 and 2, In such circumstances the relevant person should adopt a case by case approach in determining what methods they will accept to verify the customer's identity. The relevant person should clearly document why they have been unable to verify the customer's identity using the methods listed above, what alternative measures they have taken to verify their customer's identity and why they feel that this is sufficient to satisfy the requirements of the Code. Senior management approval should be obtained for all such cases.		

[8] Please note that a driving licence does not always verify nationality therefore care must be taken to ensure appropriate verification of nationality takes place for the customer if required. A further document may need to be obtained from the customer to ensure nationality is verified where necessary.

Guidance on international drivers permits…
Relevant persons should exercise caution regarding International Drivers' Permits/International Drivers' Licenses. These can be obtained from unauthorised and unscrupulous operators on the Internet who do not conduct any identification checks on the applicant for the Permit/Licence, and are marketed, for example, as a means of falsifying identity, avoiding driving fines and bans, and avoiding taking a driving test. International Drivers Permits can be genuine documents, but only when issued by competent national authorities to the holder of a valid domestic driving permit (i.e. national full driving licence) issued for use in the country of residence. The permit effectively converts a national licence into one for international use in other countries where the national licence is not recognised. An International Drivers' Permit is not a stand-alone document.

4.7.2 Acceptable methods to verify address

Table 1 below sets out the standard acceptable methods for verifying a natural person's address (this applies regardless of risk). Table 2 sets out alternative verification methods that may be considered. However this should only be used where the standard methods are not possible rather than as default methods.

Please note that a non-residential address for a natural person, such as a PO Box, is not acceptable under any circumstances. A "care of" address is also generally unacceptable other than on a fully explained, clearly documented and time-limited basis (this should not exceed 3 months). Such situations should be closely monitored by the relevant person.

4.7.2.1 Change of address

As explained in section 3.4.2 of this Handbook, where identification information previously obtained has changed such as residential address the new information must be sought in order to be in compliance with the Code. It should be considered whether this new information should be verified on a risk based approach. Consideration should also be given as to whether this change may impact on the risk assessment of the customer. This will often be a trigger event at which case to review the customer's CDD information.

In relation to a change of address a relevant person may, on a risk based approach, use one of the alternative verification methods in table 2 below to verify the new address.

Table 1: Standard address verification methods

<table>
<tr><td colspan="3">At least one from this section</td></tr>
<tr><td colspan="2">Method</td><td>Conditions</td></tr>
<tr><td>1</td><td>A recent account statement from a recognised bank, building society or credit card company.</td><td rowspan="4">No more than 6 months old
&
Received by the customer in the post</td></tr>
<tr><td>2</td><td>A recent mortgage statement from a recognised lender.</td></tr>
<tr><td>3</td><td>A recent rates, council tax or utility bill (not including a mobile telephone bill).</td></tr>
<tr><td>4</td><td>Correspondence from an official independent source such as a central or local government department or agency in an equivalent jurisdiction</td></tr>
<tr><td>5</td><td>Photographic driving licence or national identity card containing their current residential address.</td><td>Must not have been used as the sole document to verify identity</td></tr>
<tr><td>6</td><td>A documented record of a personal visit by a member of the relevant person’s staff to the individual’s residential address</td><td>n/a</td></tr>
<tr><td>7</td><td>Use independent data sources, including electronic sources.</td><td>n/a</td></tr>
<tr><td colspan="3">PLUS…on a risk based approach, consider the following additional checks…</td></tr>
<tr><td>1</td><td colspan="2">Use independent data sources, including electronic sources.</td></tr>
<tr><td>2</td><td colspan="2">Make a physical validation by:
Making a telephone call to the customer with a telephone number that has been independently verified as belonging to the address in question; or
Sending a letter by registered post or courier to the address in question requiring the customer to respond with a signed confirmation of receipt or confirm to the relevant person a password or code contained in that letter.</td></tr>
<tr><td colspan="3">When documentation cannot be provided…</td></tr>
<tr><td colspan="3">On occasion, a customer may not be able to provide any of the documentation listed above or undertake the additional checks in options 1 and 2. There is therefore a further list below in table 2 of alternative methods that could also be used.

Where the suggested validation checks are unable to be undertaken the relevant person should use a cumulative approach to ensure they are comfortable with the verification of the customer’s address. This should be clearly documented explaining alternative measures they have taken to verify their customer's address and why they feel that this is sufficient to satisfy the requirements of the Code. Senior management approval should be obtained for all such cases.</td></tr>
</table>

Table 2: Alternative address verification methods

At least one from this section		
Method		**Conditions**
1	Lawyer's confirmation of a property purchase or legal document recognising title to the property.	Additional check No2 must be carried out.
2	Tenancy agreement	Lower risk & face-to-face only
3	Checking a phone directory	
4	A letter from the head of the household at which the individual resides confirming that the individual resides at that address, setting out the relationship between the individual and the head of the household, together with evidence that the head of the household lives at that address.	For Isle of Man residents only
5	A letter from a known nursing home or residential home for the elderly confirming residence of the customer.	
6	A letter from a director or manager of a known Isle of Man employer that confirms residence at a stated address, and indicates the expected duration of employment. In the case of a seasonal worker, the worker's residential address in his/her country of origin should also be obtained and, if possible, verified.	For Isle of Man residents and seasonal workers temporarily residing in the Isle of Man
7	A letter from a person of sufficient seniority at a known university or college that confirms residence at stated address. The student's residential address in the Isle of Man should also be obtained.	For students normally resident in the Isle of Man but studying off-Island.
8	A letter from a director or manager of a verified known employer that confirms residence at a stated address (or provides detailed directions to locate a place of residence).	For overseas residents only. Detailed directions to be used where there is no formal address system in that area.
9	A letter of introduction confirming residential address from a trusted person (as defined in the Code) addressed to the relevant person. The trusted person must be able to confirm they have obtained and verified, or re-verified the individual's address information in the last 6 months.	Any customer unable to provide standard address verification in line with table 1.

10	Copy of contract of employment, or banker's or employer's written confirmation.	Additional check No2 must be carried out.
11	An e-statement from a recognised bank, building society, credit card company, recognised lender.	
12	An e-bill in relation to rates, council tax or utilities	
PLUS…at least one of the following…		
1	Use independent data sources, including electronic sources.	
2	Make a physical validation by: • Making a telephone call to the customer with a telephone number that has been independently verified as belonging to the address in question; or • Sending a letter by registered post or courier to the address in question requiring the customer to respond with a signed confirmation of receipt or confirm to the relevant person a password or code contained in that letter.	

4.8 Methods to Verify: Legal Persons

This section sets out the standard methods that can be used to verify the identity and address of legal persons. There are no alternative methods suggested here, if one of the standard methods cannot be used the relevant person should adopt a case by case approach in determining what methods it will accept to verify the legal person's identity. Further guidance on what to do in these circumstances is provided in the table.

Where hard copy documents are used these should be suitably certified for non-face-to-face customers, where electronic documents are submitted appropriate measures should be taken to verify their authenticity.

At least one from this section, ensuring that the identity, address and legal status are verified.			
Method		**What does this verify?**	**Conditions**
1	Certificate of Incorporation Memorandum & Articles of Association (or equivalent)	ID	Must be either a certified copy or sourced directly from an independent public registry
2	Bank statement or utility bill	Address	No more than 6 months old. Received by the customer in the post
3	Latest Annual Return	ID and Address	Must be in date and sourced directly from an independent public registry in an equivalent jurisdiction
4	Audited financial statements which displays the company name, directors and registered address	All	Must be audited and signed by the auditor (photocopies or documents sourced from an independent public registry are acceptable)
5	Prepared accounts by a reporting accountant which displays the company name, directors and registered address	All	Must be signed by the reporting accountant
6	Conducting and recording an enquiry by a business information service, or an undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted	All	None
7	Undertaking a company registry search, including confirmation that the institution has not been, or is not in the process of being dissolved, struck off, wound up or terminated	Legal Status	Company registry must be in an equivalent jurisdiction
PLUS… on a risk based approach, consider the following additional checks…			
1	Require payment for the product or service to be drawn from an account in the customer's name at a credit institution in an equivalent jurisdiction		
2	Use independent data sources, including electronic sources		
When documentation cannot be provided			
The relevant person should clearly document why they have been unable to verify the legal person's identity using the methods listed above, what alternative measures they have taken to verify the identity and why they feel that this is sufficient to satisfy the requirements of the Code. Senior management approval should be obtained for all such cases.			

4.9 Methods to Verify: Legal Arrangements

This section sets out the standard methods that can be used to verify the identity and address of legal arrangements. There are no alternative methods suggested here, if one of the standard methods cannot be used the relevant person should adopt a case by case approach in determining what methods it will accept to verify the legal person's identity. Further guidance on what to do in these circumstances is provided in the table.

Where hard copy documents are used these should be suitably certified for non-face-to-face customers, where electronic documents are submitted appropriate measures should be taken to verify their authenticity.

At least one from this section, ensuring that the identity, address and legal status of the parties are verified as per 4.7 and 4.8 as appropriate.			
Method		**What does this verify?**	**Conditions**
1	Trust Deed (or relevant extracts of the trust deed) and any subsequent deeds of appointment and retirement (or equivalent).	Evidences the formation of the arrangement and confirms that the persons in question are the trustees (or equivalent) of the arrangement.	Must be a certified copy
2	Bank statement (if applicable)	Trustees Mailing Address	No more than 6 months old Received by the customer in the post
PLUS… on a risk based approach, consider the following additional checks…			
1	Require payment for the product or service to be drawn from an account in the customer's name at a credit institution in an equivalent jurisdiction		
2	Use independent data sources, including electronic sources		
When documentation cannot be provided			
The relevant person should clearly document why they have been unable to verify the person's identity using the methods listed above, what alternative measures they have taken to verify the identity and why they feel that this is sufficient to satisfy the requirements of the Code. Senior management approval should be obtained for all such cases.			

4.10 Certification of Hard Copy Documents

Use of an independent suitable certifier guards against the risk that hard copy documentation provided is not a genuine copy and in the case of identity documents that it corresponds to the customer whose identity is being verified. However, for certification to be effective, the certifier will need to have seen the original documentation and have met the individual face-to-face. Where a staff member of a relevant person meets the customer face-to-face they can certify the document, otherwise a suitable certifier must be used.

For non-face-to-face business suitable persons to certify documents include known and trusted members of the community such as:

1. a member of the judiciary, a senior civil servant, a serving police or customs officer;
2. an officer of an embassy, consulate or high commission of the country of issue of documentary verification of identity;
3. a lawyer or notary public, who is a member of a recognised professional body;
4. an accountant who is a member of a recognised professional body;
5. a company secretary who is a member of a recognised professional body;
6. a director, secretary or board member of a trusted person as defined in the Code; or
7. a manager or other senior officer within the relevant person's group.

The certifier should sign and date the copy document (printing his/her name clearly in capitals underneath) and clearly indicate his/her position or capacity on it and provide contact details. The certifier should check the photograph represents a good likeness of the customer and should also state that it is a true copy of the original. There is no exact wording that has to be used, however the relevant person should ensure it covers the aforementioned areas.

The certifier may complete a covering letter or document, which is then attached to the copy identification document(s) i.e. the certification is not written on the copy identification document itself as long as the covering document contains the information specified in the paragraph above, and it is clear in the letter itself that it refers to the attached document.

In order to comply with the Code, relevant persons should satisfy themselves as to the suitability of a certifier based on the assessed risk of the business relationship and the reliance to be placed on the certified documents. In determining the certifier's suitability, a relevant person may consider factors such as the stature and track record of the certifier, previous experience of accepting certifications from certifiers in that profession or jurisdiction, the adequacy of the AML/CFT framework in place in the jurisdiction in which the certifier is located and the extent to which the AML/CFT framework applies to the certifier.

Relevant persons should ensure that any certified documents they have received are accurate and up-to-date. In any circumstance where a relevant person is unsure of the authenticity of certified documents, or that the documents actually relate to the customer, a cumulative approach should be taken and additional measures or checks

undertaken to gain comfort. If still unsatisfied with the verification of identity or address the business relationship must proceed no further, the relevant person must terminate the business relationship and consideration be given to making an internal disclosure.

Please see part 8.4 of this Handbook for details of the record keeping requirements in relation to these documents.

4.11 Use of Electronic Documents

Where a relevant person obtains verification documents electronically from the customer, original certification of these documents is not necessarily required. These documents should be provided to the relevant person as an image file or other tamper resistant format.

Below are some examples of electronic documentation that could be accepted, please note this is not an exhaustive list:

1. In the case of an identity document (such as passport or driving licence) a photograph should be provided which clearly shows the person's face and the image on the identity document being held in the same picture to demonstrate this actually belongs to the customer. A clear scanned copy of the document itself should also be provided.

2. A scanned copy of a certified document i.e. where a document has been certified in hard copy and is then scanned and emailed to the relevant person.

When considering the acceptability of electronic documents to verify a customer's identity, a relevant person should take a risk based approach to satisfy itself that the documents received adequately verify that the customer is who they say they are and that the relevant person is comfortable with the authenticity of these documents. The relevant person could check the type of file and ensure it is tamper resistant, it could check the email address it is being received from to ensure it seems legitimate and relates to the customer sending in the documentation, if the document has been certified that it is a suitable certifier etc.

In any circumstance where a relevant person is unsure of the authenticity of the documents, or that the documents actually relate to the customer, a cumulative approach should be taken and additional measures or checks undertaken to gain comfort. If still unsatisfied with the verification of identity or address the business relationship must proceed no further, the relevant person must terminate the business relationship and consideration be given to making an internal disclosure.

Please see part 8.4 of this Handbook for details of the record keeping requirements in relation to these documents.

4.12 Independent Electronic Data Sources

Independent data sources can be used in certain circumstances to electronically verify a customer's identity and address. Note that independent electronic data sources may be used to verify that documents are authentic, but will not necessarily verify that your customer is who they say they are. Therefore where independent data sources are used a further verification method must be undertaken alongside this method as explained in the table in section 4.7.1.

Independent electronic data sources can provide a wide range of confirmatory material without involving a customer and are becoming increasingly accessible. However, an understanding of the depth, breadth and quality of the data accessed will be important. The sources that are often used by electronic systems include the passport issuing office, driving licence issuing authority, companies registry, the electoral roll and other commercial / electronic databases.

Where a relevant person intends to use electronic data sources conducted by commercial agencies, it should be sure that the agency is registered with a data protection agency in the European Economic Area. Relevant persons should also satisfy themselves that the agency:

1. uses a range of positive information sources that can be called upon to link a customer to both current and historical data;
2. accesses negative information sources such as databases relating to fraud and deceased persons;
3. accesses a wide range of alert data sources; and
4. has transparent processes that enable a relevant person to know what checks have been carried out, and what the results of these checks are.

Relevant persons should also ensure that:

1. the source, scope and quality of the data are satisfactory. At least two matches of each component of an individual's identity or address should be obtained (careful thought should be given to searching with variations on spelling of the individual's name); and
2. the processes allow the business to capture or store the information used to verify identity and/or address.

4.13 Purpose and Intended Nature of Business Relationship

The Code states at paragraphs 10 and 12 that information should be obtained in relation to the nature and intended purpose of each new business relationship or occasional transaction.

Unless it is obvious from the product being provided, the following information should be established to assist in meeting the Code requirements:

In all situations:

- expected type, volume and value of activity;
- expected geographical sphere of the activity; and
- details of any existing relationships with the product/service provider.

For legal persons and arrangements:

- an understanding of the ownership and control structure of the company, including group ownership where applicable as per paragraph 13 of the Code;
- nature of activities undertaken (having regard for sensitive activities and trading activities);
- geographical sphere of the legal person's activities and assets; and
- name of regulator, if any.

4.14 Source of Funds & Source of Wealth

The Code requires at paragraphs 10 and 12 that a relevant person must take reasonable steps to establish the source of funds for all customers when entering a new relationship or carrying out an occasional transaction.

Paragraphs 14 and 15 of the Code also state that relevant persons must take reasonable steps to establish the source of wealth for higher risk customers (including higher risk domestic PEPs) and all foreign PEPs and also when unusual activity occurs.

Source of funds is concerned with the funding of the business relationship or transaction, for example an immediate source from which property has derived e.g. a bank account in the name of Mr X. Knowing who provided or will provide the funds and the account and the account or product from which they have derived is necessary in every case. The source of funds requirement refers to where the funds are coming from in order to fund the relationship or transaction. This does not refer to every payment going through the account, however the relevant person must ensure they comply with the ongoing monitoring provisions at paragraph 9 of the Code.

Source of funds will sometimes be a bank account that can be directly related to the customer. Where this is not the case, for example when third party funding is involved, the relevant person may take a risk based approach and where appropriate make further enquiries about the relationship between the ultimate underlying owner of the funds and the customer and consider beneficial ownership requirements. In addition, consideration must be given to verifying the identity of the identity of the ultimate underlying owner, i.e. the provider of the funds.

Where it is deemed necessary appropriate evidence in relation to the source of funds should be obtained and retained on file. It should be ensured that the information held is sufficient to be able to reconstruct the transaction as in accordance with paragraph 32 (c) of the Code.

Where it appears that the customer is acting on behalf of someone else there is further guidance relating to how to determine this under section 4.3.4 of the AML/CFT Handbook.

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 must be obtained for all higher risk customers (including higher risk domestic PEPs) and all foreign PEPs 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 the customer relationship.

4.15 Bearer Shares

Many jurisdictions, including the Isle of Man, have prohibited or immobilised bearer shares due to the associated AML/CFT risks. However, certain jurisdictions may still allow these to be used therefore relevant persons must take particular care to record the details of bearer shares received or delivered other than through a recognised clearing or safe custody system, including the source and destination.

To reduce the opportunity for bearer shares to be used to obscure information on beneficial ownership, the Authority expects all relevant persons to immobilise bearer shares and take them into safe custody. Should a prospective, or existing, customer refuse to allow the immobilisation of the bearer shares, the relevant person should not proceed any further with the business relationship, and must consider making an internal disclosure.

4.16 Politically Exposed Persons (PEPs)

4.16.1 PEP risk

Much international attention has been paid in recent years to 'politically exposed person' ("PEP"), with the Financial Action Task Force ("FATF") having produced a guidance document relating to PEPs. PEP risk refers to the risks associated with providing financial and business services to those with a high political profile or who hold public office. The increased risk stems from the possibility of the PEP misusing their position and power for personal gain through bribery or corruption. Family members and close associates of PEPs may also pose a higher risk as PEPs may use family members and/or close associates to hide any misappropriated funds or assets gained through abuses of power, bribery or corruption. Investigations regarding proceeds of corruption often gain publicity and can damage the reputation of both the businesses and countries involved therefore it is important that a relevant person takes their responsibility to identify PEPs seriously.

Being a PEP does not mean that the individual should automatically be classified as higher risk of ML. This is because a large percentage of PEPs do not abuse their power nor are they in a position to abuse their power. However, relevant persons should be aware that an individual who has been entrusted with a prominent public function is likely to have a greater exposure to bribery and corruption.

The risks relating to PEPs increase when the person concerned has been entrusted with a political or public office role by a jurisdiction with known problems of bribery, corruption or financial irregularity within their government or society. The risk is even more acute where such countries do not have adequate AML/CFT standards, or where they do not meet financial transparency standards. Relevant persons should take appropriate measures to mitigate those risks.

4.16.2 PEP definitions

Domestic PEP – a PEP who is or has been entrusted with prominent public functions in the Isle of Man and family members or close associates of that person regardless of location of those family members or close associates.

Foreign PEP – a PEP who is or has been entrusted with prominent public functions outside the Isle of Man and any family members or close associates of that person regardless of the location of those family members or close associates.

Politically exposed persons are defined in paragraph 3 of the Code and include natural persons who are or have been 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. The following definitions are set out in the Code.

Prominent public functions include:

(a) a head of state, head of government, minister or deputy or assistant minister;
(b) a senior government official;
(c) a member of parliament;
(d) a senior politician;
(e) an important political party official;
(f) a senior judicial official;
(g) a member of a court of auditors or the board of a central bank;
(h) an ambassador, chargé d'affaires or other high-ranking officer in a diplomatic service;
(i) a high-ranking officer in an armed force;

(j) a senior member of an administrative, management or supervisory body of a state-owned enterprise;
(k) a senior member of management of, or a member of, the governing body of an international entity or organisation; or
(l) An honorary consul.

Immediate family members include:

(a) a spouse;
(b) a partner considered by national law as equivalent to a spouse;
(c) a child or the spouse or partner of a child;
(d) a brother or sister (including a half-brother or half-sister);
(e) a parent;
(f) a parent-in-law;
(g) a grandparent; or
(h) a grandchild.

Close associate includes any natural person:

(a) known to be a joint beneficial owners of a legal entity or legal arrangement, or any other close business relationship, with such a person;
(b) who is the sole beneficial owner of a legal entity or legal arrangement known to have been set up for the benefit of such a person;
(c) known to be a beneficiary of a legal arrangement of which such a person is a beneficial owner or beneficiary; or
(d) known to be in a position to conduct substantial financial transactions on behalf of such a person.

An 'international entity or organisation', as defined at (k) above, refers to entities established by formal political agreements (international treaties) between their member states; their existence is recognised by law in their member countries and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include, but are not limited to:

- the United Nations ("UN") and any affiliated international organisations;
- institutions of the European Union;
- the Council of Europe ("CoE");
- the North Atlantic Treaty Organisation ("NATO");
- the World Trade Organisation ("WTO");
- the International Monetary Fund ("IMF");
- the World Bank; and
- the Organisation for Security and Cooperation in Europe ("OSCE")

4.16.3 PEP requirements

Paragraph 14 of the Code states that a relevant person must:

(a) maintain **appropriate procedures and controls for identifying PEPs**; and

In respect of all foreign PEPs and higher risk domestic PEPs, the relevant person must:

(b) obtain **senior management approval** to take on the business relationship, carry out an occasional transaction or retain customers that have been identified as PEPs;

(c) take **reasonable measures to establish their source of wealth**; and

(d) perform **ongoing and effective enhanced monitoring** of any business relationship.

The above listed requirements must be met in addition to any EDD requirements where the customer may also have been identified as posing a higher risk. It is important to appreciate that although it is likely that a PEP will pose a higher risk, this is only one of a number of factors that should be considered when determining the risk rating of the customer. For example, if a PEP operates a bank account which has a small turnover from expected salary, payments in and debits out to cover household and living expenses, in an equivalent jurisdiction, then this may reasonably be assessed as not posing a higher risk of ML/FT.

Where a PEP has not been identified as posing a higher risk of ML/FT they can treated like any other customer and the normal Code requirements apply.

The requirements of paragraphs 14(2), (3) and (4) of the Code apply to all foreign PEPs or domestic PEPs that have been assessed as posing a higher risk. It is important to recognise that the definitions of domestic PEP and foreign PEP are based on where the PEP's prominent function relates to rather than the residency of the individual.

Where a PEP is assessed as posing a higher risk, in addition to the requirements for PEPs in Paragraph 14 of the Code, EDD must be undertaken in accordance with paragraph 15 of the Code. When a PEP has been identified as higher risk and the relevant person has a detailed knowledge of the PEP, it is important that the relevant person does not assume that the detailed knowledge allows for the PEP to be treated as anything other than higher risk. The additional PEP requirements EDD measures set out in the Code should always be applied where relevant, regardless of a detailed knowledge of the PEP.

For the avoidance of doubt, where a PEP is not considered higher risk, the reasons for this should be documented, and the individual must still be identified as a PEP.

The below table summarises the requirements in relation to PEPs:

Customer	EDD (Para 15)	Additional PEP req's (Para 14 (2-5))
High risk domestic PEP	Yes	Yes
Standard risk domestic PEP	No	No
High risk foreign PEP	Yes	Yes
Standard risk foreign PEP	No	Yes

4.16.4 Identifying PEPs

Paragraph (14)(1) of the Code requires a relevant person to maintain appropriate procedures and controls for the purpose of determining whether any of the following is a PEP –

(a) any customer;
(b) any natural person having power to direct the activities of a customer;
(c) any beneficial owner or known beneficiaries.

When identifying if a customer is a PEP, a relevant person can utilise various methods of identification, including commercially available databases and screening tools. It can also be useful to research who the current and former holders of prominent public functions are, both locally and internationally. Various sources could be consulted to determine who holds or formerly held the prominent public functions, such as Tynwald, the UK Government, the European Parliament and international organisations including the UN and World Bank. In addition, the equivalent jurisdiction List in Appendix C and the high risk jurisdiction Lists and jurisdictions that may pose a high risk in Appendix D(a) and D(b), respectively, can be consulted.

Whilst the definition of PEP focuses on positions of prominent public function, it is important for relevant persons to be aware of the risk of junior officials being used by PEPs to bypass AML/CFT controls. Consideration can be given to assessing the extent to which an individual could be used by a PEP and the associated risks.

The obligation to identify PEPs does not end once the customer relationship has been established. Paragraph 9 of the Code requires a relevant person to perform ongoing and effective monitoring of any business relationship. Relevant persons should ensure that the procedures for identifying PEPs and ongoing monitoring are clear regarding identifying if any individuals have *become* PEPs since the business relationship was established.

There is also a common misconception is that PEPs who have immunity from prosecution or conviction, such as Heads of State immunity in office for actions committed prior to taking office or diplomats, are not subject to PEP requirements. It is important to understand that this is not the case; having knowledge of a PEP with immunity could lead to discovering information used in a SAR which in turn could trigger an investigation into individuals who do not have immunity.

4.16.5 Identifying PEP risk

Identifying that a client is a PEP forms part of the wider process of establishing the risks relating to your customers. Whilst individuals who are PEPs should not be prejudged as having links to criminal activity or abuse of the financial system, a relevant person should be aware of the risks associated with PEPs.

The FATF has developed a list of indicators and red flags which can assist in the detection of any potential misuse of the financial system by PEPs. These red flags have not been developed to stigmatise all PEPs, rather they are an aid to detect PEPs who are abusing the financial system. Matching one or more red flags may only raise the risk of doing business with the relevant PEP however in certain circumstances, matching one or more red flags could lead to a direct money laundering or terrorist financing suspicion.

The list of indicators/red flags developed by the FATF is not an exhaustive list and should be used in conjunction with the other factors to determine the risks of customers. Please refer to Annex 1 of the FATF guidance paper on politically exposed persons for red flags relating to areas such as:-

- PEPs shielding their identity;
- A PEP's position in a business;
- The industry/sector the PEP is involved in; and

- Country specific indicators.

Other examples of indicators of corruption include excessive revenue from consultancy fees or commissions, where there are inexplicable commissions being paid out or where there may be contracts with escalated prices.

Indicators can also be helpful in determining whether a PEP is lower risk. Lower risk indicators can include areas such as:-

- The relevant prominent public function being conducted in a country associated with low levels of corruption;
- The relevant prominent public function being conducted in a country with a track record of investigating political corruption;
- The PEP being subject to rigorous disclosure requirements; and
- The PEP does not have executive decision-making responsibilities.

The above is not an exhaustive list. Any decision to rate a PEP as lower risk should have a clear rationale and be clearly documented.

4.16.6 'Once a PEP, Always a PEP'?

Paragraph 3 of the Code states that a PEP is a natural person who is or has been entrusted with a prominent public function, their family members and close associates.

The Authority expects a relevant person to assume the default position of 'once a PEP, could always remain a PEP' when a PEP is no longer in that prominent public function. This is in line with the guidance issued by the FATF in 2013, which states that the treatment of PEPs should be based on an assessment of risk rather than prescribed time limits. When a PEP is no longer in the prominent public function, FIs and DFNBPs can utilise a risk based approach to determine the risks associated with the PEP.

An assessment of the risks associated with the jurisdiction, the seniority of the role as well as the individual PEP can be conducted in order to determine whether the PEP continues to represent a higher risk. Considerations can include:

- The nature and duration of the individual's role;
- How much time has passed since they were in the role;
- The level of (informal) influence that the individual could still exercise;
- Whether the individual's previous and current function are linked in any way (e.g. formally by appointment of the PEPs successor, or informally

by the fact that the PEP continues to deal with the same substantive matters);

- The level of inherent corruption risk in the jurisdiction of their political exposure;
- The level of transparency about the source of wealth and origin of funds; and
- Links to higher risk industries.

This risk based approach can also be used where a PEP is deceased but this individual was the source of funds/source of wealth for family members and close associates who have been identified as high risk domestic or foreign PEPs. In such circumstances, an individual assessment should be conducted to determine whether the relationship still merits EDD measures.

If a relevant person chooses to utilise a risk based approach, they should ensure that a clear and detailed rationale, explaining why the individual should not be treated as a PEP, is documented. Any decision to use this approach should be subject to an appropriate level of senior management review and approval and where PEPs are no longer classified as such, their former PEP status should be documented.

Whilst a risk based approach can be utilised once a PEP is no longer in the prominent public function, it is important for a relevant person to understand that a PEPs influence and prominence may not have diminished; PEPs in prominent roles may continue to have influence and power after they have left the role and thus be potentially more susceptible to bribery and corruption. In addition, a PEP may have been in a position to acquire their wealth illicitly when in the relevant role or function, therefore high level scrutiny may be warranted once they are no longer a PEP. A relevant person should be aware that the risks associated with PEPs are closely linked to the inherent corruption risk of the jurisdiction in which they held the role, the relevant role or function and the influence held during their post.

Part 5 – Specified Non-Profit Organisations

5.1 What is a Specified Non-Profit Organisation?

The only non-profit organisations that are considered as businesses in the regulated sector (and therefore subject to the Code requirements) are those that could potentially be exposed to increased risk of being abused for terrorist financing. These are deemed to be "specified non-profit organisations" and are defined by Schedule 4 to POCA as:

Specified non-profit organisation ("SNPO") means a body corporate or other legal person, the trustees of a trust, a partnership, other unincorporated association or organisation or any equivalent or similar structure or arrangement, established solely or primarily to raise or distribute funds for charitable, religious, cultural, educational, political, social or fraternal purposes with the intention of benefiting the public or a section of the public and which has —

1. an annual or anticipated annual income of £5,000 or more; and
2. remitted, or is anticipated to remit, at least 30% of its income in any one financial year to one or more ultimate recipients in or from one or more higher risk jurisdictions;

A "higher risk jurisdiction" is a jurisdiction which the business in the regulated sector determines presents a higher risk of ML/FT or of proliferation having considered any relevant guidance. The relevant guidance in this case would be the list maintained by the Department of Home Affairs on its website which is replicated at Appendix D of this Handbook.

5.2 Code Requirements

All of the paragraphs of the Code apply to SNPOs except those set out in paragraph 5 of the Code which states:

Despite paragraph 4, paragraphs 10 to 12 and 13(5) do not apply to SNPOs.

Please refer to the sector guidance for further detail of requirements specific to the activities of SNPOs.

Part 6 – Simplified Customer Due Diligence

6.1 Introduction

The FATF's Recommendations allow for jurisdictions to permit simplified CDD measures under certain conditions such as where lower risks are identified. They state that jurisdictions should understand that the discretion afforded and the responsibility imposed on relevant persons by the risk based approach is more appropriate in sectors with greater AML/CFT controls and experience. It also states that this should not exempt relevant persons from the requirement to apply EDD measures where higher risks are identified.

It is important to understand that the premise of simplified CDD measures is to simplify the CDD process and to reduce the compliance burden. It does not remove the requirement to identify the customer and any underlying person, beneficial owner and controller except in very limited situations as detailed in this part of the Handbook. Simplified CDD can only be used where the relevant conditions are met.

There are 3 main concessions detailed within Part 6 of the Code "Simplified Customer Due Diligence":

- Eligible Introducers;Acceptable Applicants; and
- Persons in a regulated sector acting on behalf of a third party ("acting on behalf of");

Each of these will be discussed in detail later in this part. Below is a table which summarises the fundamental differences between the 3 main concessions:

	Eligible Introducer (Paragraph 23(5) of the Code)[9]	**Acceptable Applicant (Paragraph 20 of the Code)**	**Acting on behalf of (Paragraph 21 of the Code)**
What is the concession?	If the conditions are met the relevant person may rely on the introducer to verify the identity of the customer. The introducer does not have to produce the verification documentation to the relevant person at the outset of the relationship or occasional transaction. The relevant person must still obtain identity information regarding the identity of the customer and the beneficial owner.	If the conditions are met the relevant person does not have to verify the identity of the customer.	If the conditions are met, and the relevant person is permitted to use this concession, the relevant person does not have to identify, verify, or determine the beneficial owner of the underlying third party client. However, the customer of the relevant person must have done this.
What is the relationship with the customer?	The relevant person's services are provided directly for, and to, the customer. The Eligible Introducer is not the relevant person's customer.	The acceptable applicant is the customer and is not acting on behalf of another party or parties.	The allowed business is the relevant person's customer and the relevant person provides services directly to the allowed business / customer, such as a bank account. However, the allowed business / customer **is** acting on behalf of another party or parties (the underlying third party / client).

[9] This refers to the eligible introducer concession, for details of the non-eligible concession please see part 6.2.1 of this Handbook.

Does the customer have to meet certain criteria?	There are no requirements relating to who the customer is. The introducer must be a trusted person, other than a nominee company of either a regulated person or a person who acts in the course of external regulated business.	The acceptable applicant must be a trusted person or must be a company listed on a recognised stock exchange.	The customer must be an "allowed business" which is set out in paragraph 21(6) of the Code.
Do higher risk circumstances dis-apply the concession?	Yes, if the introducer, or customer, is assessed as posing a higher risk of ML/FT this concession is disapplied. Therefore, the verification documentation must be produced to the relevant person, it cannot rely on the introducer to obtain and hold this.	Yes, if the customer is a higher risk of ML/FT, this concession is disapplied. The relevant person must obtain CDD and EDD on the customer.	No, this concession may still be used if the underlying third party / client, and allowed business / customer are assessed as posing a higher risk of ML/FT.
Written Terms of Business required?	Yes – must contain the items listed in the Code. There is a template of the EI certificate and terms of business at Appendix E of this Handbook.	No – but need to ensure that the customer qualifies as an acceptable applicant. There is an acceptable applicant certificate template at Appendix F of this Handbook.	Yes – must contain the items listed in the Code. There is an acting on behalf of terms of business template at Appendix G of this Handbook.
Testing of their CDD procedures required?	Yes	No	Yes

6.2 Eligible Introducer

6.2.1 Introduction to the Eligible Introducer ("EI") Concession

There are two parts to the concession at Paragraph 23 of the Code. Whichever part is used, the responsibility for ensuring that CDD procedures are compliant with the Code remains with the relevant person not the introducer.

Non-eligible introduced relationships:
Paragraphs 23(1) to 23(4) of the Code allows the relevant person to obtain evidence of the identity of a customer from any third party (introducer). This would constitute a non-eligible introduced relationship. The introducer essentially acts as a facilitator between the relevant person and the customer.

Where customers are introduced to a relevant person via a non-eligible introducer, the relevant person must identify and verify the identity of the customer themselves. However, the relevant person may request a non-eligible introducer to obtain and produce information verifying the identity of the customer from the applicant and pass it to them.

Eligibly introduced relationships:
Paragraph 23(5) of the Code allows the relevant person to place reliance on an introducer to have verified the customer's identity provided certain criteria are met. Also, the concession states that the introducer does not have to produce the verification documents to the relevant person at the outset of the relationship or an occasional l transaction. The relevant person must still obtain identity information regarding the identity of the customer and the beneficial owner which can be obtained from the introducer. These relationships are known as 'eligibly introduced' relationships.

Although the relevant person can rely on the introducer to verify the customer's identity and hold this documentation, the ultimate responsibility for ensuring CDD procedures are carried out and that AML/CFT requirements are met remains with the relevant person. This includes the requirement to undertake a customer risk assessment at paragraph 7 of the Code.

The concession at paragraph 23(5) of the Code does not apply to outsourcing or agency arrangements i.e. where the agent is acting under a contractual arrangement with the relevant person to carry out its CDD functions.

6.2.2 Conditions to use the EI Concession

In order to use the EI concession at paragraph 23(5) of the Code, the relevant person must satisfy the conditions below:

The relevant person must –

(a) have identified the customer and the beneficial owner (if any) and have no reason to doubt those identities;

(b) know the nature and intended purpose of the business relationship;

(c) not have identified any suspicious activity;

See 6.2.5 of this Handbook for further detail on the disapplication of the EI concession.

(d) have satisfied itself that –

i. the introducer is a trusted person other than a nominee company of either a regulated person or a person who acts in the course of an external regulated business; or
ii. the relevant person and the introducer [10]are bodies corporate in the same group; or
iii. the transaction is an exempted occasional transaction.

Relevant persons must obtain satisfactory evidence to verify the status and eligibility of introducers. Such evidence may comprise corroboration from the introducer's regulatory authority, or evidence from the introducer itself of such regulation. The relevant person must also take such measures as necessary to ensure it becomes aware of any material change to the introducer's status or the status of the jurisdiction in which the introducer is regulated.

(e) have satisfied itself that the introducer does not pose a higher risk of ML/FT;

See 6.2.5 of this Handbook for further detail on the disapplication of the EI concession

(f) put in place written terms of business;

Relevant persons must put in place terms of business between themselves and the introducer as required under Paragraph 23(6) of the Code. These requirements are explained under section 6.2.3 of this Handbook.

(g) ensure that the procedures for obtaining evidence of identity from the introducer, and likewise that the introducer's procedures are satisfactory and fit for purpose to obtain adequate evidence of the identity of the customer;

[10] Please note that there is a typographical error in the Code at paragraph 23(5)(d)(ii) where it states customer this should read introducer. This will be amended in due course.

This should involve the relevant person conducting an assessment of its own internal procedures and those of the introducer to ensure that the conditions to use the concession are met.

In assessing the introducer's procedures, the relevant person should consider:

- conducting a review of the Eligible Introducer's policies and procedure;
- making enquiries concerning the Eligible Introducer's stature and regulatory track record and the extent to which any group standards are applied and audited; or
- seeking copies of an independent review of the Eligible Introducer's procedures by external auditors and other experts.

(h) test that the procedures are effective by testing them on a random and periodic basis no less than once every 12 months; and

Paragraph 23(8) of the Code also requires the relevant person to test that the procedures are compliant.

On a random and periodic basis (at least once every 12 months), the relevant person should request details of any changes in the aforementioned procedures and a copy of CDD on a sample of customers which should include:

- the identification information required by Part 4 of the Code and copies of the verification of that identification; and;
- evidence that the record keeping requirements under paragraphs 32, 33 and 34 of the Code are being complied with. If the customer can provide all of the above within 7 working days, this part would be deemed to have been complied with.
- if available, the most recent copy of the customer's risk assessment along with any supporting documentation or information could also be requested.

(i) take measures to satisfy itself that the introducer is not itself reliant upon a third party for the evidence of identity of the customer.

This requirement is intended to prevent a chain of introducers; i.e. where the relevant person relies on an introducer who themselves are relying on another introducer.

6.2.3 EI Concession Terms of Business

Paragraph 23(6) of the Code states that a relevant person must not enter into a business relationship with a customer that has been introduced by an introducer unless written terms of business are in place.

The terms of business require in all cases, the introducer to –

(a) verify the identity of all customers introduced to the relevant person sufficiently to comply with the AML/CFT requirements;
(b) take reasonable measures to verify the identity of the beneficial owner (if any);
(c) establish and maintain a record of the evidence of identity for at least 5 years calculated in accordance with paragraph 33(1);

Paragraph 33(1) of the Code requires CDD to be retained for at least 5 years from the end of the business relationship.

(d) establish and maintain records of all transactions between the introducer and the customer if the records are concerned with or arise out of the introduction (whether directly or indirectly) for at least 5 years calculated in accordance with paragraph 33(1);

Paragraph 33(1) of the Code requires transaction records to be retained for at least 5 years from the date of the transaction.

(e) supply to the relevant person immediately on request, copies of the evidence verifying the identity of the customer and the beneficial owner (if any) and all other CDD information held by the introducer in any particular case;

The relevant person may request copies in order to satisfy the requirement to test the introducer's procedures or in relation to the appropriate scrutiny of unusual activity, the investigation of suspicious activity or in connection to a request from a competent authorities.

(f) supply to the relevant person immediately copies of the evidence verifying the identity of the customer and the beneficial owner (if any) and all other CDD information, in accordance with paragraphs 10(1), 12(1), 17(1) or 19(1) (as applicable), held by the introducer in any particular case if —

(i) the introducer is to cease trading;
(ii) the introducer is to cease doing business with the customer; or
(iii) the relevant person informs the introducer that it no longer intends to rely on the terms of business entered into;

(g) inform the relevant person specifically of each case where the introducer is not required or has been unable to verify the identity of the customer or the beneficial owner (if any);

This is relevant where a customer's identity information may change (such as name or address), if the introducer is then unable to verify this information, this must be disclosed to the relevant person.

(h) inform the relevant person if the introducer is no longer able to comply with the provisions of the written terms of business because of a change of the law applicable to the introducer; and

There may on occasion be instances where an introducer is unable to satisfy the requirement of the Code for example if there has been a change in secrecy laws in the jurisdiction of the introducer.

(i) do all such things as may be required by the relevant person to enable the relevant person to comply with its obligation under sub-paragraph (8).

Sub-paragraph 8 refers to the testing of procedures.

6.2.4 Eligible Introducers Certificates ("EICs")

Relevant persons can either put written terms of business in place with an Eligible Introducer without EICs having to be produced for each customer or a block of customers; or relevant persons can use EICs for each customer or block of customers. Whichever format is used it must comply with the requirements of the Code. Where one EIC is being used for a block of customers a schedule should be added to the EIC listing the relevant customers.

A template for an EIC which complies with the requirements of the Code for a written terms of business is contained at Appendix E. The EIC at Appendix E is intended as an example / template for relevant persons to use all, or part, as they see appropriate and to tailor to their individual needs, design, corporate style, identity etc.

The proforma EIC is divided into 6 sections. Section 1 should be completed for all business introduced using an EIC. The text of section 1 should not be altered as this satisfies the Code's requirement for written terms of business to be in place between the relevant person and the Eligible Introducer. Sections 2, 3, 4 and 5 have been designed as a central point for identification and relationship information.

The Authority recognises that some businesses may have designed their own forms to obtain the relevant information. Provided all the relevant information is collected these forms will be just as acceptable to use as the example in Appendix E.

Where a "block" of business is being introduced (not to be confused with acquisition of a block of customers at part 6.6 of this Handbook), section 1 of the EIC, accompanied by a schedule listing all the customers' details or relevant copies of sections 2, 3 and 4 for each customer may be accepted.

6.2.5 Disapplication of the EI Concession

Where the customer poses a higher risk of ML/FT

Where the customer has been assessed as posing a higher risk of ML/FT, paragraph 15(3) of the Code disapplies paragraph 23(5) of the Code which states that the verification documentation of the customer does not have to be produced. Therefore, the relevant person has to ID&V the customer and has to obtain the verification documentation, it cannot rely on the introducer to hold this. Also, as the customer has been assessed as posing a higher risk paragraph 15(1) of the Code states that the relevant person must obtain EDD in relation to the customer.

It is important to differentiate between the risk assessment of the underlying customer and the risk assessment of the eligible introducer itself. Just because a customer is assessed as being higher risk, this does not mean that the relationship between the relevant person and the eligible introducer has changed. The terms of business in place would not have changed and would still be valid.

Therefore, the Authority considers that, subject to certain safeguards being in place as stated below (and a terms of business/EIC being in place), it would be acceptable for a relevant person to receive copies of certified customer identity documents held by eligible introducers to verify customer identity. The additional safeguards which apply in order to be able to use this exception for higher risk customers are:

- the eligible introducer must be located on the Isle of Man (or in Jersey or Guernsey where the relevant person operates in these jurisdictions);
- the conditions in section 6.2.2 of this Handbook must have been met;
- the eligible introducer must not be considered higher risk by the relevant person;
- expired documents are not acceptable as verification of the identity of an individual (relevant persons should not accept expired documents from a direct customer as a form of identity verification); and
- the eligible introducer must be able to confirm to the relevant person that they are satisfied with the suitability of the certifier of the document(s).

In relation to non-eligibly introduced relationships, which allow relevant persons to obtain information and documentation from an introducer rather than the customer directly, this arrangement is still permitted where the customer has been assessed as posing a higher risk of ML/FT. However, the EDD requirements for higher risk customers must be met.

Where the introducer is higher risk

As stated in Paragraph 23(5)(e) of the Code in order to use the EI concession the relevant person must be satisfied that the introducer does not pose a higher risk of ML/FT. Therefore in this instance the concession is disapplied.

In relation to non-eligibly introduced relationships, which allows relevant persons to obtain information and documentation from an introducer rather than the customer directly, this arrangement is still permitted where the introducer has been assessed as posing a higher risk of ML/FT as reliance is not being placed on the introducer.

Where the conditions detailed under 6.2.2 have not been met

If relevant persons are aware of any cases where introducers have incorrectly been treated as eligible, they must take steps to obtain suitable CDD information and verification documents in relation to each affected customer. Where the conditions in 6.2.2 of this Handbook are no longer being met the, terms of business in place with that introducer are no longer valid.

IOMFSA Licenceholders licensed under the FSA are reminded of the requirement under Rule 8.1~~4~~7 of the FSRB to report any material breaches of the regulatory requirements to the Authority.

Where there is unusual activity

Where there is either an eligible or non-eligible arrangement in place, if there is unusual activity, such as a transaction, or series of transactions, appearing unusually large or complex, the relevant person must appropriately scrutinise the activity including conducting EDD in relation to that customer. It should consider whether the use of concession remains appropriate.

Where there is suspicious activity

If there is suspicious activity, the EI concession (ability to rely on the introducer to verify the customer's identity and hold the customer's verification documentation) no longer applies. As the concession no longer applies the relevant person would have to undertake its own verification of the customer's identity. It should also consider obtaining EDD in line with paragraph 15 of the Code. Where there is a suspicious activity an internal disclosure must be made.

There is no Code requirement to disapply the concession for non-eligibly introduced relationships (ability to obtain information and documentation from an introducer) in the event of a suspicious activity but there is the requirement to make an internal disclosure and consider conducting EDD. In addition to this, the relevant person should consider whether the use of the concession remains appropriate.

6.3 Acceptable Applicants

6.3.1 Introduction to the Acceptable Applicant ("AA") Concession

Paragraph 20 of the Code provides a concession where the relevant person's customer is an "acceptable applicant". Subject to conditions, the verification of the customer's identity (including the verification of identity of its beneficial owners and controllers) is not required for a new business relationship or occasional transaction.

6.3.2 Conditions to use the AA Concession

In order to use the AA concession, the following conditions apply:

(a) the identity of the customer is known to the relevant person;
(b) the relevant person knows the nature and intended purpose of the business relationship or occasional transaction; and
(c) the customer is an acceptable applicant which includes;
    (i) a trusted person; or
    (ii) a company listed on a recognised stock exchange[11] or a wholly owned subsidiary of such a company in relation to which the relevant person has taken reasonable measures to establish that there is effective control of the company by an individual, group of individuals or another legal person or arrangement (which persons are treated as beneficial owners for the purposes of this Code;)

The Authority is aware that for administrative purposes, life companies sometimes use policy identifiers when investing funds back to the life company's policyholder liabilities. For the avoidance of doubt, where the life company is the legal and beneficial owner of the funds and the policyholder has not been led to believe that they have rights over the account or investment, the life company is the customer.

6.3.3 AA Certificate

Relevant persons must obtain and retain documentation establishing that the customer is entitled to benefit from the concession. An AA Certificate may be used for this purpose. A template is provided at Appendix F of this Handbook.

[11] 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 ("MiFID"). For entities listed outside Europe, this means regulated markets subject to disclosure requirements consistent with MiFID. For example, in the context of the London Stock Exchange, this would include the Main Market but would not include the Alternative Investment Market.

6.3.4 Disapplication of the AA Concession

The concession may not be used when the conditions set out in part 6.3.2 of the Handbook are not met. It is also disapplied in the following circumstances:

Higher risk of ML/FT
Paragraph 20(2)(d)(iii) of the Code disapplies the use of the concession where the customer has been identified as posing a higher risk of ML/FT. In these circumstances the relevant person must verify the identity of the customer and must obtain EDD on the customer as stated in paragraph 15 of the Code.

Where there is unusual activity
If there is unusual activity such as the transaction appearing unusually large or complex, the relevant person must undertake appropriate scrutiny of the transaction, conduct EDD in line with paragraph 15 of the Code and consider whether to make an internal disclosure. It should also consider whether the use of the concession remains appropriate.

Where there is suspicious activity
If there is suspicious activity identified, the concession no longer applies and the relevant person must identify, and verify the identity of, that customer. Also, EDD should be considered in line with paragraph 15 of the Code and an internal disclosure must be made

6.4 Person in a Regulated Sector Acting on Behalf of a Third Party

6.4.1 Introduction to the 'acting on behalf of' concession

Paragraph 21 of the Code allows for the disapplication of paragraph 13(2)(c) of the Code where certain Regulated Persons are providing services to an 'allowed business' who is acting on behalf of a third party ("the underlying client").

This means that, subject to certain conditions, the Regulated Person does not have to identify and verify the identity of the person on whose behalf their customer is acting.

For example, where an allowed business seeks to hold money on behalf of its clients in a separate and designated pooled client account, they may avail themselves of this concession. Examples of a pooled client account which may be within the scope of this definition include:

- an advocate holding an account for funds to purchase a property;
- a CSP holding funds as an advance against fees or registry fees; or
- e-gaming business holding players funds.

6.4.2 Who can use the 'acting on behalf of' concession

This concession may only be used by:

(a) an IOMFSA Class 1 (deposit taking) licenceholder;
(b) an IOMFSA Class 2 (investment business) licenceholder;
(c) an IOMFSA Class 3 (services to collective investment schemes) licenceholder; or
(d) an IOMFSA Class 8 (money transmission services) licenceholder.

The person using the concession is referred to in this part of the Handbook as the "regulated person".

It may only be used where the customer is an "allowed business" defined as:

(a) a regulated person;
(b) a nominee company of a regulated person where the regulated person is responsible for the nominee company's compliance with the AML/CFT requirements;
(c) a collective investment scheme (except for a scheme within the meaning of Schedule 3 (exempt schemes) to the Collective Investment Schemes Act 2008) where the manager or administrator of such a scheme is a regulated person, or where the person referred to in sub-paragraph (2)(a) is an equivalent scheme in a jurisdiction in List C where the manager or administrator of that scheme is a person referred to in sub-paragraph (6)(e);
(d) a designated business;
(e) a person who acts in the course of an external regulated business and who is —
    (i) regulated under the law of a jurisdiction in List C; and
    (ii) subject to AML/CFT requirements and procedures that are at least equivalent to the Code,
    but does not solely carry on activities equivalent to either or both of Class 4 (corporate services) or Class 5 (trust services) under the Regulated Activities Order 2011; or
(f) a nominee company of a person specified in (e) where that person is responsible for the nominee company's compliance with the equivalent AML/CFT requirements.

The Handbook uses this term "allowed business" to refer to the customer in this part.

The customer on whose behalf the allowed business is acting on behalf of is referred to as the "underlying client" which includes the beneficial owner of that underlying client.

6.4.3 Conditions to use the 'acting on behalf of' concession

In order to use the concession, the following conditions must be met in addition to checking that both the business / regulated person using the concession and the customer / allowed business it is being used for meet the requirements detailed in 6.4.2 of this Handbook.

(a) the regulated person has satisfied itself that the customer [allowed business] is a person specified in sub-paragraph 21(6) of the Code;

Appropriate evidence must be obtained to verify the customer is an allowed business referred to in the above sub-paragraph of the Code, which is replicated in part 6.4.2 of the Handbook. The regulated person must take such measures as necessary to ensure it becomes aware of any material change to the allowed business's status.

(b) the customer [allowed business] has identified and verified the identity of the underlying client in accordance with paragraphs 10 to 13 and has no reason to doubt those identities;

(c) the regulated person and the customer [allowed business] know the nature and intended purpose of the business relationship;

(d) the customer [allowed business] has identified the source of funds of the underlying client;

(e) the regulated person has not identified any suspicious activity; and

See 6.4.6 disapplication of the concession for further details.

(f) written terms of business are in place between the regulated person and the customer [allowed business] in accordance with sub-paragraph (3).

The regulated person must put in place terms of business between themselves and the allowed business as required under paragraph 21(2)(f) of the Code. These requirements are explained under section 6.4.4 of this Handbook.

And…

(a) In satisfying the conditions under sub-paragraph 21(2), the regulated person must take reasonable measures to ensure that —

(i) the evidence produced or to be produced is satisfactory; and
(ii) the customer due diligence procedures of the customer [allowed business] are fit for purpose.

This should involve the regulated person conducting an assessment of its own internal procedures and those of the customer to ensure that the conditions to use the concession are met.

In assessing the allowed business's procedures, the regulated person should consider:

- conducting a review of the allowed business's policies and procedures;
- making enquiries concerning the allowed business's stature and regulatory track record and the extent to which any group standards are applied and audited; or
- seeking copies of an independent review of the allowed business's procedures by external auditors and other experts.

(b) the regulated person must take reasonable measures to satisfy itself that —

(i) the procedures for implementing this paragraph are effective by testing them on a random and periodic basis no less than once every 12 months; and

(ii) the written terms of business confer the necessary rights on the regulated person.

Paragraph 21(5) of the Code requires the regulated person to test that the procedures are compliant. On a random and periodic basis (at least once every 12 months), the regulated person should request details of any changes in the aforementioned procedures and a copy of CDD on a sample of underlying clients which should include:

- the most recent copy of the allowed businesses risk assessment on the underlying client along with any relevant supporting documentation or information if available.
- the identification information on the underlying client required by Part 4 of the Code and copies of the verification of that identification. And;
- evidence that the record keeping requirements under paragraphs 32, 33 and 34 of the Code are being complied with. If the allowed business can provide all of the above within 7 working days, this part would be deemed to have been complied with.

If transactions are pooled before receipt by the relevant person and the relevant person is therefore unable to identify an underlying customer by name or by transaction size and date, the relevant person should request information, such as a reconciliation, from their customer to assist in identifying a test sample.

If the customer cannot provide this information, the rationale for this must be documented and the relevant person must carry out alternate methods to satisfy itself of the effectiveness of the terms of business. The relevant person should review the CDD procedures of their customer and consider

speaking to their customer's staff or conducting a visit to their premises for further comfort.

6.4.4 'Acting on behalf of' terms of business

Paragraph 21(3) of the code states that there must be a written terms of business in place which requires the allowed business to:

(a) supply to the regulated person immediately on request, information on the identity of the underlying client, copies of the evidence verifying the identity of the underlying client and all other due diligence information held by the customer [allowed business] in respect of the underlying client in any particular case;

This also includes where the regulated person may seek confirmation that a named underlying client is in a pool. For example; where a bank asks a TCSP whether an underlying client by the name of "Mr X" is, or has been, in a pooled account operated by the bank for that TCSP.

Also, the regulated person may request copies in order to satisfy the requirement to test the allowed business's procedures or in relation to the appropriate scrutiny of unusual activity, the investigation of suspicious activity or in connection to a request from competent authorities.

(b) inform the regulated person specifically of each case where the customer [allowed business] is not required or has been unable to verify the identity of the underlying client;

This is relevant where an underlying client's identity information may change (such as name or address), if the allowed business is then unable to verify this information, this must be disclosed to the regulated person.

(c) inform the regulated person if the customer [allowed business] is no longer able to comply with the provisions of the written terms of business because of a change of the law applicable to the customer [allowed business]; and

There may on occasion be instances where an allowed business is unable to satisfy the requirement of the Code for example if there has been a change in secrecy laws in the jurisdiction of the allowed business.

(d) do all such things as may be required by the regulated person to enable the regulated person to comply with its obligations under sub-paragraph 21(2).

6.4.5 'Acting on behalf of' certificate (includes terms of business)

There is a template in Appendix G for a certificate / terms of business to be used when utilising this concession. The certificate at Appendix G is intended as an example / template for relevant persons to use all, or part, as they see appropriate and to tailor to their individual needs, design, corporate style, identity etc. The Authority recognises that some businesses may have designed their own forms to obtain the relevant information. Provided all the relevant information is collected these forms will be just as acceptable to use as the example in Appendix G.

6.4.6 Use of the 'acting on behalf of' concession

The concession may not be used when the conditions set out in part 6.4.3 of the Handbook are not met. It is also disapplied in the following circumstances:

Where the allowed business has been identified as posing a higher risk of ML/FT

The concession need not be disapplied if the allowed business has been identified as posing a higher risk of ML/FT but the Authority expects the regulated person to exercise their own judgement in determining whether the concession remains appropriate.

Where the underlying client has been identified as posing a higher risk of ML/FT

The concession need not be disapplied where the underlying client has been identified (by the allowed business) as posing a higher risk of ML/FT but the regulated person must remain satisfied that the allowed business has met and continues to meet the EDD requirements in relation to that underlying client.

Where there is unusual activity

If there is unusual activity, such as a transaction, or series of transactions, appearing unusually large or complex, the regulated person must appropriately scrutinise the activity including conducting EDD in relation to that customer and consider whether to make an internal disclosure. It should consider whether the use of concession remains appropriate.

Where there is suspicious activity

If there is suspicious activity the concession allowing the allowed business to identify and verify the identity of the underlying client is disapplied under paragraph 21(2)(e) of the Code. The regulated person would therefore need to identify, and verify the identity of, the underlying client. It should also

consider obtaining EDD in line with paragraph 15 of the Code. Where there is a suspicious activity an internal disclosure must be made.

6.5 Exempted Occasional Transactions

As defined in paragraph 3 of the Code, an 'occasional transaction' means any transaction (whether a single transaction or series of linked transactions) other than a transaction carried out in the course of an established business relationship between a relevant person and a customer.

Procedures must be in place to ensure that CDD procedures are conducted in line with the requirements of the Code in respect of occasional transactions. If satisfactory CDD is not obtained the occasional transaction must not be carried out and the relevant person must consider making an internal disclosure.

An 'exempted occasional transaction' means an occasional transaction (whether a single transaction or a series of linked transactions) where the amount of the transaction, or as the case may be, the aggregate in a series of linked transactions, is less in value than:

1. €3,000 in the case of a transaction entered into in the course of business referred to in paragraph 1(l) (casinos) or 1(n) (bookmakers) of Schedule 4 to the *Proceeds of Crime Act 2008*; or
2. €5,000 in the case of a transaction entered into in the course of business referred to in paragraph 1(x) (*bureau de change)* or 1(z) (cheque encashment only) *of Schedule 4 to the Proceeds of Crime Act 2008*; or
3. €1,000 in the case of a transaction entered into in the course of business referred to in paragraph 1(z) (money transmission services apart from cheque encashment) or 1(mm) (virtual currency) of Schedule 4 to the *Proceeds of Crime Act 2008*; or
4. €15,000 in any other case;

Paragraph 12(5) of the Code disapplies the requirement to verify the identity of the customer if the transaction is an exempted occasional transaction. The relevant person must however comply with the other CDD requirements in paragraph 12 such as knowing the identity of the customer, having relevant information about the purpose and intended nature of the transaction and taking reasonable measures to establish the source of funds. Requirements under other paragraphs also still apply such as those in paragraph 7 (customer risk assessment), 13 (beneficial ownership and control), 14 (politically exposed persons) and 15 (enhanced due diligence).

If there is unusual activity such as the transaction appearing unusually large or complex, the relevant person must scrutinise the activity, must conduct EDD as stated in paragraph 15 of the Code and must consider whether to make an internal disclosure. It should also consider whether the use of the concession remains appropriate.

If there is suspicious activity as defined in paragraph 3 of the Code, the concession to not verify the identity of the customer no longer applies. Appropriate verification of

identity must be obtained and EDD must be considered in line with paragraph 15 of the Code. In the case of suspicious activity an internal disclosure must be made.

A relevant person should be vigilant at all times that the total of a series of linked transactions does not exceed the exempted limits. Where the limits are exceeded, full CDD procedures must be applied immediately. The Authority recognises the difficulty in defining a timescale that linked transactions may fall within, and would recommend three months is used as the minimum acceptable standard.

6.6 Acquisition of a Block of Business

Paragraph 24(11) of the Code provides a CDD concession regarding the acquisition of a block of business. Where a relevant person (the "purchaser") is acquiring a customer or group of customers from another relevant person (the "vendor") the acquired customer or group of customers will be a new business relationship for the purchaser. CDD and EDD relating to the customer may be provided to the purchaser by the vendor.

The purchaser may acquire the business or block of business for consideration or with no consideration. In either circumstance paragraph 24(11) of the Code still applies and the relevant person remains referred to as a "purchaser"

In order to use this concession, and to rely on documentation and information previously obtained by the vendor, the following conditions must be met:

1. the vendor is —
   (i) a regulated person;
   (ii) a collective investment scheme (except for a scheme within the meaning of Schedule 3 (exempt schemes) to the *Collective Investment Schemes Act 2008*) where the manager or administrator of such a scheme is a regulated person, or where the vendor is an equivalent scheme in a jurisdiction in List C where the manager or administrator of that scheme is a person referred to in sub-paragraph (12)(a)(iv);
   (iii) a designated business;
   (iv) a person who acts in the course of external regulated business and who is —
      (A) regulated under the law of a jurisdiction in List C; and
      (B) subject to AML/CFT requirements and procedures that are at least equivalent to the Code,
   but does not solely carry on activities equivalent to either or both of Class 4 (corporate services) or Class 5 (trust services) under the Regulated Activities Order 2011;
2. the purchaser —
   (i) has identified the customer and the beneficial owner (if any) and has no reason to doubt those identities;
   (ii) has not identified the customer as posing a higher risk of ML/FT;

(iii) knows the nature and intended purpose of the business relationship;
(iv) has identified the source of funds;
(v) has not identified any suspicious activity; and
(vi) has put in place appropriate measures to remediate, in a timely manner, any deficiencies in the CDD of the acquired customer or group of customers.

The purchaser will need to undertake a risk assessment as soon as practicable of each customer being acquired to determine whether or not this concession may apply or whether it must obtain its own CDD. The Authority would expect this to be undertaken within 3 months of the purchase but there may be flexibility on this on a risk based approach (such as where a particularly large block of business is acquired and 3 months is impractical). The purchaser may not rely on the vendor's risk assessment for this purpose and should form their own view, based on their own systems, procedures and business risk assessment.

Where any of the conditions at 2 above are not met in respect of a customer (whether alone or within a block of customers) being acquired (including where the purchaser determines that the customer poses a higher risk of ML/FT) the concession at 24(11) does not apply in respect of that customer and the purchaser must obtain its own CDD on that customer. The concession may still be applied in respect of other customers to be acquired in the same block where they meet the conditions.

Where there are deficiencies identified in the CDD information and verification documentation the relevant person must determine and implement a programme to apply CDD and verification procedures on each customer to remedy deficiencies as soon as is practicable.

6.7 Miscellaneous (exceptions)

6.7.1 Contracts of insurance

Paragraphs 24 (1) – (6) of the Code provide some concessions in relation to contracts of insurance. Please refer to guidance issued for persons regulated under the insurance Act 2008 for further details on these particular concessions.

6.7.2 Retirement benefit schemes

Paragraph 24(7) of the Code provides a concession (subject to conditions), in relation to where the product or service is a pension, superannuation or similar scheme the relevant person:

(a) may treat the employer, the trustee and any other person who has control over the business relationship including the administrator or the scheme manager, as the customer; and
(b) need not comply with the provisions of 13(2)(c) of the Code (the requirement for relevant persons to identify and take reasonable

measures to verify the identity of any person on whose behalf the customer is acting).

The following conditions must be met to use the concession:

- the pension, superannuation or similar scheme must provide retirement benefits to employees;
- contributions must be made by way of deductions from wages; and
- the scheme rules do not permit the assignment of a member's interest under the scheme.

If there is a suspicious activity as defined in paragraph 3 of the Code, the concession no longer applies and EDD should be considered in line with paragraph 15 of the Code and an internal disclosure must be made.

If there is an unusual activity such as the transaction appearing unusually large or complex, the relevant person should scrutinise the activity and consider whether the use of the concession remains appropriate. Furthermore it must conduct EDD on the customer in order to appropriately investigate the activity.

Where a customer poses a higher risk of ML/FT as assessed by the customer risk assessment the concession does not apply under 15(3) of the Code.

6.7.3 Collective investment schemes

There is a CDD concession under paragraph 24(8) of the Code in relation to where a customer is a collective investment scheme.

Where a relevant person enters a relationship with a customer it should undertake appropriate CDD in line with the requirements of the Code. Also, the relevant person must comply with the requirements in paragraph 13(2)(c) of the Code which states that a relevant person should determine if the customer is acting on behalf of another person and identify, and take reasonable measures to verify the identity of that person.

However, if certain conditions are met, paragraph 24(8) of the Code provides a concession to the Code requirement at paragraph 13(2)(c). This concession may be used where a relevant person's customer is a collective investment scheme (except exempt schemes), or an equivalent arrangement in a jurisdiction in List C (Appendix C) of the AML/CFT Handbook and if the manager or administrator of the scheme is a regulated person or a person acting in the course of external regulated business carrying on equivalent regulated activities ~~jurisdiction~~ in a List C jurisdiction.

Therefore, if these conditions are met the business does not have to comply with paragraph 13(2)(c) and it can treat the collective investment scheme as its customer, meaning it does not have to identify and verify the identity of the underlying investors in the scheme.

The remaining provisions of the Code such as the requirement to conduct a risk assessment, ongoing monitoring provisions etc. continue to apply.

As stated in paragraph 24 (10) of the Code, if there is a suspicious activity as defined in paragraph 3 of the Code, the concession no longer applies and EDD must be considered in line with paragraph 15 of the Code and an internal disclosure made. If there is an unusual activity such as the transaction appearing unusually large or complex, the business should undertake EDD in line with paragraph 15 of the Code and consider whether the use of the concession remains appropriate.

Also, as stated in paragraph 15 of the Code, this concession cannot be used if the customer is identified as posing a higher risk of ML/FT. In these circumstances EDD must be undertaken on the customer.

6.7.4 Isle of Man Post Office

There is a CDD concession under paragraph 24(9) of the Code in relation to the business of the Isle of Man Post Office.

Where a customer poses a higher risk of ML/FT as assessed by the customer risk assessment the concession does not apply under 15(3) of the Code.

If there is a suspicious activity the use of this concession is disapplied as stated in paragraph 24(10) of the Code.

Please refer to the Isle of Man Post Office specific guidance for further details of this concession.

6.8 Generic Designated Business

Designated businesses may avail themselves of the concession at paragraph 22 of the Code which states that a customer's identification need not be verified if the relevant person is conducting generic designated business provided that the conditions are met.

The conditions are as follows:

(a) the relevant person has identified the customer (any beneficial owners) and has no reason to doubt those identities;
(b) the customer has not been identified as posing a higher risk of ML/FT
(c) the relevant person knows the nature and intended purpose of the business relationship;
(d) the relevant person has not identified any suspicious activity; and;
(e) the relevant person has identified the source of funds.

Generic designated business means designated business carried on by a relevant person that does not involve participation in any financial transactions on behalf of

thecustomer. The provision of professional advice or audit services may be examples of generic designated business.

Certain businesses such as accountants and tax advisors may seldom “participate in” financial transactions, albeit they will frequently advise on aspects of a financial transaction, such advice would reasonably be assessed as generic designated business.

Where a customer poses a higher risk of ML/FT as assessed by the customer risk assessment the concession does not apply under 15(3) of the Code.

Further information is provided in relation to this concession in the sector specific guidance for Accountants and Tax Advisors.

Part 7 – Unusual and Suspicious Activity

7.1 Introduction

Relevant persons have the opportunity to observe the day to day transactions of their customers. Law enforcement agencies do not have unlimited resources to monitor every transaction performed in the financial system by every individual or business but do have access to confidential information relating to known or suspected criminals and terrorists.

The FATF Recommendations, and in turn, the Island's AML/CFT framework is designed to match the respective strengths of each party to achieve two key effects:

1. strategically, as a result of increased detection and prosecution success, the framework raises the cost of ML and subsequently reduces the profitability of crime; and

2. operationally,

    - it disrupts criminal operations by freezing laundered assets;
    - it slows down the rate at which laundering can occur by setting caps;
    - it puts assets beyond the use of criminals through seizure;
    - it improves the quality of evidence available for prosecutions; and
    - it creates tension and schisms between criminal/terrorist financiers and the operational/tactical arms of their organisations leading to weaknesses that can be exploited by the authorities.

In the absence of being able to positively determine whether a customer is a person of interest to the authorities, it is inevitable that a proportion of SARs will result in no further action. The effort however must not be considered wasted. The submission of usefully detailed information allows the authorities to cross refer reported individuals or businesses with intelligence databases and when matches do occur, the authorities gain valuable opportunities to exploit the information.

Relevant persons can assist the authorities by ensuring that any reports they submit and the records they keep refer to credible suspicions and are detailed enough to allow the authorities to efficiently bracket individuals or businesses on their databases and to establish audit trails of the suspects' transactions.

7.2 Code Requirements

7.2.1 Role of the Money Laundering Reporting Officer

Paragraph 25 of the Code requires relevant persons to appoint a MLRO to exercise functions conferred by paragraphs 26 (reporting procedures) and 28 (external disclosures) of the Code.

Paragraph 25 of the Code states the MLRO must:

(a) be sufficiently senior in the organisation of the relevant person or have sufficient experience and authority;

(b) have a right of direct access to the directors or the managing board (as the case may be) of the relevant person; and
(c) have sufficient time and resources to properly discharge the responsibilities of the position,

to be effective in the exercise of its functions.

The MLRO is the person who is nominated to ultimately receive internal disclosures and who considers any report to determine whether an external disclosure is required.

A relevant person may appoint a Deputy Money Laundering Reporting Officer ("DMLRO") in order to exercise the functions in the MLRO's absence. The DMLRO should be of similar status and experience to the MLRO. Please note that licenceholders subject to the FSRB must appoint a DMLRO as per Rule 8.21 of the FSRB. Where this Handbook refers to the MLRO it means the DMLRO in the MLRO's absence.

Whilst not a requirement under the Code, the Authority would expect all relevant persons to appoint an MLRO who is normally resident on the Island. This is also a requirement for licenceholders subject to the FSRB under rule 8.21.

The principal objective of the MLRO is to act as the focal point within a relevant person for the oversight of all activity relating to the prevention and detection of ML/FT. The responsibilities of the MLRO will normally include:

1. undertaking a review of all internal disclosures in the light of all available relevant information and determining whether or not such internal disclosures have substance and require an external disclosure to be made to the FIU;
2. maintaining all related records;
3. giving guidance on how to avoid tipping off the customer if any disclosure is made and managing any resulting constructive trust scenarios;
4. providing support and guidance to the board and senior management to ensure that ML/FT risks are adequately managed;
5. liaising with the FIU and if required the Authority and participating in any other third party enquiries in relation to money laundering or terrorist financing prevention, detection, investigation or compliance; and;
6. providing reports and other information to senior management.

7.2.2 Unusual activity

Unusual activity is defined in paragraph 3 of the Code and includes any activity or information relating to a business relationship, occasional transaction or an attempted transaction where there is no apparent economic or lawful purpose, including transactions that are –

(i) complex;
(ii) both large and unusual; or
(iii) of an unusual pattern.

Unusual activity also includes anything that causes the relevant person to doubt the identity of the customer (including beneficial owners and controllers or introducer where appropriate) or anything that causes the relevant person to doubt the good faith of the customer (including beneficial owners and controllers or introducer where appropriate).

Situations that are likely to appear unusual include:

1. transactions or instructions which have no apparent legitimate purpose and appear not to have a commercial rationale;
2. transactions, instructions or activity that involve apparent unnecessary complexity;
3. where the transaction being requested by the customer is out of the ordinary range;
4. where the size or pattern of transactions is out of line with expectations for that customer;
5. where the customer is not forthcoming with information about their activities, reason for a transaction, source of funds, CDD documentation etc.;
6. where the customer who has entered into a business relationship uses the relationship for a single transaction or for only a very short period of time where that was not expected;
7. the extensive use of offshore structures where the customer's needs are inconsistent with the use of such services;
8. transfers to or from high risk jurisdictions which are not consistent with the customer's expected activity;
9. unnecessary routing of funds through third party accounts;
10. unusual investment transactions with no discernible purpose; and
11. extreme urgency in requests from the customer, particularly where they are not concerned by large transfer fees, early repayment fees etc.

Please note that this is not an exhaustive list.

Unusual activity is likely to be detected during ongoing monitoring (see parts 3.4.1 and 3.4.2 of the Handbook), when receiving an application from a new customer, when receiving an instruction to carry out a transaction or during other communications with the customer.

Where a relevant person identifies unusual activity, paragraph 27(2) of the Code requires relevant persons to perform 'appropriate scrutiny' of the activity and to obtain EDD. Appropriate scrutiny of the activity may involve making enquiries of the customer and asking the questions an honest man would reasonably ask in the circumstances. For further detail on how to conduct 'appropriate scrutiny', please refer to part 7.5 of this Handbook.

7.2.3 Suspicious activity reporting procedures

Paragraph 3 of the Code defines 'suspicious activity' as

> *"any activity or information received in the course of a business relationship, occasional transaction or attempted transaction that causes the relevant person to –*
>
> *(a) know or suspect; or*
> *(b) have reasonable grounds for knowing or suspecting,*
>
> *that the activity or information is related to money laundering or the financing of terrorism"*

The reporting procedures required under paragraph 26 of the Code must also apply to prospective customers and transactions that were attempted but that did not take place.

This paragraph of the Code requires a relevant person to have documented reporting procedures in place that will:

(a) enable all its directors, management and all appropriate employees and workers to know to whom they should report any knowledge or suspicion of ML/FT activity;
(b) ensure that there is a clear reporting chain to the MLRO[12];
(c) require reports to be made to the MLRO ("**internal disclosures**") of any information or other matters that come to the attention of the person handling that business and which in that person's opinion gives rise to any knowledge or suspicion that another person is engaged in ML/FT activity;
(d) require the MLRO to then consider these reports in the light of all other relevant information available to determine whether or not it gives rise to any knowledge or suspicion of ML/FT activity;
(e) ensure that the MLRO has full access to any other available information that may be of assistance; and
(f) enable the information or other matters contained in a report ("**external disclosure**") to be provided as soon as is practicable the Financial Intelligence Unit if the MLRO knows or suspects that another is engaged in ML/FT activity.

The recording of internal and external disclosures are covered further in 7.2.6 of this Handbook.

[12] By way of additional guidance the IOMFSA would expect that a clear reporting chain would not allow for reports to be filtered or delayed. Reports could be referred to supervisors or a technical expert for guidance but a staff member must ensure if they have a suspicion the STR must be made in accordance with the Code and POCA.

7.2.4 Internal disclosures

Where suspicious activity is identified an internal disclosure must be made to the MLRO in accordance with paragraphs 26 and 27 of the Code. It is the responsibility of the MLRO (or if appropriate the Deputy MLRO) to consider all internal disclosures he/she receives in the light of full access to all relevant documentation, this may include reviewing CDD, transaction patterns and other connected accounts / relationships. The evaluation process should be fully documented. All relevant persons must ensure that the MLRO receives full cooperation from all staff and full access to all relevant documentation so that he/she is in a position to decide whether ML/FT (whether attempted or actual) is suspected or known.

Failure by the MLRO to diligently consider all relevant material may lead to vital information being overlooked and the suspicious transaction or activity not being externally disclosed to the FIU in accordance with the requirements of the legislation. Alternatively, it may lead to vital information being overlooked which may have made it clear that a disclosure would have been unnecessary. As a result, the MLRO must document internal disclosures made by employees to record the results of the assessment of each disclosure.

Relevant persons must ensure that all employees are made aware of the identity of the MLRO and his/her Deputy, and the procedure to follow when making an internal disclosure report to the MLRO. Reporting lines should be as short as possible with the minimum number of people between the employee with suspicion and the MLRO. This ensures speed, confidentiality and accessibility to the MLRO. All disclosure reports must reach the MLRO without any undue delay. Under no circumstances should reports be filtered out by supervisors or managers such that they do not reach the MLRO.

All suspicions reported to the MLRO must be documented (in urgent cases this may follow an initial discussion by telephone). The report must include the full details of the customer and as full a statement as possible of the information giving rise to the suspicion.

The MLRO should acknowledge receipt of the internal disclosure and at the same time, provide a reminder of the obligation to do nothing that might prejudice enquiries i.e. tipping off the customer or any other third party.

7.2.5 External disclosures

Paragraph 28(1) requires the MLRO, in the event of an internal disclosure being made, to assess the information contained within the disclosure to determine whether there are reasonable grounds for knowing or suspecting that the activity is related to ML/FT.

Paragraph 28(2) requires the MLRO to make an external disclosure (in line with their reporting procedures established under paragraph 26) as soon as is practicable to the Financial Intelligence Unit if the MLRO-

(a) knows or suspects; or
(b) has reasonable grounds for knowing or suspecting,

that another is engaged in ML/FT.

For further information on the specific reporting requirements in relation to POCA and ATCA offences, please refer to Section 7.6 of the Handbook.

7.2.6 Recording of internal and external disclosures

Paragraph 35 of the Code requires the relevant person to establish and maintain a register of all ML/FT internal disclosures made to the MLRO or Deputy MLRO. The register must include details of:

- the date the report was made;
- the person who made the report;
- whether the report was made to the MLRO or Deputy MLRO; and;
- information to allow the papers and relevant documentation to be located.

Appendix I contains a pro forma register which may be used as a template for this purpose by relevant persons.

Paragraph 35 of the Code requires the relevant person to establish and maintain a register of all ML/FT external disclosures made to the FIU. The register must include details of:

- the date of the disclosure;
- the person making the disclosure;
- the person to whom the disclosure is being made (by reference to the disclosure acknowledgement from the FIU); and;
- information to allow the papers relevant to the disclosures to be located.

Appendix J contains a pro forma register which may be used as a template for this purpose by relevant persons.

Paragraph 35(2) of the Code states that the registers of internal and external disclosures may be contained in a single document if the details included in the registers can be presented separately for internal and external disclosures upon request by a competent authority.

7.2.7 Recording money laundering and terrorist financing enquiries

Relevant persons may be asked to assist law enforcement or other competent authorities[13] with enquiries relating to ML/FT.

Paragraph 36 of the Code requires a relevant person to establish and maintain a register of all such enquiries. This register must be kept separate from other records and include:

- the date of the enquiry;
- the nature of the enquiry;
- the name and agency of the enquiring officer,
- the powers being exercised; and;
- details of the accounts or transactions involved.

7.3 Overview of Money Laundering, Terrorist Financing, Proliferation and Sanctions

7.3.1 What is money laundering?

In general terms, ML is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of criminal activities. If successful, the criminal property can lose its criminal identity and appear legitimate, meaning that criminals can benefit from their crimes without the fear of being caught by tracing their money or assets back to a crime.

Illegal arms sales, smuggling, and the activities of organised crime, including for example, drug trafficking and prostitution, can generate huge profits. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits and create the incentive to "legitimise" the ill-gotten gains through ML. When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds or assets to a place where they are less likely to attract attention.

In relation to the Proceeds of Crime Act ("POCA") which is the island's primary ML legislation, the term 'money laundering' can be misleading because the money laundering offences (sections 139, 140 & 141 of POCA) relate to criminal property not money.

[13] Defined in the Code as all Isle of Man administrative or law enforcement authorities concerned with AML/CFT, including in particular the Financial Supervision Commission, the Insurance and Pensions Authority (now the Financial Services Authority), the Isle of Man Gambling Supervision Commission, the Department of Home Affairs, the Financial Intelligence Unit, the Office of Fair Trading, the Attorney General and the Customs and Excise and Income Tax Divisions of the Treasury.

Further detail on the POCA offences including the POCA definition of criminal property can be found at 7.4.1 of the Handbook.

Traditional money laundering model:

ML will often involve a complex series of transactions, traditionally considered as representing three separate phases.

Placement: Where the proceeds of crime are placed into the financial system.

Layering: Where funds are converted from one form to another, e.g. moved between various accounts and/or jurisdictions to disguise the audit trail and the illegitimate source of the funds.

Integration: Where funds that now appear legitimate re-enter the economy for what would appear to be normal business or personal transactions.

Rather than getting caught up in trying to establish whether activity relates to a particular phase of the traditional model, the relevant person should ask themselves – "*do I know, suspect or have reasonable ground to suspect that the property in question is criminal property?"*

Further detail on the POCA offences including the POCA definition of criminal property can be found at 7.4.1 of the Handbook.

7.3.2 What is financing of terrorism?

In general terms, FT is the financial support, in any form, of terrorism or those who encourage, plan or engage in terrorism. FT differs from ML in that the source of funds can either be legitimate, such as an individual's salary, or illegitimate, often the proceeds of crimes such as selling pirate DVDs, fraud or drug trafficking.

Usually, the focus of scrutiny for potential terrorist financing activity will be the end beneficiary and intended use of the money or assets. A terrorist financier may only need to disguise the origin of the property if it was generated from criminal activity but in the vast majority of cases they will seek to disguise the intended use i.e. the act of terrorism.

Traditional terrorist financing model:

Terrorist financing often involves a complex series of transactions, generally considered as representing three separate phases.

Collection: Funds are often acquired through seeking donations, carrying out criminal acts or diverting funds from genuine charities.

Transmission: Where funds are pooled and transferred to a terrorist or terrorist group.

Use: Where the funds are used to finance terrorist acts, training, propaganda etc.

Like the traditional three phase model for money laundering, this model is rather simplistic and outdated. Rather than getting caught up in trying to establish whether activity relates to a particular phase of the traditional model, the relevant person should ask themselves – "*do I know, suspect or have reasonable cause to suspect that the property in question is terrorist property?"*

Further detail on the ATCA offences including the ATCA definition of terrorist property can be found at 7.4.2 of the Handbook.

For further information regarding terrorist financing, including typologies, see appendix L.

7.3.3 The consequences of money laundering and terrorist financing

ML/FT can have serious negative consequences for the economy, national security and society in general. Some of these consequences may include:

1. reputational damage from being perceived as being a haven for money launderers and terrorist financiers, leading to legitimate business taking their business elsewhere;
2. attracting criminals including terrorists and their financiers to move to or establish new business relationships within the jurisdiction;
3. damaging the legitimate private sector who may be unable to compete against front companies;
4. weakening of financial institutions who may come to rely on the proceeds of crime for managing their assets, liabilities and operations, plus additional costs of investigations, seizures, fines, lawsuits etc.;
5. economic distortion and instability;
6. increasing tax rates due to the loss of tax revenues following tax evasion; or
7. increased social costs to deal with additional criminality such as policing costs or hospital costs for treating drug addicts.

A summary of potential consequences that can apply to the relevant person and related individuals can be found at part 7.7 of this Handbook.

7.3.4 What is the proliferation of weapons of mass destruction?

Proliferation of weapons of mass destruction ("WMDs") can be in many forms, but ultimately involves the transfer or export of technology, goods, software, services or expertise that can be used in programmes involving nuclear, biological or chemical weapons, and their delivery systems (such as long range missiles). It poses a significant threat to global security. If appropriate safeguards are not established, maintained and enforced for sensitive materials, technology, services and expertise, they can –

- become accessible to individuals and entities seeking to profit from acquiring and selling them on;
- be used in WMD programmes; or
- find their way into the hands of terrorists.

Financial support provided to terrorist organisations that want to acquire and/or use WMD is also by its nature contributing to the proliferation of WMDs.

Proliferation of WMD financing is an important element and, as with international criminal networks, proliferation support networks use the international financial system to carry out transactions and business deals. Unscrupulous persons may also take advantage of the potential profits to be made by facilitating the movements of sensitive materials, goods, technology and expertise, providing seemingly legitimate front organisations or acting as representatives or middlemen.

It is important to note that proliferation of WMDs is illegal regardless of the destination receiving or the intended target of the weapons.

7.3.5 What are international sanctions?

International sanctions are prohibitions and restrictions put in place with the aim of maintaining or restoring international peace and security. They generally target specific individuals or entities; or particular sectors, industries or interests. They may be aimed at certain people and targets in a particular country or territory, or some organisation or element within them. There are also sanctions that target those persons and organisations involved in terrorism, including Al Qaida.

The Isle of Man does not issue its own sanctions lists, instead, Government policy is to maintain a list which is the same as that designated by HM Treasury in the UK. In turn, the UK list reflects both UN and EU measures (both of which publish their own lists), as well some national sanctions. Other sources of sanctions include the Office of Foreign Asset Control (OFAC) in the United States, which may differ from those imposed by the EU or UK. These have no legal effect in the Isle of Man. However, because of

the extra-territorial effect of the US measures, and their implications for international banking transactions in US dollars, any business should take note of them.

The types of sanctions that may be imposed include:

1. targeted sanctions focused on named persons or entities, generally freezing assets and prohibiting making any assets available to them, directly or indirectly (these may be referred to as "specific directions");
2. economic sanctions that prohibit doing business with, or making funds or economic resources available to, designated persons, businesses or other entities, directly or indirectly (these may be referred to as "general directions");
3. currency or exchange control (such as the requirement for prior notification or authorisation for funds sent to or from Iran);
4. arms embargoes, which would normally encompass all types of military and paramilitary equipment (note that certain goods, such as landmines, are subject to a total prohibition and others, such as certain policing and riot control equipment, are subject to strict controls under export and trade control law);
5. prohibiting investment, financial or technical assistance in general or for particular industry sectors or territories, including those related to military or paramilitary equipment or activity;
6. controls on the supply of dual-use items (i.e. items with both a legitimate civilian use as well as a potential military or WMD use), including supplies of technology etc. and intangible supplies;
7. import and export embargoes involving specific types of goods (e.g. oil products), or their movement using aircraft or vessels, including facilitating such trade by means of financial or technical assistance, brokering, providing insurance etc.;
8. measures designed to prevent WMD proliferation; and
9. visa and travel bans (e.g. banning members of a ruling regime from visiting the EU).

All of the above are in addition to –

1. normal import and export controls;
2. trade controls which prohibit or require licensing for trafficking and brokering movements of certain goods (such as military equipment) between other countries (i.e. where the goods are not imported into, or exported from, the Isle of Man or UK); and
3. other EU or international measures on the movements of particular types or categories of goods intended to prevent, monitor or control the trade in those goods, such as –

    (i) the Kimberley Process certification scheme intended to prevent the trade in "blood" or "conflict" diamonds;
    (ii) the Wassenaar Arrangement on dual-use items;
    (iii) the PIC Convention and REACH Regulation on the import, export, manufacture and supply of chemicals;

(iv) EU restrictions on the export of electrical and other waste products;
(v) the FLEGT controls on the import into the EU of timber products; and
(vi) CITES controls on the movements of endangered species.

More information about sanctions, import and export and trade controls can be found on the Isle of Man Customs and Excise website. The Authority recommend that all regulated entities sign up to the Isle of Man Customs and Excise News RSS feed. Isle of Man Customs and Excise have a number of notices and documents which may be of use to regulated entities, these include:

Factsheet 200 MAN - What does my business have to do with EU sanctions and export and trade controls

Sanctions Notice 26 - Financial Sanctions Regimes

Sanctions Notice 22 - Terrorism

Notice 1000 MAN - Trade-Based Money Laundering

What are the obligations?

Isle of Man Customs and Excise, as agent for the Treasury, **directs** that any funds held for or on behalf of the individuals or entities named in the published lists having effect in the Island must not be made available, except under the authority of a licence in writing from the Treasury.

Any funds should be blocked or frozen and the details reported to the FIU. ~~Isle of Man Customs and Excise.~~

All persons in business or a profession in the Island, including financial institutions, **must** check whether they maintain any account, or otherwise hold or control funds or economic resources, for individuals or entities included in the lists and, if so, they should freeze the account, funds or economic resources and report their findings to ~~Isle of Man Customs and Excise.~~the FIU.

Any person, entity or body with information that would facilitate compliance with the sanctions Regulation(s) **must** supply such information to the ~~Division~~ FIU and co-operate in any verification of the information.

If there are details of other involvement with a listed individual or entity, directly or indirectly, or of any attempted (or suspected attempted) transactions involving those individuals or entities, this should also be reported to ~~Isle of Man Customs and Excise~~the FIU.

Payments from Frozen accounts are prohibited unless a written licence has been granted by the Treasury. ~~To seek a written licence form CEM 85 MAN~~

~~should be completed.~~Sanctions Notice 32 gives further information regarding the granting of licences by IOM treasury.

Any breaches of financial sanctions must be reported to ~~Isle of Man Customs and Excise using form CEM 80 MAN.~~the FIU, those registered to use THEMIS should make their reports using this system. For those not registered to use THEMIS, a link to the appropriate form is available on the FIU website [WA1]

Further information regarding sanctions regimes and what action must be taken (including how to deal with false positives) can be found in Sanctions Notice 26 - Financial Sanctions Regimes and Factsheet 300 MAN.

7.4 Summary of Offences Relating to Money Laundering, Terrorist Financing, Proliferation and Sanctions

7.4.1 Money laundering offences

The Proceeds of Crime Act 2008 ("POCA") clarifies the activities that constitute ML and which need to be reported

The interpretation section provides important definitions of 'money laundering', 'criminal conduct' and 'criminal property':

158 Interpretation of Part 3

(1) This section applies for the purposes of this Part.

(2) Criminal conduct is conduct which –
(a) constitutes an offence in the Island; or
(b) would constitute an offence in the Island if it occurred there.

(3) Property is criminal property if –
(a) it constitutes a person's benefit from criminal conduct or it represents such a benefit (in whole or in part and whether directly or indirectly); and
(b) the alleged offender knows or suspects that it constitutes or represents such as benefit.

(4) It is immaterial-
(a) who carried out the conduct;
(b) who benefited from it;
(c) whether the conduct occurred before or after the passing of this Act.

...

(11) Money laundering is an act which-
(a) constitutes an offence under section 139, 140 or 141;

(b) constitutes an attempt, conspiracy or incitement to commit an offence specified in paragraph (a);
(c) constitutes aiding, abetting, counselling or procuring the commission of an offence specified in paragraph (a); or

(d) would constitute an offence under paragraphs (a), (b) or (c) if done in the Island.

...

The money laundering offences are set out in sections 139, 140 and 141:

139 Concealing etc.

(1) A person commits an offence if that person –
(a) conceals criminal property;
(b) disguises criminal property;
(c) converts criminal property;
(d) transfer criminal property;
(e) removes criminal property from the Island.

...

140 Arrangements

(1) A person commits an offence if that person enters into or becomes concerned in an arrangement which the person knows or suspects facilitates (by whatever means) the acquisition, retention , use or control of criminal property by or on behalf of another person.

...

141 Acquisition, use and possession

(1) A person commits an offence if that person –
(a) acquires criminal property;
(b) uses criminal property;
(c) has possession of criminal property.

...

Please note that in relation to the offences under 139, 140 and 141, there is a de minimis threshold of £250 for deposit taking bodies only. This threshold provides a defence to a ML offence but does not remove the requirement to make an external disclosure.

In addition to the reportable offences above, relevant persons need to be aware of the offences detailed below surrounding non-reporting and tipping off. There are further offences in POCA such as prejudicing an investigation but these are not included in this guidance.

The terms ‘knowledge’, suspicion’ and ‘reasonable grounds’ and their meanings are explained under 7.6 of this Handbook.

142 Failure to disclose: regulated sector (and also see 143 Failure to disclose: nominated officers in the regulated sector and 144 Failure to disclose: other nominated officers)

(1) A person commits an offence if the conditions in subsections (2) to (5) are satisfied.

(2) The first condition is that the person –
(d) knows or suspects; or
(e) has reasonable grounds for knowing or suspecting.

that another person is engaged in money laundering.

(3) The second condition is that the information or other matter –
(a) on which the person's knowledge or suspicion is based; or
(b) which gives reasonable grounds for such knowledge or suspicion,

came to that person in the course of a business in the regulated sector.

(4) The third condition is –
(a) that the person can identify the other person mentioned in subsection (2) or the whereabouts of any of the laundered property; or
(b) that the person believes, or it is reasonable to expect the person to believe, that the information or other matter mentioned in subsection (3) will or may assist in identifying that other person or the whereabouts of any of the laundered property.

(5) The fourth condition is that the person does not make the required disclosures to –
(a) a nominated officer; or
(b) the FIU;

as soon as reasonably practicable after the information or other matter mentioned in subsection (3) comes to that person.

...

Please see section 7.5 for further detail on the reporting of suspicious activity.

145 Tipping off: regulated sector

(1) A person commits an offence if –
(a) the person discloses any matter within subsection (2);
(b) the disclosure is likely to prejudice any investigation that is or might be conducted following the disclosure referred to in that subsection; and

(c) the information on which the disclosure is based came to the person in the course of a business in the regulated sector.

(2) The matters are that the person or other person has made a disclosure under this part (Part 3 POCA 2008) –
(a) to the Financial Intelligence Unit; or
(b) to a nominated officer.

of information that came to that person in the course of business in the regulated sector.

(3) A person commits an offence if –
(a) the person discloses that an investigation into allegations that an offence under this part (Part 3 POCA 2008) has been committed, is being contemplated or is being carried out;
(b) the disclosure is likely to prejudice that investigation; and
(c) the information on which the disclosure is based came to the person in the course of business in the regulated sector.

...

Please see part 7.6 of this Handbook for further detail on tipping off.

7.4.2 Terrorist financing offences

The Anti-Terrorism and Crime Act 2003 ("ATCA") defines **'terrorism'** as:

1 Terrorism: interpretation

(1) In this act "terrorism" means the use or threat of action including outside the Island) where –
(a) the action falls within subsection (2),
(b) the use or threat is designed to influence the government or an international organisation or to intimidate the public or a section of the public, and
(c) the use or threat is made for the purpose of advancing a political, religious, racial or ideological cause.

(2) Action falls within this subsection if it –
(a) involves serious violence against person (wherever it is situated),
(b) involves serious damage to a property,
(c) endangers a person's life, other than that of the person committing the action,
(d) creates a serious risk to the health or safety of the public or a section of the public;
(e) is designed seriously to interfere with or seriously to disrupt an electronic system;
*(f) constitutes a **Convention offence***; or*
(g) would constitute a Convention offence if done in the Island.

...

*(5) In this Act reference to action taken for the purposes of terrorism includes a reference to action taken for the benefit of a **proscribed organisation*****

...

***A Convention Offence** is an offence listed in Schedule 13A to ATCA which includes:

- *Explosive offences*
- *Biological weapons*
- *Offences against internationally protected persons*
- *Hostage-taking*
- *Hijacking and other offences against aircraft*
- *Offences including nuclear material*
- *Offences relating to aviation and maritime security*
- *Offences involving chemical weapons*
- *Terrorist funds*
- *Directing a terrorist organisation*
- *Offences involving nuclear weapons*
- *Conspiracy etc.*

****A Proscribed Organisation** is a terrorist organisation as listed in Schedule 2 to the UK's Terrorism Act 2000 - http://www.legislation.gov.uk/ukpga/2000/11/schedule/2

ATCA defines **'terrorist property'** as:

6 Terrorist Property

(1) In this Act "terrorist property" means –
(a) money or other property which is likely to be used for the purpose of terrorism (including any resources of a proscribed organisation),
(b) proceeds of the commission of an act of terrorism, and
(c) proceeds of act carried out for the purpose of terrorism.

(2) In subsection (1) –
(a) a reference to proceeds of an act includes a reference to any property which is wholly or party, and directly or indirectly, represents the proceeds of the act (including payments or other rewards in connection with its commission), and
(b) the reference to the organisation's resources includes a reference to any money or other property which is applied or made available, or is to be applied or made available, for use by the organisation.

...

Note that the definition of terrorist property above includes property derived from acts of terror in addition to those used for the purpose of terrorism.

Property could be derived from terrorism, for example, through the payment of ransoms.

ATCA clarifies the activities that constitute FT and which need to be reported:

7 Fund raising

(1) A person commits an offence if he -

(a) invites another to provide money or other property, and

intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism.

(2) A person commits an offence if he –

(a) receives money or other property, and

(b) intends that it should be used, or has reasonable cause to suspect that it may or will be used for the purposes of terrorism.

(3) A person commits an offence if he –

(a) provides money or other property, and

(b) knows or has reasonable cause to suspect that it will or may be used for the purposes of terrorism.

...

8 Use and possession

(1) A person commits an offence if he uses money or other property for the purposes of terrorism.

(2) A person commits an offence if he –

(a) possesses money or other property, and

(b) intends that it should be used or has reasonable cause to suspect that it may be used, for the purposes of terrorism.

...

9 Facilitating funding

(1) A person commits an offence if –

(a) he or she facilitates money or other property being made available to another person; and

(b) he or she –

(i) knows;

(ii) has reasonable cause to suspect that; or

(iii) has failed to exercise due diligence or adequately investigate whether,

it will or may be used for the purposes of terrorism.

...

10 Money laundering

(1) A person commits an offence if he facilitates the retention or control of terrorist property –
(a) by concealment,
(aa) by disguise,
(ab) by conversion,
(b) by removal from the jurisdiction,
(c) by transfer to nominees, or
(d) in any other way.

...

In addition to the reportable offences above, relevant persons need to be aware of offences surrounding non-reporting and prejudicing an investigation (tipping off). See part 7.6.9 of the Handbook for further details.

14 Failure to disclose: regulated sector

(1) A person commits an offence if each of the following three conditions is satisfied.

(2) The first condition is that he –
(a) knows or suspects, or
(b) has reasonable grounds to knowing or suspecting,

that another person has committed an offence under section 7 to 10.

(3) The second condition is that the information or other matter –
(a) on which his knowledge or suspicion is base, or
(b) which gives reasonable grounds for such knowledge or suspicion,

came to him in the course of a business in the regulated sector.

(4) The third condition is that he does not disclose the information or other matter to the FIU or nominated officer as soon as is practicable after it comes to him.

...

27 Disclosure of information to prejudice terrorist investigations

(1) Subsection (2) applies where a person knows or has reasonable cause to suspect that a constable is conducting or proposes to conduct a terrorist investigation.

(2) The person commits an offence if he –
(a) discloses to another anything which is likely to prejudice the investigation, or
(b) interferes with material which is likely to be relevant to the investigation.

(3) Subsection (4) applies where a person knows or has reasonable cause to suspect that a disclosure has been or will be made...

(4) The person commits an offence if he –
(a) discloses to another anything which is likely to prejudice an investigation resulting from the disclosure..., or
(b) interferes with material which is likely to prejudice an investigation resulting from the disclosure.

...

This offence is equivalent to the "tipping off" offence relating to ML investigations. For ease of reference, this offence is also referred to as "tipping off" throughout this Handbook. The ATCA s27 offence also includes interfering with material which is likely to prejudice an investigation, there is an equivalent offence at section 160 of POCA 2008.

7.4.3 Proliferation of weapons of mass destruction offences

Anti-Terrorism and Crime Act 2003 ("ATCA") –

49B Use etc. of nuclear weapons

(1) A person commits an offence if the person –
...
(b) develops or produces, or participates in the development or production of, a nuclear weapon
...
(d) participates in the transfer of a nuclear weapon...
...

(3)For the purposes of subsection (1)(b) a person participates in the development or production of a nuclear weapon if he or she does any act which –
(a) facilitates the development by another of the capability to produce or use a nuclear weapon; or

(b) facilitates the making by another of a nuclear weapon,

knowing or having reason to believe that his or her act has (or will have) that effect.

(4) For the purpose of subsection (1)(d) a person participates in the transfer of a nuclear weapon if –
...
(c) he or she makes arrangements under which another person either acquires or disposes of it or agrees with a third person to do so.
...

49E Assisting or inducing certain weapons-related acts outside the Island

(1) A person who aids, abets, counsels or procures, or incites, a person to do a relevant act outside the Island is guilty of an offence.

(2) For this purpose a relevant act is an act that would constitute an offence under any of the following provisions –

(a) section 1 of the Biological Weapons Act 1974 (offences relating to biological agents and toxins) (of Parliament), as that Act has effect in the Island.

(b) section 2 of the Chemical Weapons Act 1996 (offences relating to chemical weapons) (of Parliament), as that Act has effect in the Island; or

(c) section 49B (use etc. of nuclear weapons)

...

7.4.4 Sanctions offences

The following are some of the offences and penalties provided in the Terrorism and Other Crime (Financial Restrictions) Act 2014 ("TOCFRA") for breaches of sanctions law relating to "designated person" (which includes those persons included on terrorism sanctions lists having effect in the Island). They may be regarded as indicative of typical offences and penalties provided for throughout sanctions legislation.

You should note, however, that unlawful acts relating to sanctions and individuals, entities, organisations, countries and territories subject to sanctions may also be breaches of export control law (see Notice 279 MAN), trade control law (see Notice 279T MAN), the Proceeds of Crime Act 2008 , the Anti-Terrorism and Crime Act 2003 or other provisions in criminal law.

–

3 Interpretation

...

*"**designated person**" means –*

(a) person designated by the Treasury for the purposes of Part 2 (including a designation that has effect by virtue of section 24(1));

(b) a natural or legal person, group or entity included in the list provided for by Article 2(3) of Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism as it has effect in the Island;

...

*"**direction**" means a direction given under section 6 (*final directions) *or section 7* (interim directions);

39 Contravention of requirement imposed by a direction

(1) A person who contravenes a requirement of a direction commits an offence, subject to the following provisions.

(2) No offence is committed if the person took all reasonable steps and exercised all due diligence to ensure that the requirement would be complied with.

...

40 Relevant person circumventing direction requirements: offence

(1) A relevant person who intentionally participates in activities knowing that the object or effect of them is (whether directly or indirectly) to circumvent a requirement of a direction commits an offence.

...

41 Offences in connection with licences

*(1) A person commits an offence if he or she, for the purposes of obtaining a licence under paragraph 7 of Schedule 1*** –*

(a) provides information that is false in a material respect or a document that is not what it purports to be; and

(b) knows that, or is reckless as to whether, the information is false or the document is not what it purports to be.

...

****Schedule 1;** Requirements of Directions.*

(7) Directions limiting or ceasing business; exemption by licence

44 Freezing of funds and economic resources

(1) A person ("P") must not deal with funds or economic resources owned, held or controlled by a designated person if P knows, or has reasonable cause to suspect, that P is dealing with such funds or economic resources.

(2) In subsection (1) "deal with" means –

(a) in relation to funds –

(i) use, alter, move, allow access to or transfer;

(ii) deal with the funds in any other way that would result in any change in volume, amount, location, ownership, possession, character or destination; or

(iii) in relation to economic resources, exchange or use in exchange for funds, goods or services.

(3) Subsection (1) is subject to sections 50 and 51 (exceptions and licences).

(4) Any person who contravenes the prohibition in subsection (1) commits an offence.

45 Making funds or financial services available to designated person

(1) A person ("P") must not make funds or financial services available (directly or indirectly) to a designated person if P knows, or has reasonable cause to suspect, that P is making the funds or financial services so available.

(2) Subsection (1) is subject to sections 50 and 51 (exceptions and licences).

(3) Any person who contravenes the prohibition in subsection (1) commits an offence.

48 Making funds or financial services available for benefit of designated person

(1) A person ("P") must not make funds or financial services available to any person for the benefit of a designated person if P knows, or has reasonable cause to suspect, that P is making the funds or financial services so available.

(2) For the purposes of this section –
(a) funds are made available for the benefit of a designated person only if that person thereby obtains, or is able to obtain, a significant financial benefit; and
(b) "financial benefit" includes the discharge of a financial obligation for which the designated person is wholly or partly responsible.(3) Subsection (1) is subject to sections 50 and 51 (exceptions and licences).

(4) Any person who contravenes the prohibition in subsection (1) commits an offence

47 Making economic resources available to designated person

(1) A person ("P") must not make economic resources available (directly or indirectly) to a designated person if P knows, or has reasonable cause to suspect –
(a) that P is making the economic resources so available; and
(b) that the designated person would be likely to exchange the economic resources, or use them in exchange, for funds, goods or services.

(2) Subsection (1) is subject to section 51 (licences).
(3) Any person who contravenes the prohibition in subsection (1) commits an offence.

48 Making economic resources available for the benefit of designated person

(1) A person ("P") must not make economic resources available to any person for the benefit of a designated person if P knows, or has reasonable cause to suspect, that P is making the economic resources so available.

(2) For the purposes of this section –
(a) economic resources are made available for the benefit of a designated person only if that person thereby obtains, or is able to obtain, a significant financial benefit; and
(b) "financial benefit" includes the discharge of a financial obligation for which the designated person is wholly or partly responsible.

(3) Subsection (1) is subject to section 51 (licences).
(4) Any person who contravenes the prohibition in subsection (1) commits an offence.

49 Circumventing prohibitions etc.

A person commits an offence who intentionally participates in activities knowing that the object or effect of them is (whether directly or indirectly) –
(a) to circumvent any of the prohibitions in sections 44 to 48; or
(b) to enable or facilitate the contravention of any such prohibition.

7.4.5 Other POCA & ATCA offences

Under both ATCA and POCA, a range of orders may be issued requesting a financial institution to assist with ML/FT investigations by producing customer and transaction information, documentation and monitoring accounts. Failure to comply with such an order would constitute an offence.

A freezing order may be issued where funds are suspected of being related to terrorism. The order may prevent the financial institution from allowing a person to withdraw from an account, honouring cheques, making payments etc. The freezing order must include the provision for the financial institution to request a licence to authorise a transaction. The order may include requirements relating to the disclosure of information. A person commits an offence if they fail to comply with the Order, if they engage in an activity that would facilitate another person to commit the aforementioned offence or if they fail to provide (or provide false) information or materials as requested by them to assist with an investigation following the freezing order.

7.5 Unusual Activity

7.5.1 Conducting "appropriate scrutiny" of unusual activity

Paragraph 27(2) of the Code requires the relevant person to conduct 'appropriate scrutiny' of any unusual activity and to obtain EDD. The activity should be looked at in detail in conjunction with additional information such as the customer's CDD, expected activity, an explanation of the activity from the customer, supporting documentary evidence or information from independent data sources. CDD provides the basis for recognising unusual activity therefore it is imperative that CDD is satisfactory on all customers and that business relationships are monitored appropriately.

The aim of conducting 'appropriate scrutiny' is to enable the relevant person to determine whether the activity is in fact suspicious and, if so, make a disclosure. If the activity is not deemed to be suspicious but still appears unusual or risky, the relevant person should consider other actions such as reviewing and updating the customer's risk assessment, arranging further ongoing monitoring or considering whether they have the risk appetite to continue doing business with the customer.

When conducting 'appropriate scrutiny', other connected customers, accounts or relationships may need to be examined. Connectivity can arise though commercial connections e.g. linked accounts, introducers etc. or through connected individuals e.g. third parties, controllers, signatories etc. The need to search for information concerning connected accounts or relationships should not delay making an external disclosure to the FIU.

The nature and scale of the scrutiny required will vary greatly depending on the type of activity, the risk factors involved and the size and scope of the activity. Regardless of the methods adopted, it is essential that the investigation and outcome are clearly documented. The consequences of failing to do so are summarised in part 7.7 of the Handbook.

The following are likely to cause suspicion after conducting appropriate scrutiny:

1. the customer is unable or refuses to provide a reasonable explanation for the activity and this is perceived as being an attempt to conceal criminal conduct rather than the customer being awkward, unhelpful or secretive for personal reasons;
2. the explanation does not "sit right" or does not make economic sense. For example a bank's customer sending repeat small amounts on a regular basis overseas despite transfer fees incurred with no reasonable explanation;
3. documentation supplied appears to be fraudulent, incomplete or doctored;
4. independent data sources reveal negative information on the customer or related parties such as allegations of corruption; or
5. activity appears consistent with known ML/FT typologies.

Please note that this is not an exhaustive list.

7.5.2 Appropriate scrutiny tips

Below are some tips that should be borne in mind when conducting 'appropriate scrutiny'

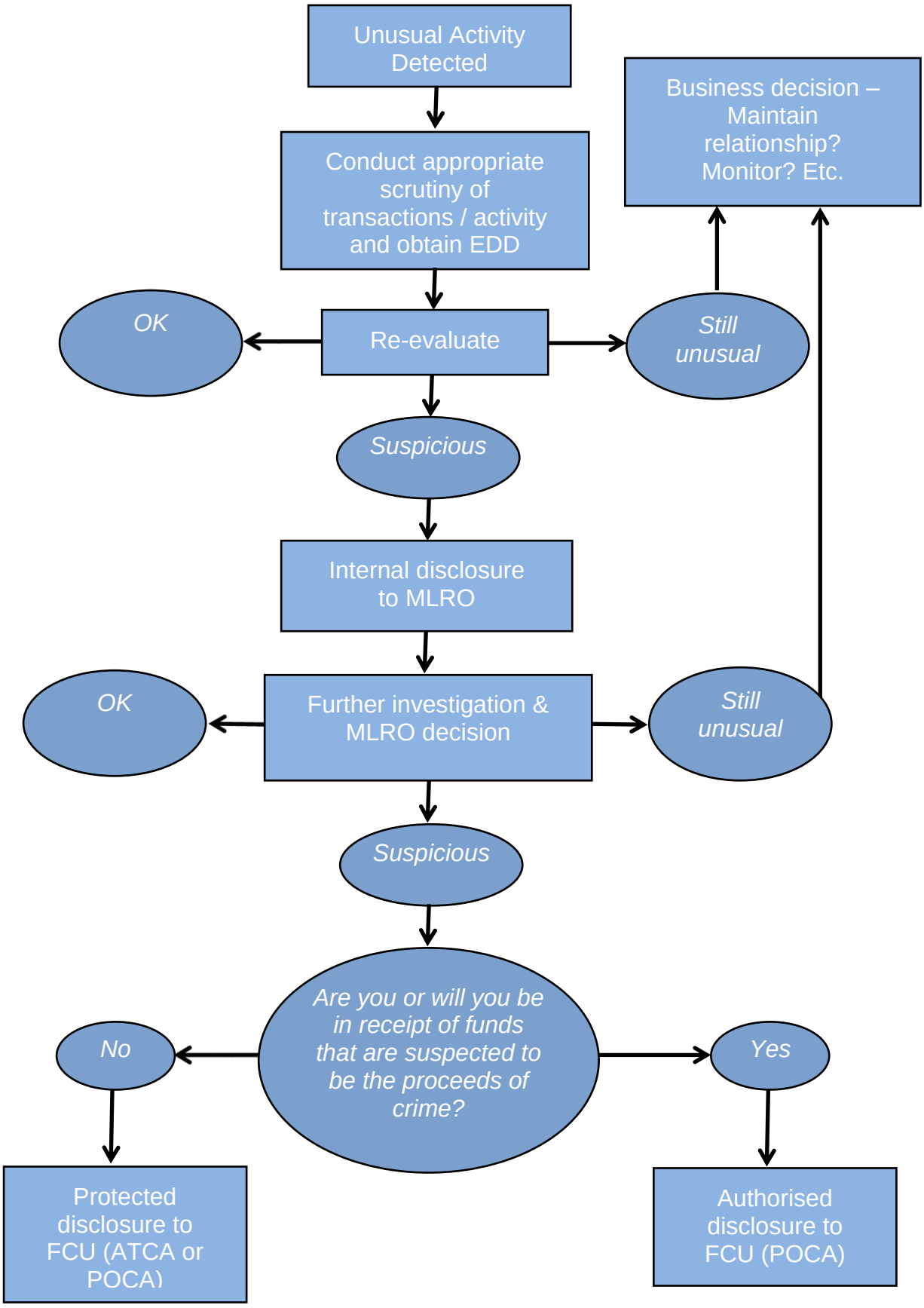
- Investigate until you feel comfortable with the activity or have sufficient information to submit a disclosure.
- Consider using a broad range of data sources – e.g. companies registers, address verification sites, social networks, news.
- Obtain an understanding of the relationships between the customer and any related parties.
- Find out if the customer is or was acting on behalf of another person. If so, who and why? (And carry out CDD in line with paragraph 13 of the Code)
- Compare the customer's explanation with publicly available information. For example, if a large credit supposedly relates to the sale of a house, consider checking the address and average prices in that area.
- Consider the information held against known typologies and high risk indicators - transaction type, customer background, location and currency.
- By checking the customer's historic activity you may be able to detect a pattern. For example a local business may always see a surge in cash deposits in June due to tourism.
- If requesting information or documentation from a customer, allow a reasonable timeframe for them to respond and communicate by phone, email, online messaging and fax wherever possible to expedite the process.
- If appropriate use this as an opportunity to gain a better understanding of what activity to expect going forward.

Ensure that any investigation is fully documented as details of this may have to be provided to competent authorities during their investigation if it progresses to that stage.

This could also be your defence to a charge of failing to report should you determine that there are not reasonable grounds to know or suspect.

And, if you do make an external disclosure and your customer takes civil action against you, this is your rationale for why you suspected.

7.5.3 Standard investigation process



7.5.4 Investigations and legal professional privilege

If a relevant person places reliance on a third party (using an appropriate Code concession) to identify / verify the identification of a customer but that third party is bound by legal professional privilege (or statutory secrecy laws) the relevant person must ensure that they are able to obtain upon request sufficient information or verification to satisfy the requirements of the Code to meet the conditions of the relevant concession (see Part 6 of this document for further details of the concessions).

In some cases restrictions such as legal professional privilege may still allow an entity bound by such restrictions to provide sufficient information to allow the relevant person to meet the requirements of the Code without breaching the restrictions. For example a lawyer (bound by legal professional privilege) providing a bank with customer due diligence in a pooled account or eligible introducer arrangement.

On occasion it is recognised that further information may need to be sought by the relevant person from the intermediary when investigating unusual activity as explained in this Handbook. If the third party cannot provide any further information due to legal professional privilege (or other restrictions), the relevant person should make an external disclosure in the normal manner highlighting in the disclosure that additional information may be held by the intermediary but cannot be disclosed to them due to certain restrictions.

7.6 Suspicious Activity

7.6.1 POCA & ATCA reporting requirements

Under POCA and ATCA, a relevant person has to make a disclosure where it knows or suspects ML/FT is attempted, or has taken place (sections 142/143 POCA / section 14 ATCA).

Failure to report knowledge, suspicion or where there should have been knowledge or suspicion (reasonable grounds/cause) is a criminal offence.

Please see part 7.7 of the Handbook for details on the potential consequences for failing to implement effective suspicious activity reporting procedures.

The reporting of a suspicion does not remove the need to report further suspicions that arise subsequently in respect of that customer. If other suspicious transactions occur, whether of the same nature or different to the previous suspicion, these new suspicions must continue to be reported to the MLRO/FIU as they arise. The requirement to report also covers situations where the business or transaction has not proceeded and there is a suspicion of ML/FT.

7.6.2 Suspicious activity reporting of declined business

If a relevant person turns away business that they know, or suspect might be, criminal in intent or origin a disclosure must be made to the FIU, albeit that no transaction or activity has taken place. Reporting of such events will allow the FIU to build a clearer picture of the ML/FT threat to the Island, and to use such intelligence on a proactive basis. A further benefit of reporting such declined business is that money launderers will perhaps be discouraged from trying to place criminal business on the Island in future.

7.6.3 Making an external disclosure

Since 1 May 2016 disclosures are required by the PROCEEDS OF CRIME (PRESCRIBED DISCLOSURES) ORDER 2015 to be made to the FIU using their online reporting facility. Their online system (Themis) can be accessed through the FIU website at http://www.fiu.im. MLROs will need to register in order to obtain a username for the system and application forms to do this are available on the FIU website, please see the web-page on Suspicious Activity Reports. (It should be noted that the FIU use Themis to issue communications.)

The FIU recognise that in exceptional circumstances, such as the sensitivity of the subject, a reporter may wish to submit a paper report and this is acceptable. However, businesses are advised to register at the earliest opportunity because not having an MLRO registered as a user or being disinclined to register for the online reporting facility is not viewed as exceptional circumstances.

Full contact details for the FIU are as follows:

Financial Intelligence Unit
PO Box 51
Douglas, Isle of Man, IM99 2TD
Tel: (01624) 686000 (office hours)
Email: fiu@gov.im

Relevant persons are encouraged to provide as much detail as possible. In cases where relevant persons inform the Authority of matters surrounding an imminent disclosure, it is not sufficient to merely state that the Authority has been informed, and nothing more. The relevant person may state that they have informed the Authority, but they must also provide full details of their knowledge or suspicion to the FIU. It is important to remember that the FIU and the Authority are different entities.

Failure to provide sufficient information to the FIU at the outset may hinder the commencement or progress of an investigation by the authorities, and, where consent has been sought to carry out a transaction, may result in a “consent letter” being initially withheld or delayed.

The FIU may go back to the relevant person to request further information or clarification in relation to the disclosure. Please note that if the relevant person fails to cooperate with a request for additional information the report may not be accepted as an authorised disclosure and action could be taken by the FIU against the relevant person.

Relevant persons that routinely send copies of any disclosures to their Head Office in the UK should note that where a disclosure contains any investigable information, regardless of whether there is a UK connection, the MLRO or nominated officer in the UK will be obliged under UK legislation to pass on to the National Crime Agency (NCA) any copy of the disclosure that he receives. It should be noted that the legal responsibility for reporting suspicious transactions in the Isle of Man to the FIU rests with the Isle of Man relevant person rather than with its Head Office.

7.6.4 Knowledge, suspicion and reasonable cause to know or suspect

Both POCA and ATCA have offences for failing to report:

(a) knowledge;
(b) suspicion; or
(c) reasonable grounds/cause for knowledge or suspicion

of money laundering/terrorist financing

Knowledge:

Knowledge of ML means that actual knowledge of ML/FT is possessed.

Suspicion:

Suspicion of ML/FT is a subjective test that a person applies. It is defined in case law* as something more than a fanciful possibility– it is more than a feeling of vague unease. The law does not require the suspicion to be 'clear', 'firmly grounded on targeted or specific facts' or 'based on reasonable grounds'. However it is important that concerns are justified by the existence of facts even if those facts do not prove ML is occurring. Typically suspicion will arise when something unusual is noticed and subsequent investigation continues to produce unusual or contradictory facts.

The case of R vs ML [2009] crim.952 proves that a ML conviction can occur even where there is no knowledge of a predicate offence that the property derived from. In this case, the suspicion was based on lifestyle assumptions. The defendant was found in possession of cash in excess of £20,000 which was not in line with his earnings or lifestyle and he was convicted due to the inference that the cash must have originated from criminal activity.

The Authority recommends that MLROs clearly document their evidence when considering whether to make a protected disclosure to the FIU. In this

way, if such a disclosure is not made, it is easy for the MLRO to evidence the logic behind the decision.

Further, as in cases such as Shah & Anor vs HSBC, this evidence may be required to defend against civil action from the customer who is the subject of an external disclosure.

*case law:
Da Silva (EWCA 1996)
Shah & Anor vs HSBC 2010
Commission for Corporate Affairs v Guardian Investments PTY Limited 1985
K Ltd vs Natwest Bank 2006
R vs ML [2009] crim.952

Reasonable grounds for knowledge/suspicion:

Reasonable grounds for knowledge of suspicion of ML/FT are facts which, if presented to a reasonable person (or a person working in the regulated sector), would suggest that ML/FT could be occurring. The test is included to prevent individuals from deliberately failing to investigate any concerns arising from the AML/CFT framework to the extent necessary and using the excuse “I wasn’t suspicious”.

The use of terms in the Proceeds of Crime Act:-

The Act uses the above terms explicitly in relation to reporting requirements, and also implies knowledge or suspicion as key criteria in certain clauses. It is important for relevant persons to understand when these terms apply.

Protected disclosures must be made whenever ML or attempted ML is known, suspected or there are reasonable grounds for knowing or suspecting it. In other words, the act of laundering must be reported under all possible circumstances.

Authorised disclosures are subject to a much tighter criteria. Section 154 of POCA defines an authorised disclosure as follows: “it is a disclosure...that property is criminal property.”

Criminal property is property which is the benefit of crime, where that property is known or suspected as such. Therefore any property which a relevant person knows or suspects represent the benefit of crime becomes criminal property, at which point it can be disclosed.

7.6.5 Protected disclosures

Section 153 of POCA mandates the reporting of ML by others using a “protected disclosure”.
Protected disclosures made to the FIU must satisfy a number of key tests:

(1) the report must be made to the FIU;;

(2) it should be made by the MLRO ("the nominated officer");
(3) the offence that has led to the assets being labelled as the proceeds of crime or terrorist property must be a criminal offence in the Isle of Man or an act committed elsewhere that would, if committed on the Island, be a crime;
(4) the information that suggests the assets are proceeds of crime must arise in the course of the relevant person's business; and
(5) the report must contain sufficient information to allow the criminal property, terrorist property or person to be identified.

Each instance of a report to the FIU must be preceded by a consideration of whether a reasonable suspicion or knowledge of ML/FT exists. This will ordinarily involve the MLRO considering the facts of the case and may require additional research and confirmation of the suspicion.

The FIU expects to see information included in each report which explains the reasons why suspicion or knowledge has been established. Similarly if an MLRO upon consideration concludes that a report need not be made, it is important that a record of the decision not to report is made along with the reasons why the report was not made.

7.6.6 Authorised disclosures – seeking consent

Sections 139 to 141 of POCA make it an offence to conceal, arrange, acquire, possess, use etc. known or suspected criminal property. It is difficult to see how a relevant person - once in possession of funds that are known or suspected to be criminal property – can avoid a charge of ML.

Section 154 of POCA therefore provides a reporting mechanism called "an authorised disclosure" a means by which a defence against ML can be obtained. Making an authorised disclosure can be used as the vehicle to seek consent to commit a prohibited act (i.e. possessing, acquiring, moving known or suspected criminal property).

Under the rules governing authorised disclosures, the discloser knows they are performing a prohibited act. This gives them the status of an alleged offender.

Depending on the timing of the transaction, the alleged offender has one of three opportunities to obtain a defence using criteria specified in section 154:

(a) if the ML has yet to take place, a notification prescribed by section 155 of POCA and seeking consent under 151 can be made;
(b) if the ML is in progress AND the alleged offender didn't know (or suspect) the property was criminal property when the transaction was started AND the alleged offender discloses of his/her own initiative, then a notification in the format prescribed in section 155 can be made and consent can be sought under section 151;
(c) if the ML has occurred AND the alleged offender has a reasonable excuse for performing the prohibited act AND the alleged offender

discloses of his/he own initiative then a notification in the format prescribed in section 155 and can be made and consent can be sought under section 151 .

When seeking consent, the relevant person should locate and tick the appropriate box on the disclosure form. On version 9 of the FIU form, this is located at the foot of page 1 with the question, "Is this request for appropriate consent as required by section 151 of The Proceeds of Crime Act 2008?"

7.6.7 Authorised disclosures – receiving consent

Consent can be obtained by anyone to perform a prohibited activity if:

(a) it is requested from a nominated officer (MLRO) and he/she gives consent (which is allowed to be given by the MLRO) provided either:
- an authorised disclosure has been made to the FIU with a request for consent and it has been given;
- an authorised disclosure has been made to the FIU with a request for consent and nothing further is heard from the FIU within 7 working days starting on the day following the disclosure;
- an authorised disclosure has been made to the FIU with a request for consent and it has been refused but 31 days have elapsed without further activity from the FIU);

(b) it is requested from FIU and he/she gives consent;

(c) an authorised disclosure has been made to the FIU and consent has not been refused within 7 working days (starting on the first working day after the disclosure was made); or

(d) an authorised disclosure has been made to the FIU and consent has been refused within 7 working days but no further action has been taken by the FIU in the 31 elapsed days following the refusal of consent (where the FIU's initial refusal is counted as day one).

Once consent has been obtained either directly from the FIU or by virtue of the expiry of either the 7 working day period (the notice period) or the 31 elapsed day period (the moratorium period), the relevant person may perform activity with the criminal property without committing an offence of ML.

Note that even if consent is obtained, it has no overriding effect on other crimes that may be committed if the property is processed. E.g. relevant persons would need to understand the law concerning their status as a potential constructive trustee, handling stolen goods where a theft had occurred to create criminal property, etc.

Please note that section 156(3) of POCA, states that the FIU may provide a threshold for consent. This means that in exceptional circumstances, rather than a simple "yes" or "no" to consent, a relevant person may be given consent for transactions meeting certain requirements or under a certain value limit.

7.6.8 The timing of disclosures

The timing of disclosures is specified three times in the law:

(a) in the case of a protected disclosure (reporting money laundering committed by another), as soon as practicable after the information or other matter comes to the discloser.
(b) in the case of authorised disclosures:

- in the case where the alleged laundering is occurring, as soon as practicable after the alleged offender first knows or suspects that the property that they are concealing, etc., arranging, acquiring etc. Is criminal property; or
- in the case where the alleged laundering has occurred, as soon as it is practicable for it to be made.

The law does not specify an absolute time limit before a disclosure is made. The timing of a disclosure is a subjective decision made by the MLRO or other person making the report. Relevant persons must make the submission a priority, whilst at the same time ensuring the disclosure itself is comprehensive and meaningful. The Authority offers the following guidance on what it deems to be “as soon as practicable” and what it deems to not be “as soon as practicable”:

(The column on the left provides examples of justifiable situations that may cause a delay in an external disclosure being made. The column on the right provides examples of situations that are not justifiable to cause a delay.

As soon as practicable	Not as soon as practicable
- Further information is being gathered to assist the FIU to identify a person or the whereabouts of criminal property. - The circumstances of suspicion are being investigated to determine whether they constitute grounds for disclosure. - The relevant person has received specific instructions from the FIU which must be processed before the disclosure is submitted. - Holidays and non-work days prevent the disclosure from being made. - Ongoing discussions with the FIU are determining the format of the disclosure. - Ongoing discussions with the FIU are determining whether a disclosure is justified. - The organisation is experiencing a disaster and systems are temporarily unavailable to the MLRO and deputies. - The MLRO and deputies are unavailable under extraordinary and unexpected circumstances. - A large number of cases where suspicious transactions may need to be processed has unexpectedly occurred and the relevant person's systems are gearing up to handle them. (The Authority would expect a dialogue between the relevant person and the FIU in this instance). - Legal advice is being sought on the correct procedure for complying with the AML/CFT requirements. - The FIU are unavailable to receive the disclosure.	- MLRO unavailable and no deputy appointed. - No MLRO or deputy available (for example, both persons on annual leave). - Confusion exists over the reporting requirements. - An investigation into whether a report should be made has stalled. - Workload is preventing reports from being made quickly enough and the relevant person is chronically understaffed. - All reports must be done manually and there is insufficient resource. - Internal sign-off by management is blocking reporting (note that relevant persons should ensure that MLROs are able to report directly to the FIU without interference from management). - The MLRO has multiple duties and other work is preventing access to the MLRO workload. - Preferred channel (say internet or electronic submission) not available and preference not to report until preferred channel becomes available again.

7.6.9 Tipping off

Tipping off occurs when a person working in the regulated sector (as defined in Schedule 4 to POCA) discloses that an investigation might be underway following a disclosure. The law is designed to apply to unscrupulous confederates of the money launderer or terrorist financier who find themselves in the reporting chain and relevant persons should therefore ensure their staff are sufficiently trained to avoid accidentally committing a tipping-off offence

Relevant persons who:

- are considering terminating their business relationship with a particular customer on the grounds of the risk that the customer represents; or
- who decline to enter a business relationship after a risk assessment has been conducted

need to understand if either of those actions are likely to constitute a tipping-off offence by referring to the criteria below. The same criteria apply to asking the customer for further information or documentation regarding any unusual activity.

In order to tip off, all three of the below criteria must be fulfilled:

- It must be revealed that either a disclosure in relation to ML/FT has been made or that an investigation relating to terrorist financing is being carried out or considered in relation to an alleged ML/FT offence;
- The information about the disclosure or investigation must be known as a result of undertaking business in the regulated sector; and
- The information that is passed to another is likely to prejudice an investigation that is being conducted or that might be conducted in future.

A relevant person is therefore faced with a simple question when communicating with customers in relation to unusual activity, terminating a business relationship or declining to enter into a business relationship:

> *Has a transaction or attempted transaction occurred which gives rise to the suspicion or knowledge of actual money laundering or terrorist financing?*

If the answer is 'no' then no disclosure to an MLRO or the FIU should have been made and it will therefore be impossible to commit an offence of tipping off.

If the answer is 'yes' then a report to the MLRO and possibly the FIU will need to be made, and in these cases, the relevant person will need to consider the following points when interacting with its customer:

- the ultimate decision on whether to engage in business with a customer lies with the relevant person. The FIU will never ask a relevant person to maintain a relationship with its customer as a vehicle to obtain intelligence;
- it will become apparent to criminals that something of their criminal activity is known to the relevant person if it begins to ask probing questions regarding certain activities or if it seeks to terminate the relationship or decline entering into a business relationship without a meaningful pretext. Relevant persons are therefore encouraged to consider carefully the wording of any statements they offer customers by way of explanation for their decision; and
- in order for a report to the FIU to be relevant, it must be possible from the report's information to identify criminal property or a person.

7.6.10 Refusing to carry out a transaction or declining a customer's business following a disclosure

As detailed in this Handbook, the relevant person commits a ML/FT offence it if handles funds that are known or suspected to be the proceeds of crime unless "consent" has either been received from the authorities or the 7/31 working day limits have passed with no response from the FIU.

The consent letter issued by the FIU following an authorised disclosure is provided to a relevant person as a defence against a charge of ML/FT. The consent letter issued by the FIU is not intended to override normal commercial judgement, and relevant persons are not obliged to continue relationships with customers if such action would place them at a commercial risk.

Relevant persons can reduce the potential threat of civil proceedings being instigated by customers suspected of ML/FT for breach of contract, by ensuring that the terms of business governing their customer relationships specifically exclude breaches in such circumstances whereby following a customer instruction may lead to the commission of a criminal offence.

7.6.11 Data protection law

Relevant persons are expected to adhere to Isle of Man data protection legislation. A relevant person should never fail to report for fear of breaching data protection law.

Section 31 of the Data Protection Act makes a specific exemption for disclosures authorised by other law; POCA creates a specific authorisation to disclose (provided the criteria for disclosure are adhered to) despite any other prohibitions on disclosure – irrespective of how they are imposed (including the Data Protection Act) and client confidentiality.

7.6.12 Managing a constructive trust scenario

A relevant person holding property that it knows or suspects, or has reasonable grounds to know or suspect does not belong to its customer may be regarded in law as a constructive trustee. In such situations legal advice should be taken by the relevant person.

7.6.13 Handling of suspicion in outsourced back office functions

The Authority is aware that many relevant persons conduct transactions on behalf of other entities either in other jurisdictions or the same jurisdiction e.g. back office work. When undertaking this type of work, relevant persons must bear in mind that they still have obligations placed upon them by the primary legislation as described in the Handbook, and also by the Code where the work undertaken constitutes business in the regulated sector (as set out in Schedule 4 to POCA).

Such back office functions may be for example the processing of account opening documentation or the establishment of legal persons, albeit that the account or client company may to be operated or administered by another entity in another jurisdiction. In such circumstances, the AML/CFT rules and regulations applicable to the processing of the application would be those of the other jurisdiction.

However, if during the processing of such an application or the establishment of a legal person, staff in the Isle of Man develop knowledge or suspicion of ML/FT (whether actual or attempted), a disclosure must be made locally on the Isle of Man in addition to any report made to the FIU (or Financial Intelligence Unit) of that other jurisdiction, this is known as dual-reporting.

In the event of a disclosure, relevant persons need to consider how they will handle the relationship with the other entity. While it is inevitable that suspicious transactions or suspicious attempted transactions do occur from time to time, frequent disclosures or disclosures that appear to highlight AML/CFT deficiencies by that other entity should be considered with a view to re-evaluating the business relationship with that other entity.

The relevant person may wish to inform the other entity of the disclosure, particularly where the other entity is part of the same corporate group. Whilst each relevant person must decide their own position on this point, they should approach such situations with caution, perhaps under legal advice and remain mindful of the “tipping off” offence.

Where a local disclosure results in a Production Order being served on the relevant person (or any other court order requiring action by relevant person) by a competent authority, the Production Order should be complied with in full and promptly. There should be no question of the person for whom the back office functions are being carried out having any say in the speed and thoroughness with which the relevant person complies with the Production Order.

7.7 Summary of the Consequences for Failing to Implement Effective Suspicious Activity Reporting Procedures

There is a broad range of potential consequences for failing to implement effective suspicious activity reporting procedures that apply to relevant persons and their directors, controllers and certain staff. The consequences below are in summary form only, for full details, please refer to the relevant legislation.

Code Breaches:

Offence	Summary conviction	Conviction on information
Code breach	Up to 12 months custody; Up to £5,000 fine; or Both	Up to 2 years custody; An unlimited fine; or Both

POCA/ATCA breaches:

For other offences such as those relating to information orders and freezing, please refer to the legislation.

Offence	Summary conviction	Conviction on information
Money laundering POCA 139, 140, 141 ATCA 10	Up to 6 months custody (up to 12 months for ATCA); Up to £5,000 fine; or Both	Up to 14 years custody; An unlimited fine; or Both
Terrorist financing ATCA 7, 8, 9	Up to 12 months custody; Up to £5,000 fine; or Both	Up to 14 years custody; An unlimited fine; or Both
Failure to disclose (regulated sector) POCA 142, 143 ATCA 14	Up to 6 months custody (up to 12 months for ATCA); Up to £5,000 fine; or Both	Up to 5 years custody; An unlimited fine; or Both
Tipping off POCA 145	Up to 3 months custody; Up to £5,000 fine; or Both	Up to 2 years custody; An unlimited fine; or Both
Prejudicing an investigation POCA 160	Up to 6 months custody; Up to £5,000 fine; or Both	Up to 5 years custody; An unlimited fine; or Both
Prejudicing an investigation (equivalent to POCA145) ATCA27	Up to 12 months custody; Up to £5,000 fine; or Both	Up to 5 years custody; An unlimited fine; or Both

Sanctions breaches:

As detailed in part 7.3.5 of the Handbook there are various types of sanctions. The offences and related consequences may vary. This table refers to the offences under the Terrorist and Other Crimes (Financial Restrictions) Act 2014 (“TOCFRA”), which primarily governs terrorism-related financial sanctions.

Offence	Summary conviction	Conviction on information
Dealing with funds or economic resources owned, 31 held or controlled by a designated person TOCFRA 44	Up to 12 months custody; Up to £5,000 fine; or Both	Up to 7 years custody; An unlimited fine; or Both
Making funds or financial services available to designated person TOCFRA 45	Up to 12 months custody; Up to £5,000 fine; or Both	Up to 7 years custody; An unlimited fine; or Both
Making funds or financial services available for benefit of designated person TOCFRA 46	Up to 12 months custody; Up to £5,000 fine; or Both	Up to 7 years custody; An unlimited fine; or Both
Making economic resources available to designated person TOCFRA 47	Up to 12 months custody; Up to £5,000 fine; or Both	Up to 7 years custody; An unlimited fine; or Both
Making economic resources available for benefit of designated person TOCFRA 48	Up to 12 months custody; Up to £5,000 fine; or Both	Up to 7 years custody; An unlimited fine; or Both
Intentionally participation in activities knowing that the object or effect of them is (whether directly or indirectly) to circumvent any prohibitions, or to enable or facilitate the contravention of any such prohibition relating to a designated person TOCFRA 49	Up to 12 months custody; Up to £5,000 fine; or Both	Up to 7 years custody; An unlimited fine; or Both
For the purpose of obtaining a licence, knowingly or recklessly, providing information that is false in a material respect, providing or producing a document that is not what it purports to be, or failing to comply with a condition of a licence TOCFRA 51	Up to 12 months custody; Up to £5,000 fine; or Both	Up to 2 years custody; An unlimited fine; or Both

For further detail, please refer to http://www.gov.im/categories/tax-vat-and-your-money/customs-and-excise/sanctions-and-export-control/

Proliferation of WMD breaches:

There are various proliferation related offences, please refer to the Terrorism and other Crime Financial Restrictions Act 2014.

Civil Litigation:

Relevant persons should be mindful of the threshold for making an external disclosure and avoid 'defence reporting' where no knowledge, suspicion or reasonable grounds exists. A customer who is the subject of a disclosure may take civil action against you if you have failed to comply with a transaction request and they have faced losses. See section 7.6.4 for further detail on knowledge and suspicion.

Financial Services Act 2008:

The Authority's General Licening Policy (which can be found here) details the Authority's "fit and proper" person criteria. The "fit and proper" criteria applies to all licence applicants and licenceholders, as well as persons acting or seeking to act as controller, director, or "key person". The "fit and proper" criteria cover integrity, competence and solvency, both on initial license application, or vetting, and on a continuous basis.

Serious or repeated breaches of legislation or codes of conduct in the Island, or in another jurisdiction by an applicant, its directors, key persons or controllers, will, prima facie, suggest a lack of competence and/or integrity.

There are a suite of remediation, disciplinary and enforcement tools available to the Authority under the FSA that could be used in cases where a relevant person has not complied with the AML/CFT requirements including:

- Individual:
    - Section 11 Warning notice
    - Section 10 Not fit and proper directions
    - Section 10A Prohibitions

Firm:

    - Fixed penalties
    - Directions
    - Licence conditions
    - Licence suspension
    - Skilled persons report
    - Public notice
    - Discretionary civil penalties
    - Manager appointments
    - Licence revocation
    - Prosecution

Designated Businesses (Registration and Oversight) Act 2015 ("DBRO"):

In relation to designated businesses the Authority's Designated Businesses Registration Policy details the Authority's "fit and proper" criteria. The "fit and proper" criteria applies to all designated business applicants and registered designated businesses. The "fit and proper" criteria cover the integrity and competence of the business, both on initial application and on a continuous basis.

Serious or repeated breaches of legislation or codes of conduct in the Island, or in another jurisdiction by an applicant, or its specified persons, will, prima facie, suggest a lack of integrity and/or competence.

There are a suite of remediation, disciplinary and enforcement tools available to the Authority under the DBRO Act that could be used in cases where a relevant person has not complied with the AML/CFT requirements including:

- Issuing a report stating action to be taken
- Injunction / remedial order
- Directions
- Civil penalties
- Public statement
- Revocation of registration
- Prosecution

Part 8 – Compliance

8.1 Monitoring

Paragraph 29 of the Code states that a relevant person must have appropriate procedures to monitor and test the implementation and operation of all AML/CFT procedures and controls. The nature and scale of this testing should be based on the business risk assessment undertaken in accordance with paragraph 6 of the Code. Any deficiencies should be remediated as soon as practicable. The effectiveness of training for appropriate staff should also be monitored and tested on a regular basis.

If appropriate, having regard to the risk of ML/FT and the size of the business, the board or senior management should commission a periodic report (the Authority would expect this to be at least annually) from the MLRO (or Compliance Officer if appointed). This report is to ensure that AML/CFT compliance is being undertaken to the required standards and should specify the details of the compliance of the relevant person with the Code.

The periodic report may include:

1. the means by which the effectiveness of the relevant person systems, controls and procedures have been managed and tested;
2. any significant compliance deficiencies identified and details of action taken or proposed to address any such deficiencies;
3. details of any failures to apply the Isle of Man AML/CFT requirements in branches and subsidiaries;

4. the number of internal disclosures to the MLRO and the number of subsequent external disclosures submitted to the FIU, any perceived deficiencies in internal or external reporting procedures, and the nature of changes proposed or implemented to address any such deficiencies;
5. information concerning the training programme for the preceding year, which staff have received training, the methods of training and the nature of the training;
6. changes made or proposed in respect of new legislation, regulatory requirements or guidance;
7. a risk assessment of any new types of product or service, or new distribution channels, and the proposed or implemented measures to counter ML/FT in line with paragraph 8 of the Code;
8. the nature of actions taken in response to notices highlighting jurisdictions which are the subject of international countermeasures, and the measures taken to manage and monitor business relationships connected with such jurisdictions or such jurisdictions that have been highlighted as posing a higher risk of ML/FT; and
9. any recommendations concerning additional resource requirements to ensure effective compliance with the relevant person's statutory and regulatory obligations.

8.2 Staff Appointments

Under paragraph 30 of the Code relevant persons must establish, maintain and operate appropriate procedures to enable them to satisfy themselves of the integrity of new directors, officers or partners and all new appropriate employees and workers. The extent of procedures undertaken should take into account the role of the employee and should be appropriate to the risk of ML/FT and the size of the business.

The terms "appropriate employees" and "workers" are not unique to high level staff such as MLROs, or Deputy MLRO's and Compliance Officers (where appointed), it may also include other members of staff such as customer facing staff where there are ML/FT risks.

In order to meet these requirements, relevant persons should where possible:

1. obtain and confirm references;
2. confirm employment history and the qualifications advised;
3. request details of any regulatory action taken against the individual (or the absence of such action); and
4. request details of any criminal convictions (or the absence of such convictions) and verify where possible.

Relevant persons should document the steps taken to satisfy these requirements including the information and confirmations obtained. Relevant persons should also document where it has not been possible to obtain such information including the reasons why this is the case.

8.3 Training

Successful AML/CFT strategies rely on effective communication of a relevant persons' policies and procedures to prevent and detect ML/FT. Communication of these policies and procedures and training in how to apply those procedures is key in ensuring compliance with the Code.

The guiding principle of all AML/CFT training should be to encourage employees, irrespective or seniority to understand and accept their responsibility to contribute to the protection of the business against the threat of ML/FT and what to do if such an event occurs.

8.3.1 Training requirements

Paragraph 31 of the Code requires relevant person to ensure that all directors, officers, or, as the case may be, partners, all other persons involved in its management, all key staff and appropriate employees and workers receive education and training in relation to:

(a) the provisions of the AML/CFT requirements;
(b) their personal obligations in relation to the AML/CFT requirements;
(c) the reporting procedures established under paragraph 26 of the Code;
(d) the relevant person's policies and procedures for AML/CFT;
(e) the relevant person's CDD, record-keeping and other procedures;
(f) the recognition and handling of transactions and attempted transactions that may give rise to an internal disclosure;
(g) their personal liability for failure to report information or suspicions in accordance with internal procedures, including the offence of tipping off; and
(h) new developments, including information on current techniques, methods and trends in ML/FT.

This training must be provided at least annually and it should be ensured the training being provided is up-to-date and keeps employees aware of AML/CFT developments. The effectiveness of training provided should be monitored.

Although it is not explicit in the Code, it is important to ensure that employees and staff have an appropriate level of knowledge regarding the relevant person's products and services, what their 'normal use' is and how they may be abused for the purposes of ML/FT.

Relevant persons should have a clear and well-articulated policy for ensuring that their appropriate employees are:

1. competent and have integrity;
2. aware of their personal obligations and liabilities under Part 3 of the Proceeds of Crime Act 2008, section 9 of the Prevention of Terrorism Act 1990, sections 7 to 11 and section 14 of the Anti-Terrorism and

Crime Act 2003, the Terrorism and Other Crimes (Financial Restrictions) Act 2014 and the Code;

3. aware of any new developments including current techniques, methods and trends in ML/FT; and
4. trained in the identification and reporting of anything that gives grounds for knowledge or suspicion or reasonable grounds to know or suspect that ML/FT is taking place, has taken place or is attempted.

Note that "Employee" and "Worker" are defined in the Code as:

> "**employee**" and "**worker**" of a relevant person, have the same meanings as in section 173 of the Employment Act 2006 and include an individual who —
>
> (a) works under a contract of employment or any other contract of service;
> (b) practises alone or with others under the terms of a partnership agreement;
> (c) is otherwise engaged within the business of a designated business, in all cases where the individual undertakes to do or perform, directly or indirectly, any work or service within a designated business, whether or not engaged directly by the designated business or through another entity forming part of the group of entities of which the designated business is a part, and the designated business is not by virtue of the contract a customer of the individual; or
> (d) is a director or officer.

8.3.2 Awareness of legislation and procedures

Employee awareness can be achieved and demonstrated in a number of ways and relevant persons should consider the following means of demonstrating and monitoring awareness:

1. providing employees with a document consolidating information outlining the relevant persons and their own obligations and potential criminal liability under AML/CFT legislation;
2. requiring employees to acknowledge that they have received and understood the information contained in the above document; and
3. providing relevant employees with a copy of the relevant persons' procedures for AML/CFT.

It would not normally be sufficient solely to provide employees with a copy of this guidance. One of the purposes of the Handbook is to enable relevant persons to design their own policies and procedures that are appropriate to their business taking into account the nature and size of the business.

8.3.3 New employees

Irrespective of seniority, the Authority would expect that training for all new employees who will be dealing with customers, client companies or their transactions should cover:

1. a general introduction to the background to ML/FT;
2. a clear indication of the importance placed on AML/CFT issues by the organisation;
3. the legal requirement to make disclosures and their personal legal obligations in this regard; and;
4. the procedures for reporting suspicious transactions to the MLRO.

The Authority expects that this training should be provided prior to them becoming actively involved in day-to-day operations.

8.3.4 Customer facing staff

Employees and workers such as cashiers, dealers, sales persons, company administrators etc., who deal directly with customers, are the first point of contact with potential money launderers or terrorist financiers. Their efforts are vital to an organisation's effectiveness in combating ML/FT at the new business stage, and as the business relationship progresses.

Employees and workers who are responsible for forming new customer relationships, opening new accounts, forming new client entities or dealing with new customers or occasional transactions should receive relevant training in:

1. the need to obtain satisfactory information and verification for all areas of CDD including documentary evidence of the customer's identity;
2. the identification of unusual activity and the scrutiny of this activity;
3. factors that may give rise to suspicions about a customer or client entity's activities;
4. their obligation to make disclosures even if the transaction, activity or business relationship does not proceed, in respect of both new and existing business relationships; and
5. the procedures to follow when a transaction, activity or attempted transaction or activity is considered to be suspicious.

Employees and workers should be vigilant when dealing with occasional customers or companies established for a single purpose, especially where large cash transactions or bearer securities are involved.

Employees and workers involved in processing deals or transactions should receive relevant training in:

1. CDD procedures;

2. recognising abnormal company activity, abnormal settlement, payment or delivery instructions, or any change in the normal pattern of business;
3. recognising unusual activity and the scrutiny of this activity;
4. the type of transactions or activity that require appropriate scrutiny and may need reporting to the relevant authorities regardless of whether the transaction was completed; and
5. the procedures to follow when a transaction, activity or attempted transaction or activity is considered to be suspicious.

8.3.5 Training for management

Employees and workers who are managerially responsible for handling customer transactions or business relationships should receive a higher level of training covering all aspects of AML/CFT procedures including:

1. offences and penalties arising from relevant primary legislation for non-reporting or for assisting money launderers or those involved in terrorist financing;
2. procedures for dealing with Production and Restraint Orders;
3. requirements for CDD including verification of identity and retention of records; and
4. in particular, the application of the relevant persons' risk-based strategy and procedures.

8.3.6 Training for Money Laundering Reporting Officers ("MLROs")

MLROs and their deputies should receive in depth training on all aspects of the prevention and detection of ML/FT including but not limited to:

1. AML/CFT legislative and regulatory requirements;
2. the international standards and requirements on which the Isle of Man strategy is based, namely the FATF 40 Recommendations and ML/FT typology reports that are relevant to their business;
3. the identification and management of ML/FT risk;
4. the design and implementation of internal systems of AML/CFT control;
5. the design and implementation of AML/CFT compliance testing and monitoring programs in accordance with paragraph 29 of the Code;
6. the identification and handling of suspicious activity and arrangements and suspicious attempted activity and arrangements;
7. the money laundering and terrorist financing vulnerabilities of relevant services and products;
8. the handling and validation of internal disclosures;
9. the process of submitting an external disclosure;
10. liaising with law enforcement;
11. money laundering and terrorist financing trends and typologies;
12. the risk of constructive trusteeship;
13. managing the risk of tipping off; and
14. the handling of Monitoring, Production and Restraint Orders.

The role of the MLRO is critical. The MLRO acts as the final arbiter on whether internal disclosures have substance and thus whether they should form the basis of external disclosures to the Isle of Man FIU. The MLRO also has an important record-keeping role and acts as the point of communication with the competent authorities in relation to investigations and information requests. MLRO training should therefore reflect the seriousness of the role. Please see part 7.7 of this Handbook for a summary of the consequences for failing to implement effective suspicious activity reporting.

8.4 Record Keeping

Record keeping is an essential component of the audit trail procedures that the Code and the Handbook seek to establish to ensure that tracing and confiscation of criminal and terrorist property can be made.

To comply with the requirements of the Code the records prepared and maintained by a relevant person should be such that:

1. the requirements of the Code have been met including:
    - documenting risk assessments conducted under Part 3 of the Code;
    - Obtaining CDD under Part 4 of the Code;
    - Documenting what action has been taken to scrutinise unusual activity;
    - Documenting any disclosures made under Part 7 of the Code;
    - Any corroborating information obtained to increase or mitigate risk(s); and;
    - The use of any concessions or exemptions in the Code (for example paragraph 10(4) of the Code which is the concession concerned with timing of CDD and Part 6 of the Code (simplified CDD)).
2. supervisors, auditors and law enforcement agencies will be able to assess the effectiveness of the AML/CFT policies and procedures that are maintained by a relevant person;
3. any transactions or instructions effected via the relevant person on behalf of any individual customer can be reconstructed;
4. the audit trail for funds entering and leaving the Isle of Man is clear and complete;
5. the details and records pertaining to any customer can be properly identified and located;
6. a CDD profile can be established for all customers for whom there is a business relationship;
7. all unusual activity reports received internally, and disclosures made externally, can be identified;
8. the rationale for not passing on any internal disclosures to the FIU can be understood;
9. a relevant person can satisfy, within a reasonable time frame, any enquiries or Court Orders from the appropriate authorities as to disclosure of information.; and;
10. disaster recovery procedures relating to retrieval of records must be established and periodically monitored.

8.4.1 Due diligence and transaction records

Paragraph 32(a) of the Code requires relevant persons to keep a copy of the documentation obtained during the CDD process. CDD records includes information that will be collected for each business relationship or occasional transaction under Part 4 of this Handbook and any customer files and business correspondence relating to the relationship or transaction.

Records relating to verification of identity must comprise the evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy. Where any reliance on third parties is used within the CDD process such as the EI concession the relevant person must ensure the introducers are aware of the record keeping requirements of the Code.

Paragraph 32(b) of the Code requires the relevant person to maintain a record containing details of all transactions carried out with or for a customer in the course of their regulated business activities.

In every case transaction records must contain:

1. details of the customer or counterparty, including account details;
2. the nature of the transaction; and
3. details of the transaction.

Relevant persons must ensure that a satisfactory audit trail can be established for AML/CFT purposes and that a financial profile of a customer, an account or client company can be established. To satisfy this requirement, the following additional information should be sought as appropriate, and transaction records retained of:

1. the volume of funds flowing through the account/turnover of client entity;
2. the origin of the funds;
3. the form in which the funds were offered or withdrawn, i.e. cash, cheque, etc.;
4. the identity of the person undertaking the transaction;
5. the destination of the funds;
6. the form of instruction and authority;
7. the name and address (or identification code) of the counter party; the security dealt in, including price and size;
8. whether the transaction was a purchase or a sale;
9. the account details from which the funds were paid (including, in the case of cheques, bank name, sort code, account number and name of account holder);
10. the form and destination of payment made by the business to the customer;

11. whether the investments were held in safe custody by the business or sent to the customer or to his/her order and, if so, to what name and address;
12. activities of the client entity; and
13. any large item/exception reports created in the course of transaction monitoring.

Paragraph 32(c) of the Code requires relevant persons to keep copies of other records as are sufficient to permit reconstruction of individual transactions and compliance with the code.

8.4.2 Electronically stored records

The Authority would have no objection to records being held electronically. The relevant person should ensure that working documents should be legible and in a usable filing system so that they can be found without undue delay and produced within 7 working days as required by paragraph 34 of the Code. This is especially important where the originals are not to be retained.

Where a relevant person chooses to implement an electronic storage system, an assessment of the risks must be undertaken in line with paragraph 8 of the Code and this should be factored into the business risk assessment undertaken under paragraph 6 of the Code. It is up to the individual business whether they determine it appropriate to retain the originals.

8.4.3 Retention of records

Paragraph 33 of the Code sets out the retention periods for records obtained. In order to comply with this paragraph of the Code:

- transaction records must be retained for at least five years from the date when all activities relating to the transaction were completed;

- CDD records must be retained for five years from the time of the occasional transaction or the end of the business relationship;

- where any reliance has been placed on a third party for elements of the CDD process, relevant persons must ensure that the third party is aware of the requirements under paragraphs 32 to 34 of the Code concerning record keeping;
- where an external disclosure has been made, or a relevant person knows or believes that a matter is under investigation, the relevant person must retain the records for as long as required by the constable or competent authority; and / or

- where a relevant person is aware that a request for information or an enquiry is being conducted by a competent authority, relevant persons must retain all relevant records for as long as required by that authority.

8.4.4 Training records

So that relevant persons can demonstrate that they have complied with the requirements of paragraph 31 of the Code concerning staff training, they must maintain documented records which should include:

1. details of the content of the training programmes provided;
2. the names of staff who have received the training;
3. the date on which the training was delivered; and
4. the results of any testing carried out to measure staff understanding of the anti-money laundering and counter terrorist financing requirements.

8.4.5 Format and retrieval of records

Paragraph 34(1) of the Code requires that any records required to be maintained and established under the Code must be capable of retrieval and the Code requires that –

(a) if the records are in the form of hard copies kept in the Island, they must be capable of retrieval without undue delay;
(b) if the records are in the form of hard copies kept outside the Island, they must be available within 7 working days; and
(c) in the case of other records (e.g. copies kept on a computer system), they must be readily accessible in or from the Island and capable of retrieval without undue delay.

Paragraph 34(2) of the Code permits a relevant person to rely on the records of a third party in respect of details of payments and transactions by customers, if it is satisfied that the third party will produce copies on request. Also, the third party must notify the relevant person if they are no longer able to comply with this requirement.

8.4.6 Responding to Production Orders

All relevant persons must be in a position to retrieve relevant information without undue delay in response to Production Orders etc. The timescale allowed for response will be specified in the Order.

Much reputational damage may be done to the Island if requests for international assistance, duly authorised by the Isle of Man Attorney General's Chambers, are not serviced within the time period specified in the notice.

Due to the importance the Isle of Man Government places on our international co-operation mechanisms, in circumstances of failure by a relevant person to comply with such notices, the Authority may consider that the relevant person is not complying with paragraph 34(1) of the Code which could impact upon the Authority's view of the relevant persons' fitness and propriety. This is in addition to any criminal offence for failure to comply.

8.5 Registers

Paragraph 35 and 36 of the Code require a relevant person to operate and maintain 3 registers:

(a) internal Disclosures – Paragraph 35 (1) (a) – see part 7.2.4 of this Handbook
(b) external Disclosures – Paragraph 35 (1) (b) – see part 7.2.5 of this Handbook
(c) ML and FT Enquiries – Paragraph 36 (1) – see part 7.2.7 of this Handbook

These registers must be readily accessible to Authority's officers as these will usually be examined during a supervisory visit.

The registers of internal and external disclosures may be contained in a single document if the details required to be included in them can be presented separately for internal disclosures and external disclosures upon request by a competent authority.

All three registers must be kept separate from other records.

Appendices I, J and K contain proforma registers which may be used as templates for this purpose.

Part 9 – Miscellaneous

9.1 Foreign Branches and Subsidiaries

A relevant person in the Isle of Man may have overseas branches, subsidiaries or associates. In such cases, control can be exercised over business conducted outside of the Isle of Man. Alternatively, elements of the Isle of Man regulated business may have been outsourced to other jurisdictions.

Paragraph 37(1) of the Code requires an Isle of Man relevant person to ensure that any branch or subsidiary in a jurisdiction outside the Island takes measures consistent with the Code and guidance (including the AML/CFT Handbook) in any branch or subsidiary outside the Island.

This is not intended to mean that the measures must mirror those of the Isle of Man in every detail, rather, that the measures should be of an equivalent or consistent standard to those in the Isle of Man. In such cases, a relevant person should consider establishing a group AML/CFT strategy to protect its global reputation as well as its Isle of Man business.

Where the law of the jurisdiction in which the branch is situated or the subsidiary is carrying on business, imposes requirements and procedures that are lower than those set by the Code and Handbook, the branch or subsidiary must apply the higher Isle of Man standard as explained in paragraph 37(2) of the Code. Reporting procedures and the offences to which the ML/FT legislation in the host country relates must be adhered to in accordance with local laws and procedures.

In accordance with paragraph 37(3) of the Code relevant persons must advise the Authority of any failure to apply the Isle of Man requirements in branches and subsidiaries, including where legislation in place in any host country prevents compliance that is at least in line with the Code. Additionally, where a host county prevents compliance that is at least in line with the Code relevant persons should apply appropriate additional measures to manage ML/TF risks. Relevant persons who have informed the Authority of such a failure should follow any advice, recommendations or directions the Authority or another competent authority provides as to the action to take.

9.2 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 38 of the Code, relevant persons must not enter into or continue relationships with shell banks. Relevant persons must also take adequate measures to ensure that they do not enter into or continue a relationship with a respondent institution that permits its accounts to be used by a shell bank.

9.3 Correspondent Services

Correspondent services are the provision of services (usually banking or Money Value Transfer Services ("MVTS")) by an institution in one jurisdiction (the correspondent) to another institution in another jurisdiction (the respondent). Used by institutions throughout the world, correspondent accounts enable banks and MVTS to conduct business and provide services that the institution does not offer directly.

Relevant persons must not enter into or continue correspondent relationships with shell banks (see above re shell banks). In addition, relevant persons must be satisfied that the respondent institutions with which they have a correspondent relationship do not permit their accounts to be used by shell banks.

Before entering into a business relationship or occasional transaction involving correspondent services or other similar arrangements, relevant persons must take steps additional to CDD requirements as per paragraph 39 of the Code as follows:

(a) obtain sufficient information about the respondent institution to understand fully the nature of its business;
(b) determine from publicly available information the respondent institution's reputation and quality of supervision including whether it has been subject of a ML/FT investigation or regulatory action;
(c) assess the respondent institution'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 relationships; and
(e) clearly understand and document the respective AML/CFT responsibilities of the relevant person and the respondent institution with respect to measures to prevent and detect ML/FT.

Where correspondent services involve a payable-through account, a relevant person must be satisfied that the respondent institution —

(a) has taken measures complying with the requirements of Recommendations 10 and 11 (CDD and record keeping) of the FATF Recommendations[14], with respect to every customer having direct access to the account; and

[14] The FATF requirements of Recommendations 10 and 11 are transpired in the AML/CFT Code at paragraphs 10-15 (customer due diligence), 32-34 (record keeping) and 40 (anonymous accounts).

(b) will provide relevant evidence of the customer's identity on request.

9.4 Fictitious, Anonymous and Numbered Accounts

As per paragraph 40 of the Code, relevant persons must not setup or maintain anonymous accounts, numbered accounts or accounts in fictitious names for any new or existing customers.

Where numbered accounts exist, relevant persons must maintain them in such a way that full compliance can be achieved with the Code, the FSRB and this Handbook. relevant persons must properly ID&V the customer in accordance with the Code and be able to demonstrate compliance when requested by a competent authority.

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.

Glossary & Acronyms

'Acceptable applicant' means a customer that satisfies the conditions of paragraph 20 (of the Code, as detailed in 6.3.2).

'Account' usually refers to bank accounts but should be read as including other similar business relationships between relevant persons and their customers.

'Agent' means any natural or legal person providing services to a customer on behalf of a regulated or designated person, whether by contract or under the direction of a regulated or designated person.

'Allowed business' is the customer of a regulated person using the 'acting on behalf of' concession and must meet the criteria of 21(6) of the Code as detailed in section 6.4.2.

'AML/CFT' means anti-money laundering and countering the financing of terrorism

'AML/CFT Code' means the Anti-Money Laundering and Countering the Financing of Terrorism Code 2015.

'AML/CFT requirements' has the same meaning as paragraph 3 of the Code.

'Appropriate scrutiny' is the term used to describe the scrutiny of unusual activity with the aim of determining whether the activity is in fact suspicious. Appropriate scrutiny will involve comparing the unusual activity to the customer's profile and expected activity and may require further investigation such as querying the source of funds or rationale for the activity with the customer as detailed in section 7.5.1.

'ATCA' means the Anti-Terrorism and Crime Act 2003.

'Authorised disclosure' means an external disclosure made under Section 154 of POCA as detailed in section 7.6.6.

'Bearer negotiable instruments' include money instruments in bearer negotiable form such as bearer instruments (including cheques, promissory notes and money orders) that are either in bearer form, are endorsed without restriction, are made out to a fictitious payee, or are otherwise in such form that title thereto passes upon delivery.

'Bearer shares' are negotiable instruments that accord ownership in a corporation to the person who is in physical possession of the bearer share certificate.

'Beneficial owner' has the same meaning as paragraph 3 of the Code (as detailed in section 4.3.4.

'beneficiary' ***(general)*** written with a lower case "b" means any person that receives benefit from something.

'Beneficiary' ***(of a trust)*** means a person who is or may be entitled to the benefit of a trust and includes fixed beneficiaries (who have a fixed entitlement) and discretionary beneficiaries (whose entitlement is at the discretion of the trustees).

'Blind trust' means a trust in which the executors have full discretion over the assets, and the trust beneficiaries have no knowledge of the holdings of the trust. Blind trusts are generally used when a trustee wishes to keep the beneficiary unaware of the specific assets in the trust, such as to avoid conflict of interest between the beneficiary and the investments.

'BNIs' means bearer negotiable instruments.

'Business relationship' has the same meaning as paragraph 3 of the Code.

'CDD' means customer due diligence.

'Certification' in relation to CDD means the process by which an employee or worker, or, a known and trusted member of the community confirms that a copy document is a true copy of the original. For identification documents, the certifier is also confirming that the document corresponds to the customer whose identity is being verified.

'Code' (the) means the Anti-Money Laundering and Countering the Financing of Terrorism Code 2015.

'Collective investment scheme' has the meaning given in section 1 of the Collective Investment Schemes Act 2008.

'Authority' (the) means the Financial Services Authority

'Competent authority' means all Isle of Man administrative and law enforcement authorities concerned with AML/CFT, including in particular the Financial Services Authority, the Isle of Man Gambling Supervision Commission, the Department of Home Affairs, the Financial Intelligence Unit, the Office of Fair Trading, the Attorney General, and the Customs and Excise and Income Tax Division of the Treasury.

'Concentration risk' means the probability of loss arising from heavily lopsided exposure to a particular group of counterparties.

'Confiscation' includes forfeiture where applicable and means the permanent deprivation of funds or other assets by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or administrative procedure that transfers the ownership of specified property to be transferred to the State. In this case the person(s) or entity(ies) that held an interest in the property at the time

of the confiscation or forfeiture loses all rights, in principle, to the confiscated or forfeited property. Confiscation or forfeiture orders are usually linked to a criminal conviction or a court decision whereby the confiscated or forfeited property is determined to have been derived from or intended for use in a violation of the law.

'Consent' means consent of a nominated officer or of a constable or customs officer as provided for under sections 151 and 152 of the Proceeds of Crime Act 2008.

'Constable' includes any officer appointed under section 1(2) of the Customs and Excise Management Act 1986.

'Constructive trust' means a relationship by which a person who has obtained title to property has an equitable duty to transfer it to another, to whom it rightfully belongs, on the basis that the acquisition or retention of it is wrongful and would unjustly enrich the person if he or she were allowed to retain it.

'Correspondent services' means banking, money or value transfer services and other similar relationships provided by a financial institution in one jurisdiction ("the correspondent institution") to a financial institution in another jurisdiction ("the respondent institution").

'Co-trustee' means a trustee of a trust when there is more than one trustee serving at the same time, usually with the same powers and obligations. Occasionally a co-trustee may be a temporary fill-in, as when the original trustee is ill but recovers. The co-trustee must act in consultation with the other trustee(s), unless the language of the trust allows one co-trustee to act alone.

'Country' all references in the FATF Recommendations to country or countries apply equally to territories or jurisdictions.

'Criminal conduct' is conduct which –

(a) constitutes an offence in the Island; or
(b) would constitute an offence in the Island if it occurred there.

'Currency' would usually mean a system of money in general use in a particular country but for the purposes of the Code and Handbook, this also includes virtual currencies.

'Customer' has the same meaning as paragraph 3 of the Code.

'Customer due diligence' encompasses KYC but it goes further than knowing who your customer is. It involves obtaining, documenting and using a broad range of information relating to a customer relationship or an occasional transaction. Areas to be considered include identity, address, source of funds and expected business or transactional activity. Certain elements of this information must also be verified. The term CDD also incorporates the ongoing monitoring of a business relationship, including the due diligence information obtained, to ensure it remains up to date and that the relationship is operating as expected for that customer. CDD is required for all new or continuing business relationships or occasional transactions.

'Designated non-financial businesses and professions' or **'designated businesses'** means relevant persons that are subject to oversight for compliance with the AML/CFT requirements by Financial Services Authority or the Isle of Man Gambling Supervision Commission or one of its delegates, apart from regulated persons.

'De-risking' refers to the phenomenon of financial institutions terminating or restricting business relationships with customers or categories of customers to avoid, rather than manage, risk in line with the FATF's risk-based approach. De-risking can be the result of various drivers, such as concerns about profitability, prudential requirements, anxiety after the global financial crisis, and reputational risk. It is a misconception to characterise de-risking exclusively as an anti-money laundering issue.

'DHA' means the Department of Home Affairs.

'Director' and **'Officer'** have the same meaning as paragraph 3 of the Code.

'DMLRO' means Deputy Money Laundering Reporting Officer.

'DNFBP' means designated non-financial businesses and professions.

'Document' includes information recorded in any form and, in relation to information recorded otherwise than in legible form, references to its production include references to produce a copy of the information in legible form.

'Domestic PEP' means a natural person who is or has been entrusted with prominent public functions in the Isle of Man and any family members or close associates of that person, regardless of the location of those family members or close associates.

'Dummy settlor(s)' may be used in an attempt to disguise the identity of the real settlor. This person would usually be a friend or a relative of the real settlor and his would be the name which appeared on the face of the trust deed as 'the original settlor', the person who initially established the trust. The only requirement was that the dummy settlor provided the original trust fund which was usually a nominal amount, thus perfecting the requirement of certainty of subject. The recitals would state that other assets would be later transferred to the trustees. In this way, the real settlor could add whatever assets he chose, without disclosing his identity. It would also be possible for the real settlor to be appointed as the protector. The illusion of the dummy settlor also allowed the real settlor to be recommended to the trustees in the settlor's Letter of Wishes. This would allow the real settlor to retain some element of influence over the trustees, something which the settlor was not supposed to be able to do.

'EDD' means enhanced due diligence.

'EIC' means eligible introducer's certificate.

'Eligible introducer' means an introducer that satisfies the conditions of paragraph 23 (of the Code, as detailed in 6.2.2). The Code allows the relevant person to place reliance on the introducer to have verified the customer's identity provided certain criteria are met. The introducer does not have to produce the verification documents to the relevant person. The relevant person must still obtain identity information regarding the identity of the customer and the beneficial owner which can be obtained from the introducer.

'Employee' and 'Worker' have the same meaning as paragraph 3 of the Code.

'Enhanced due diligence' goes further than obtaining CDD. This involves considering whether additional identification information needs to be obtained, considering whether additional verification of identity is required, taking reasonable measures to establish source of wealth (in addition to source of funds) of the customer and beneficial owner and considering what ongoing monitoring of this information should be undertaken. EDD is to be undertaken when a new business relationship, occasional transaction, or a continuing business relationship is assessed as posing a high risk of ML/FT, or when unusual activity is identified. When a suspicious activity is detected EDD should be considered.

'Enhanced monitoring' means examining all aspects of the business relationship including the CDD / any EDD obtained and the customer's activity. It should also focus on any changes in transactional activity or transactional activity that is not in line with the customer's expected activity, these transactions should be scrutinised more thoroughly. Appropriate screening for negative press should also be undertaken. The Code requires that enhanced monitoring is undertaken of the business relationship in relation to any foreign PEP, and higher risk domestic PEPs.

'Established business relationship' means a business relationship formed by a relevant person where that person has obtained, or is required to obtain, under procedures established, maintained and operated in accordance with this Code, satisfactory evidence of identity of the person who, in relation to the formation of that business relationship, was the customer.

'European Economic Area' unites the EU Member States and the three EEA EFTA States (Iceland, Liechtenstein, and Norway) into an Internal Market governed by the same basic rules. These rules aim to enable goods, services, capital, and persons to move freely about the EEA in an open and competitive environment, a concept referred to as the four freedoms. For further information, refer to http://www.efta.int/eea/eea-agreement.

'Exempted occasional transaction' has the same meaning as paragraph 3 of the Code.

'External disclosure' means a report made under paragraphs 26(1)(f) and 28 (of the Code, as detailed in 7.2.5).

'External regulated business' means business outside the Island that is regulated or supervised for AML/CFT purposes by an authority (whether a governmental or professional body and whether in the Island or elsewhere) empowered (whether by law or by the rules of the body) to regulate or supervise such business for such purposes.

'FATF Recommendations' means the 40 Recommendations set out in the Financial Action Task Force ("FATF") document 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation', adopted by the FATF in February 2012.

'FIU' the Isle of Man Financial Intelligence Unit.

'Financial institution' is a term used frequently by the FATF in their Recommendations and typology reports. In this Handbook, a financial institution has the same meaning as a 'regulated person'.

'Financing of Terrorism' includes the financing of proliferation and is to be construed in accordance with the definitions of 'financing', 'terrorism' and 'proliferation' in Section 3 of the Terrorism and Other Crime (Financial Restrictions) Act 2014.

'Fit and proper' refers to the initial and ongoing test of a business or individual's fitness and propriety in relation to carrying out a regulated activity.

'Foreign PEP' means a natural person who is or has been entrusted with prominent public functions outside the Isle of Man and any family members or close associates of that person, regardless of the location of those family members or close associates.

'Forfeiture' see 'confiscation'.

'Foundation' means a foundation established under the Foundations Act 2011 or a foundation or similar entity established under the law of another jurisdiction.

'FSA' means the Financial Services Act 2008.

'FSRB' means the Financial Services Rule Book.

'GSC' means the Isle of Man Gambling Supervision Commission.

'ID & V' refers to establishing a customer's identity and verifying that customer's identity. Identity includes; name, address, date of birth, nationality, place of birth, gender, a personal identification number and any other identification information relating to any underlying customers or persons purporting to act on behalf of the customer. Verification refers to the verification of elements of the identification information by using independent reliable sources, such sources may be obtained from the customer such as a passport to verify the customer's name.

'IMF' means the International Monetary Fund.

'Independent source' is a source that has no vested interest in a certain matter and is therefore expected to describe the matter from a disinterested perspective.

'Information' includes data.

'Internal disclosure' means a report made under paragraphs 26(1)(c) and 27 (of the Code, as detailed in 7.2.4).

'Introducer' means a third party that introduces a customer to a relevant person having no further involvement in the business relationship between the relevant person and the customer except providing the relevant person with CDD information and documentation for that customer.

'IOMPO' means the Isle of Man Post Office.

'Key person' is defined in the FSA and includes individuals with significant powers or responsibilities in an IOMFSA Licenceholder. For the purposes of the Handbook, a key person is a person that has significant powers and responsibilities within any business in the regulated sector regardless of their status as a regulated business or designated business.

'KYC' is short for "know your customer" and is the term used to describe the process of obtaining, retaining and using information about a customer to verify that they are who they say they are.

'Legal arrangement' means —

(a) an express trust; or
(b) any other arrangement that has a similar legal effect (such as a fiducie, Treuhand or fideicomiso).

'Legal person' includes any body corporate or unincorporate capable of establishing a customer relationship with a financial institution or of owning property.

'List A' is a list maintained by the Department of Home Affairs on its website specifying jurisdictions regarding which the FATF (or a FATF-style regional body) has made a call on its members and other jurisdictions to apply countermeasures to protect the international financial system from the on-going and substantial risks of ML/FT emanating from the jurisdiction (as detailed in section 3.5).

'List B' is a list maintained by the Department of Home Affairs on its website specifying jurisdictions with strategic AML/CFT deficiencies or those considered to pose a higher risk of ML/FT (as detailed in section 3.5).

'List C' is a list maintained by the Department of Home Affairs on its website specifying jurisdictions which are considered to operate CDD and record keeping requirements under their AML/CFT legislation at least equivalent to those of the Isle of Man (as detailed in section 3.5).

'Mitigation' is the term given to determining the necessary controls or procedures that need to be in place in relation to a particular part of the business in order to reduce the risk identified.

'ML' means money laundering.

'ML/FT' means money laundering and financing of terrorism, or both, and includes attempted transactions in relation to ML/FT.

'MLRO' means Money Laundering Reporting Officer.

'Money laundering' means an act that falls within section 158(11) of the Proceeds of Crime Act 2008 (as detailed in section 7.3.1 and 7.4.1).

'Money laundering reporting officer' means an individual appointed under paragraph 25 and includes a deputy MLRO appointed under paragraph 25(3) (of the Code).

'MONEYVAL' means the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism.

'MVTS' means money/value transfer services.

'NCA' means the UK's National Crime Agency.

'Nominated officer' means the natural person that has been appointed as the person who may receive internal disclosures from colleagues. In the case of a regulated or designated business, this would be the MLRO.

'Nominee shareholder' means the ostensible or registered owner who holds shares (stock) on behalf of the actual owner (beneficial owner) under a custodial agreement.

'Nominee company' means a wholly owned subsidiary that complies with paragraphs 2.7 or 3.1 of Schedule 1 to the Financial Services (Exemptions) Regulations 2011 or similar legislation in a jurisdiction in List C.

'Non-eligible introducer' means any person who introduces a customer to a relevant person other than an eligible introducer as defined above. Where customers are introduced to relevant persons via non-eligible introducers, the relevant person must identify and verify the identity of the customer themselves. However, the relevant person may request non-eligible introducers to obtain documentation from the applicant and pass it to them. However, the relevant person cannot rely on the non-eligible introducer to have verified the information or documentation. The introducer essentially acts as a facilitator between the relevant person and the customer.

'Non-profit organisation' means a body corporate or other legal person, the trustees of a trust, a partnership, other unincorporated association or organisation or any equivalent or similar structure or arrangement, established solely or primarily to raise or distribute funds for charitable, religious, cultural, educational, political, social or fraternal purposes with the intention of benefiting the public or a section of the public.

'NPO' means a non-profit organisation.

'Occasional transaction' means any transaction (whether a single transaction or series of linked transactions) other than a transaction carried out in the course of an established business relationship formed by a relevant person.

'Ongoing monitoring' is the term used to describe monitoring the conduct and activities of any business relationship, this covers the entire relationship including information held and transactions undertaken by the customer, as detailed in section 3.4.

'Payable-through account' means an account maintained by a correspondent institution that may be operated directly by a customer of the respondent institution.

'PEP' means politically exposed person.

'Person' includes any body of persons, corporate or unincorporated.

'POCA' means the Proceeds of Crime Act 2008.

'Politically exposed person' has the same meaning as paragraph 3 of the Code, as detailed in section 4.16

'Pooled client accounts' exist where funds belonging to more than one person are combined in a single account owned or controlled by a relevant person or their customer. Examples include —

(a) an advocate holding an account for funds to purchase a property;
(b) CSP holding funds as an advance against fees or registry fees; or
(c) e-gaming business holding players funds.

'Proceeds of crime' has the same meaning as criminal property.

'Production order' is the legal term for using powers under POCA/ATCA (or other legislation including Police Powers and Procedures Act 1998) to require the custodian of documents to deliver or make available the documents to persons such as law enforcement officials within a specified period.

'Proliferation' means the proliferation of weapons of mass destruction and its financing.

'Protected disclosure' means an external disclosure made under Section 153 of POCA as detailed in section 7.6.5.

'Protector' means a person or group of people (not the settlor, beneficiary, or trustee) who are appointed to exercise one or more powers affecting a trust and the interest of the beneficiaries. The concept of a trust protector is to protect beneficiaries from a rogue trustee.

'Reasonable measures' means appropriate measures which are commensurate with the money laundering or terrorist financing risks.

'Recognised stock exchange' - 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 ("MiFID"). For entities listed outside Europe, this means regulated markets subject to disclosure requirements consistent with MiFID. For example, in the context of the London Stock Exchange, this would include the Main Market but would not include the Alternative Investment Market.

'Regulated person' means —

(a) any person holding a financial services licence issued under section 7 of the Financial Services Act 2008;
(b) any person authorised under section 8 the Insurance Act 2008;
(c) any person registered under section 25 of the Insurance Act 2008;
(d) a retirement benefits schemes administrator registered under section 36 of the Retirement Benefits Schemes Act 2000; or
(e) a person holding an online gambling licence issued under section 4 of the Online Gambling Regulation Act 2001.

'Regulated sector' means a business activity listed in Schedule 4 to POCA.

'Relevant person' means a person carrying on a business in the regulated sector.

'Restraint order' is an order made under POCA which has the effect of freezing the assets and bank accounts of the persons against whom it is directed, in consequence of a belief by the authorities the assets concerned represent in whole or in part the proceeds of crime

'Risk' - all references to risk refer to the risk of money laundering and terrorist financing unless otherwise specified. Risk is the general term to describe threat, likelihood and consequence.

'S.NPO' means a specified non-profit organisation.

'Sanctions' is the term use to collectively describe —

(a) targeted financial sanctions;
(b) economic sanctions;
(c) currency and exchange controls;
(d) arms embargoes;
(e) prohibitions;

(f) dual-use item controls;
(g) import and export embargoes; and/or
(h) visa and travel bans.

'SAR' means suspicious activity report.

'Senior management' means the directors or key persons who are nominated to ensure that the relevant person is effectively controlled on a day-to-day basis and who have responsibility for overseeing the relevant person's proper conduct.

'Settlor' in relation to a trust means and includes each and every person who, directly or indirectly, on behalf of himself or on behalf of any other or others, as owner or as the holder of a power in that behalf, makes a disposition of property to be held in such trust or declares or otherwise creates such trust, and includes a person who assigns property to a trust.

'Shell bank' means a bank that is —

(a) incorporated in a jurisdiction in which it has no physical presence; and
(b) not affiliated with a financial services group that is subject to effective consolidated supervision.

'Signatory' is a natural person who signs a document and is subject to it. Reference to signatories in the Handbook means a person with signing authority over the affairs of a customer unless otherwise stated.

'Source of funds' includes the immediate source of funds from which property has derived e.g. a bank account in the name of Mr X.

'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.

'Specified non-profit organisation' means a non-profit organisation which has —

(a) an annual or anticipated annual income of £5,000 or more; and
(b) remitted, or is anticipated to remit, at least 30% of its income in any one financial year to one or more ultimate recipients in or from one or more higher risk jurisdictions.

'STR' means suspicious transaction report.

'Subsidiary' means a company whose voting stock is more than 50% controlled by another company, usually referred to as the parent company or holding company. A subsidiary is a company that is partly or completely owned by another company that holds a controlling interest in the subsidiary company.

'Suspicious activity' means any activity or information received in the course of a business relationship, occasional transaction or attempted transaction that causes the relevant person to —

(a) know or suspect; or
(b) have reasonable grounds for knowing or suspecting, that the activity or information is related to money laundering or the financing of terrorism.

'Tamper resistant format' is the term used to describe a type of electronic file that is of low risk of being tampered with, for example an image file with a time and date stamp is much more secure than a Microsoft word document.

'Terrorism' has the same meaning as Section 1 of ATCA, as detailed in section 7.4.2.

'Terrorist property' has the same meaning as Section 6 of ATCA, as detailed in section 7.4.2.

'FT' means financing.

'Tipping off' has the same meaning as 145 of POCA and 27 of ATCA, as detailed in section 7.6.9.

'Trusted person' has the same meaning as paragraph 3 of the Code.

'Trustee' means a person or firm that holds or administers property or assets for the benefit of a third party. A trustee may be appointed for a wide variety of purposes, such as in the case of bankruptcy, for a charity, a trust fund or for certain types of retirement plans or pensions. They are trusted to make decisions in the beneficiary's best interests.

'Underlying client' is the name given to the person on whose behalf a customer may be acting.

'Unusual activity' means any activity or information received in the course of a business relationship, occasional transaction or attempted transaction where —

(a) there are transactions that have no apparent economic or lawful purpose, examples of which include transactions that are —
    (i) complex;
    (ii) both large and unusual; or
    (iii) of an unusual pattern;

(b) the relevant person becomes aware of anything that causes the relevant person to doubt the identity of a person it is obliged to identify under this Code.
(c) the relevant person becomes aware of anything that causes the relevant person to doubt the good faith of a customer, beneficial owner, beneficiary or introducer.

'Virtual currency' means convertible virtual currencies such as crypto-currencies or similar concepts where the concept is accepted by persons as a means of payment for goods or services, a unit of account, a store of value or a commodity.

'Weapons of mass destruction' is a term used frequently by the FATF in their Recommendations and typology reports. In this Handbook, weapons of mass destruction has the same meaning of Section VIA of ATCA, as detailed in section 7.3.4 and 7.4.3.

'WMD' means weapons of mass destruction.

Appendix A

Anti-Money Laundering and Countering the Financing of Terrorism Code 2015[1]

ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM CODE 2015

Index

[1] Please note that this piece of secondary legislation has not yet been updated to take account of the creation of the Financial Intelligence Unit as a result of the FIU Act 2016. Where in this Code it states Financial Crime Unit this should be read as Financial Intelligence Unit and references to a constable serving in the Financial Crime Unit should read Financial Intelligence Unit.

Statutory Document No. 2015/0102

Proceeds of Crime Act 2008,
Terrorism and Other Crime (Financial Restrictions) Act 2014

ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM CODE 2015

Laid before Tynwald: 17 March 2015
Coming into Operation: 1 April 2015

The Department of Home Affairs makes the following Code under section 157 of the Proceeds of Crime Act 2008[2] and section 68 of the Terrorism and Other Crime (Financial Restrictions) Act 2014[3] after consulting such persons and bodies that appeared to it to be appropriate[4].

PART 1 – INTRODUCTORY

1 Title

This Code is the Anti-Money Laundering and Countering the Financing of Terrorism Code 2015.

2 Commencement

This Code comes into operation on 1 April 2015.

3 Interpretation

(1) In this Code —

"acceptable applicant" means a customer that satisfies the conditions of paragraph 20;

"AML/CFT" means anti-money laundering and countering the financing of terrorism;

[2] AT 13 of 2008
[3] AT 13 of 2014
[4] As required by section 157(4) of the *Proceeds of Crime Act 2008* and section 68(4) of the *Terrorism and Other Crime (Financial Restrictions) Act 2014*

"AML/CFT requirements" means the requirements of the following enactments —

(a) section 9 of the *Prevention of Terrorism Act 1990*[5] ;

(b) sections 7 to 11 and section 14 of the *Anti-Terrorism and Crime Act 2003*[6] ;

(c) part 3 of the *Proceeds of Crime Act 2008*;

(d) parts 2, 3 and 4 of the *Terrorism and Other Crime (Financial Restrictions) Act 2014*;

(e) this Code,

and includes, in the case of anything done otherwise than in the Island, anything that would constitute a requirement under the enactments specified in (a) to (d) if done in the Island;

"beneficial owner" means the natural person who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted and includes but is not restricted to —

(a) in the case of a legal person other than a company whose securities are listed on a recognised stock exchange, a natural person who ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings) 25% or more of the shares or voting rights in the legal person;

(b) in the case of any legal person, a natural person who otherwise exercises ultimate effective control over the management of the legal person;

(c) in the case of a legal arrangement, the trustee or other person who exercises ultimate effective control over the legal arrangement; and

(d) in the case of a foundation, a natural person who otherwise exercises ultimate effective control over the foundation;

"business in the regulated sector" has the meaning assigned by paragraph 1 of Schedule 4 to the *Proceeds of Crime Act 2008*, except that paragraph 1(o) (online gambling) of that Schedule is excluded;

"business relationship" means an arrangement between two or more persons where —

[5] Although this Act has been repealed it is possible for proceedings to be taken in respect of acts that took place when it was in force

[6] AT 6 of 2003

(a) at least one of those persons is acting in the course of a business;

(b) the purpose of the arrangement is to facilitate the carrying on of business in the regulated sector between the persons concerned on a frequent, habitual or regular basis; and

(c) the total amount of any payments to be made by any person to any other person in the course of that arrangement may neither be known nor be capable of being ascertained at the time the arrangement is made;

"collective investment scheme" has the meaning given in section 1 of the *Collective Investment Schemes Act 2008*[7] ;

"competent authority" means all Isle of Man administrative and law enforcement authorities concerned with AML/CFT, including in particular the Financial Supervision Commission, the Insurance and Pensions Authority, the Isle of Man Gambling Supervision Commission, the Department of Home Affairs, the Financial Intelligence Unit , the Office of Fair Trading, the Attorney General, and the Customs and Excise and Income Tax Divisions of the Treasury;

"constable" includes any officer appointed under section 1(2) of the *Customs and Excise Management Act 1986*[8] ;

"correspondent services" means banking, money or value transfer services and other similar relationships provided by a financial institution in one jurisdiction ("**the correspondent institution**") to a financial institution in another jurisdiction ("**the respondent institution**");

"currency" for the purposes of this Code includes virtual currencies;

"customer" —

(a) of a relevant person other than a relevant person that is a specified non-profit organisation, means a person —

(i) seeking to form a business relationship or carry out an occasional transaction; or
(ii) carrying on a business relationship or carrying out an occasional transaction,

[7] AT 7 of 2008
[8] AT 34 of 1986

with a relevant person who is carrying on business in the regulated sector in or from the Island and includes a person introduced to the relevant person within the meaning of paragraph 23; and

(b) of a specified non-profit organisation, means the persons, or groups of persons, who receive benefit (either directly or indirectly) for charitable, religious, cultural, educational, political, social or fraternal purposes. For the purposes of paragraphs 17 and 18, a customer is considered to be establishing a business relationship;

"customer due diligence" (except in the expression **"enhanced customer due diligence"**) means the measures specified in paragraphs 9 to 14, 17 to 24, 37 and 39 of this Code;

"designated non-financial businesses and professions" or **"designated businesses"** means relevant persons that are subject to oversight for compliance with the AML/CFT requirements by the Insurance and Pensions Authority, the Isle of Man Gambling Supervision Commission, or the Financial Supervision Commission or one of its delegates, apart from regulated persons;

"director" and **"officer"** include —

(a) for a limited liability company constituted under the *Limited Liability Companies Act 1996*[9], a member, manager or registered agent of such a company;

(b) for a limited partnership with legal personality in accordance with sections 48B to 48D of the *Partnership Act 1909*[10] —

(i) if a general partner is a natural person, that person;
(ii) if a general partner is a body corporate, the directors and officers of that body corporate;
(iii) if a general partner is a foundation, the council members (or equivalent) of that foundation; and

(c) for a foundation, a member of the council (or equivalent) of the foundation;

"document" includes information recorded in any form and, in relation to information recorded otherwise than in legible form, references to its production include references to produce a copy of the information in legible form;

[9] AT 19 of 1996
[10] AT 3 of 1909

"donor" in respect of a specified non-profit organisation means any person who provides funds to that specified non-profit organisation. For the purposes of paragraph 19, a donor is considered to be undertaking an occasional transaction;

"eligible introducer" means an introducer that satisfies the conditions of paragraph 23;

"employee" and **"worker"** of a relevant person have the same meanings as in section 173 of the *Employment Act 2006*[11] and include an individual who —

(a) works under a contract of employment or any other contract of service for the relevant person;

(b) practises alone or with others under the terms of a partnership agreement for the relevant person;

(c) is otherwise engaged within the business of a relevant person, in all cases where the individual undertakes to do or perform, directly or indirectly, any work or service for a relevant person, whether or not engaged directly by the relevant person or through another entity forming part of the group of entities of which the relevant person is a part, and the relevant person is not by virtue of the contract a customer of the individual; or

(d) is a director or officer of the relevant person;

"enhanced customer due diligence" means steps, additional to the measures specified in paragraphs 9 to 14, 17 to 24, 37 and 39, for the purpose of identifying customers and other persons, namely —

(a) considering whether additional identification information needs to be obtained;

(b) considering whether additional aspects of the identity of the customer need to be verified;

(c) the taking of reasonable measures to establish the source of the wealth of the customer and any beneficial owner; and

(d) considering what on-going monitoring should be carried on in accordance with paragraph 9;

"evidence of identity" means evidence of a person's identity obtained in accordance with the procedures specified in paragraphs 10(1), 12(1), 17(1) or 19(1) (as applicable);

[11] AT 21 of 2006

"exempted occasional transaction" means an occasional transaction (whether a single transaction or a series of linked transactions) where the amount of the transaction or, as the case may be, the aggregate in the case of a series of linked transactions, is less in value than —

(a) €3,000 in the case of a transaction entered into in the course of business referred to in paragraph 1(l) (casinos) or 1(n) (bookmakers) of Schedule 4 to the *Proceeds of Crime Act 2008*; or

(b) €5,000 in the case of a transaction entered into in the course of business referred to in paragraph 1(x) (*bureau de change*) or 1(z) (cheque encashment only) of Schedule 4 to the *Proceeds of Crime Act 2008*; or

(c) €1,000 in the case of a transaction entered into in the course of business referred to in paragraph 1(z) (money transmission services apart from cheque encashment) or 1(mm) (virtual currency) of Schedule 4 to the *Proceeds of Crime Act 2008*; or

(d) €15,000 in any other case;

"external disclosure" means a report made under paragraphs 26(1)(f) and 28;

"external regulated business" means business outside the Island that is regulated or supervised for AML/CFT purposes by an authority (whether a governmental or professional body and whether in the Island or elsewhere) empowered (whether by law or by the rules of the body) to regulate or supervise such business for such purposes;

"FATF Recommendations" means the 40 Recommendations set out in the Financial Action Task Force ("**FATF**") document 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation', adopted by the FATF in February 2012;

"financing of terrorism" includes the financing of proliferation and is to be construed in accordance with the definitions of "**financing**", "**terrorism**" and "**proliferation**" in section 3 of the *Terrorism and Other Crime (Financial Restrictions) Act 2014*;

"foundation" means a foundation established under the *Foundations Act 2011*[12] or a foundation or similar entity established under the law of another jurisdiction;

"information" includes data;

[12] AT 17 of 2011

"insurer" means a person authorised to carry on insurance business under section 8 of the *Insurance Act 2008*[13] or to whom a permit is issued under section 22 of that Act;

"internal disclosure" means a report made under paragraphs 26(1)(c) and 27;

"introducer" has the meaning given in paragraph 23(1);

"legal arrangement" means —

(a) an express trust; or

(b) any other arrangement that has a similar legal effect (such as a *fiducie, Treuhand or fideicomiso*);

"legal person" includes any body corporate or unincorporate capable of establishing a customer relationship with a financial institution or of owning property;

"List A" is a list maintained by the Department of Home Affairs on its website specifying jurisdictions regarding which the FATF (or a FATF-style regional body) has made a call on its members and other jurisdictions to apply countermeasures to protect the international financial system from the on-going and substantial risks of ML/FT emanating from the jurisdiction;

"List B" is a list maintained by the Department of Home Affairs on its website specifying jurisdictions with strategic AML/CFT deficiencies or those considered to pose a higher risk of ML/FT;

"List C" is a list maintained by the Department of Home Affairs on its website specifying jurisdictions which are considered to operate laws equivalent to those of the Isle of Man;

"ML/FT" means money laundering and financing of terrorism, or both, and includes attempted transactions in relation to ML/FT;

"Money Laundering Reporting Officer" or **"MLRO"** means an individual appointed under paragraph 25 and includes a deputy MLRO appointed under paragraph 25(3);

"money laundering" means an act that falls within section 158(11) of the *Proceeds of Crime Act 2008*;

"nominee company" means a wholly owned subsidiary that complies with paragraphs 2.7 or 3.1 of Schedule 1 to the Financial Services (Exemptions) Regulations 2011[14] or similar legislation in a jurisdiction in List C;

[13] AT 16 of 2008

[14] SD 0885/11 as amended by SD 0374/13

"occasional transaction" means any transaction (whether a single transaction or series of linked transactions) other than a transaction carried out in the course of an established business relationship formed by a relevant person and, for the purposes of this definition, a business relationship is an "established business relationship" if it is formed by a relevant person where that person has obtained, or is required to obtain, under procedures established, maintained and operated in accordance with this Code, satisfactory evidence of identity of the person who, in relation to the formation of that business relationship, was the customer;

"payable-through account" means an account maintained by a correspondent institution that may be operated directly by a customer of the respondent institution;

"person" includes any body of persons, corporate or unincorporate;

"politically exposed person" or **"PEP"** means any of the following —

(a) a natural person who is or has been entrusted with prominent public functions, including —

(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, *chargé d'affaires* or other high-ranking officer in a diplomatic service;
(ix) a high-ranking officer in an armed force;
(x) a senior member of an administrative, management or supervisory body of a state-owned enterprise;
(xi) a senior member of management of, or a member of, the governing body of an international entity or organisation; or
(xii) an honorary consul;

(b) any of the following family members of a natural person in (a) —

(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;
(vii) a grandparent; or
(viii) a grandchild;

(c) any close associate of a natural person in (a), including —

(i) any natural person known to be a joint beneficial owner of a legal entity or legal arrangement, or any other close business relationship, with such a person;
(ii) any natural person who is the sole beneficial owner of a legal entity or legal arrangement known to have been set up for the benefit of such a person;
(iii) any natural person known to be beneficiary of a legal arrangement of which such a person is a beneficial owner or beneficiary; or
(iv) any natural person known to be in a position to conduct substantial financial transactions on behalf of such a person;

and for the purposes of this definition —

"domestic PEP" means a natural person in (a) who is or has been entrusted with prominent public functions in the Isle of Man and any family members or close associates of that person in (b) or (c), regardless of the location of those family members or close associates; and

"foreign PEP" means a natural person in (a) who is or has been entrusted with prominent public functions outside the Isle of Man and any family members or close associates of that person in (b) or (c), regardless of the location of those family members or close associates;

"regulated person" means —

(a) any person holding a financial services licence issued under section 7 of the *Financial Services Act 2008*[15];

(b) any person authorised under section 8 *the Insurance Act 2008*;

(c) any person registered under section 25 of the *Insurance Act 2008*;

(d) a retirement benefits schemes administrator registered under section 36 of the *Retirement Benefits Schemes Act 2000*[16]; or

(e) a person holding an online gambling licence issued under section 4 of the *Online Gambling Regulation Act 2001* [17];

"relevant person" means a person carrying on a business in the regulated sector;

[15] AT 8 of 2008
[16] AT 14 of 2000
[17] AT 10 of 2001

"senior management" means the directors or key persons who are nominated to ensure that the relevant person is effectively controlled on a day-to-day basis and who have responsibility for overseeing the relevant person's proper conduct;

"shell bank" means a bank that is —

(a) incorporated in a jurisdiction in which it has no physical presence; and

(b) not affiliated with a financial services group that is subject to effective consolidated supervision;

and for the purposes of this definition —

"consolidated supervision", in relation to a financial services group, means supervision of the group by a regulatory body on the basis of the totality of its business, wherever conducted;

"financial services group" means a group of companies whose activities include to a significant extent activities that are, or if carried on in the Island would be, regulated activities under the *Financial Services Act 2008*; and

"physical presence" means the presence of staff and management based in the jurisdiction who operate at a level at which they are able to make meaningful decisions in respect of the functions and activities of the bank;

"specified non-profit organisation" means a relevant person carrying on the business of a specified non-profit organisation within the meaning assigned by paragraph 1(6) of Schedule 4 to the *Proceeds of Crime Act 2008*;

"suspicious activity" means any activity or information received in the course of a business relationship, occasional transaction or attempted transaction that causes the relevant person to —

(a) know or suspect; or

(b) have reasonable grounds for knowing or suspecting,

that the activity or information is related to money laundering or the financing of terrorism;

"trusted person" means —

(a) a regulated person;

(b) a nominee company of a regulated person where the regulated person is responsible for the nominee company's compliance with the AML/CFT requirements;

(c) an advocate within the meaning of the *Advocates Act 1976*[18], a registered legal practitioner within the meaning of the *Legal Practitioners Registration Act 1986*[19] or an accountant carrying on business in or from the Isle of Man, if the relevant person is satisfied that the rules of the professional body of the advocate, legal practitioner or accountant embody requirements and procedures that are at least equivalent to this Code;

(d) a person who acts in the course of external regulated business and is regulated under the law of a jurisdiction in List C, unless the relevant person has reason to believe that the jurisdiction in question does not apply, or insufficiently applies, the FATF Recommendations in respect of the business of that person; or

(e) a nominee company of a person who acts in the course of external regulated business and is regulated under the law of a jurisdiction included in List C where the person is responsible for the nominee company's compliance with the AML/CFT requirements, unless the relevant person has reason to believe that the jurisdiction in question does not apply, or insufficiently applies, the FATF Recommendations in respect of the business of that person;

"unusual activity" means any activity or information received in the course of a business relationship, occasional transaction or attempted transaction where —

(a) there are transactions that have no apparent economic or lawful purpose, examples of which include transactions that are —

(i) complex;
(ii) both large and unusual; or
(iii) of an unusual pattern;

(b) the relevant person becomes aware of anything that causes the relevant person to doubt the identity of a person it is obliged to identify under this Code;

(c) the relevant person becomes aware of anything that causes the relevant person to doubt the good faith of a customer, beneficial owner, beneficiary or introducer.

[18] AT 27 of 1976
[19] AT 15 of 1986

"virtual currency" means convertible virtual currencies such as crypto-currencies or similar concepts where the concept is accepted by persons as a means of payment for goods or services, a unit of account, a store of value or a commodity;

"virtual currency business" means the business of issuing, transmitting, transferring, providing safe custody or storage of, administering, managing, lending, buying, selling, exchanging or otherwise trading or intermediating virtual currencies.

(2) In this Code, a reference to an amount of currency expressed in Euros is to be construed as also meaning that amount converted into, and expressed as, an amount of any other currency.

(3) In this Code, in any case where a financial product (such as a life assurance policy) has been transferred by its holder (the assignor) to another person (the assignee), references in any provision to requirements in relation to a customer should be construed as including a reference to an assignee.

PART 2 – GENERAL REQUIREMENTS

4 General requirements

(1) In conducting business in the regulated sector a relevant person must not enter into or carry on a business relationship or carry out an occasional transaction with or for another person unless the relevant person —

(a) establishes, maintains and operates —

(i) risk assessment and ongoing monitoring procedures in accordance with Part 3;
(ii) customer due diligence procedures in accordance with parts 4, 5 and 6 and paragraphs 37 and 39;
(iii) reporting and disclosure procedures in accordance with Part 7;
(iv) compliance procedures in accordance with Part 8;
(v) procedures in accordance with Part 9; and
(vi) internal controls and communication procedures that are appropriate for the purposes of forestalling and preventing ML/FT;

(b) takes appropriate measures for the purpose of making employees and workers aware of —

(i) the AML/CFT requirements; and
(ii) the procedures established, maintained and operated under (a);

(c) monitors and tests compliance in accordance with paragraph 29;

(d) provides education and training in accordance with paragraph 31; and

(e) complies with paragraphs 38 and 40.

(2) The procedures and controls referred to in sub-paragraph (1) must be approved by the senior management of the relevant person.

(3) The customer due diligence procedures referred to in sub-paragraph (1)(a)(ii) must enable the relevant person to manage and mitigate the risks of ML/FT that have been identified by the risk assessments and ongoing monitoring carried out in accordance with Part 3.

(4) A relevant person must carry out customer due diligence in accordance with parts 4 to 6 —

(a) on the basis of materiality and risk of ML/FT;

(b) in accordance with the risk assessments and ongoing monitoring carried out under Part 3; and

(c) having particular regard to whether a customer poses a higher risk of ML/FT.

5 Specified non-profit organisations

Despite paragraph 4, paragraphs 10 to 12 and 13(5) do not apply to specified non-profit organisations.

PART 3 – RISK ASSESSMENT AND ONGOING MONITORING

6 Business risk assessment

(1) A relevant person must carry out an assessment (a "**business risk assessment**") that estimates the risk of ML/FT on the part of the relevant person's business and customers.

(2) The business risk assessment must be —

(a) undertaken as soon as reasonably practicable after the relevant person commences business;

(b) regularly reviewed and, if appropriate, amended so as to keep it up-to-date; and

(c) documented in order to be able to demonstrate its basis.

(3) The business risk assessment must have regard to all relevant risk factors including —

(a) the nature, scale and complexity of the relevant person's activities;

(b) the products and services provided by the relevant person;

(c) the persons to whom and the manner in which the products and services are provided;

(d) reliance on third parties for elements of the customer due diligence process; and

(e) technological developments.

7 Customer risk assessment

(1) A relevant person must carry out an assessment (a "**customer risk assessment**") that estimates the risk of ML/FT posed by a customer.

(2) The customer risk assessment must be —

(a) undertaken prior to the establishment of a business relationship or the carrying out of an occasional transaction with or for that customer;

(b) regularly reviewed and, if appropriate, amended so as to keep it up-to-date; and

(c) documented in order to be able to demonstrate its basis.

(3) The customer risk assessment must have regard to all relevant risk factors, including —

(a) the business risk assessment carried out under paragraph 6;

(b) the nature, scale, complexity and location of the customer's activities;

(c) the persons to whom and the manner in which the products and services are provided; and

(d) reliance on third parties for elements of the customer due diligence process.

8 Technological developments risk assessment

(1) A relevant person must carry out an assessment (a "**technological developments risk assessment**") that estimates the risk of ML/FT posed by any technological developments to the relevant person's business.

(2) The technological developments risk assessment must be —

(a) undertaken prior to the launch or implementation of new products, new business practices and delivery methods including new delivery systems;

(b) undertaken prior to the use of developing technologies for both new and pre-existing products; and

(c) documented in order to be able to demonstrate its basis.

(3) The technological developments risk assessment must have regard to all relevant factors including —

(a) the business risk assessment carried out under paragraph 6;

(b) digital information and document storage;

(c) electronic verification of documents; and

(d) data and transaction screening systems.

9 Ongoing monitoring

(1) A relevant person must perform ongoing and effective monitoring of any business relationship, including —

(a) review of information held for the purpose of customer due diligence to ensure that it is up-to-date and appropriate (in particular where the relationship poses a higher risk of ML/FT);

(b) appropriate scrutiny of transactions and other activities, paying particular attention to suspicious and unusual activity; and

(c) appropriate scrutiny of transactions to ensure that they are consistent with —

(i) the relevant person's knowledge of the customer, the relevant person's business and risk profile and, if necessary, the source of funds for the transaction;
(ii) the business risk assessment carried out under paragraph 6;
(iii) the customer risk assessment carried out under paragraph 7; and
(iv) any relevant technological developments risk assessment carried out under paragraph 8.

(2) The extent and frequency of any monitoring under this paragraph must be determined —

(a) on the basis of materiality and risk of ML/FT;

(b) in accordance with the risk assessments carried out under this Part; and

(c) having particular regard to whether a customer poses a higher risk of ML/FT.

PART 4 – CUSTOMER DUE DILIGENCE

10 New business relationships

(1) A relevant person must, in relation to each new business relationship, establish, maintain and operate the procedures specified in sub-paragraph (3), which procedures must comply with the requirements of this paragraph.

(2) The procedures must be undertaken —

(a) before a business relationship is entered into; or

(b) during the formation of that relationship.

(3) The procedures referred to in sub-paragraph (1) are —

(a) the identification of the customer;

(b) the verification of the identity of the customer using reliable, independent source documents;

(c) the verification of the legal status of the customer using relevant information obtained from a reliable, independent source;

(d) the obtaining of information on the nature and intended purpose of the business relationship; and

(e) the taking of reasonable measures to establish the source of funds.

(4) In exceptional circumstances the verification of the identity of the customer in accordance with sub-paragraph (3)(b) may be undertaken following the establishment of the business relationship if —

(a) it occurs as soon as reasonably practicable;

(b) it is essential not to interrupt the normal course of business;

(c) the customer has not been identified as posing a higher risk of ML/FT and the risks of ML/FT are effectively managed;

(d) the relevant person has not identified any suspicious activity;

(e) the relevant person's senior management has approved the establishment of the business relationship and any subsequent activity until sub-paragraph (3)(b) has been complied with; and

(f) the relevant person ensures that the amount, type and number of transactions is appropriately limited and monitored.

(5) Except as provided in sub-paragraph (4) and Part 6, procedures comply with this paragraph if they require, when satisfactory evidence of identity in accordance with sub-paragraph (1) is not obtained or produced —

(a) the business relationship to proceed no further; and

(b) the relevant person to terminate the business relationship and consider making an internal disclosure in accordance with paragraphs 26 and 27.

11 Continuing business relationships

(1) A relevant person must, in relation to each continuing business relationship, establish, maintain and operate the procedures specified in sub-paragraph (3), which procedures must comply with the requirements of this paragraph.

(2) The procedures must be undertaken during a business relationship as soon as reasonably practicable.

(3) The procedures referred to in sub-paragraph (1) are —

(a) an examination of the background and purpose of the business relationship;

(b) if no evidence of identity was produced after the business relationship was established, the taking of such measures as will require the production of such information in accordance with paragraph 10(1);

(c) if evidence of identity was produced in accordance with paragraph 10(1), the taking of such measures as will determine whether the evidence of identity produced under that paragraph is satisfactory; and

(d) if evidence of identity produced in accordance with paragraph 10(1) is not for any reason satisfactory, the taking of such measures as will require the production by the customer of evidence of identity or the taking of such measures as will produce evidence of identity in accordance with paragraph 10(1).

(4) The relevant person —

(a) must keep written records of any examination, steps, measures or determination made or taken under sub-paragraph (1) (which records shall be records to which paragraph 32 applies); and

(b) must, on request, make such findings available to the competent authorities and auditors (if any).

(5) Except as provided in Part 6, procedures comply with this paragraph if they require, when satisfactory evidence of identity, in accordance with paragraph 10(1), is not obtained or produced —

(a) the business relationship to proceed no further; and

(b) the relevant person to consider terminating the business relationship and consider making an internal disclosure in accordance with paragraphs 26 and 27.

12 Occasional transactions

(1) A relevant person must, in relation to an occasional transaction, establish, maintain and operate the procedures specified in sub-paragraph (3), which procedures must comply with the requirements of this paragraph.

(2) The procedures must be undertaken before the occasional transaction is entered into.

(3) The procedures referred to in sub-paragraph (1) are —

(a) the identification of the customer;

(b) the verification of the identity of the customer using reliable, independent source documents;

(c) the verification of the legal status of the customer using relevant information obtained from a reliable, independent source;

(d) the obtaining of information on the nature and intended purpose of the occasional transaction; and

(e) the taking of reasonable measures to establish the source of funds.

(4) Except as provided in paragraph 12(5) and Part 6, procedures comply with this paragraph if they require, when satisfactory evidence of identity in accordance with sub-paragraph (1) is not obtained or produced —

(a) the occasional transaction not to be carried out; and

(b) the relevant person to consider making an internal disclosure in accordance with paragraphs 26 and 27.

(5) Sub-paragraph (1) does not require verification of identity in accordance with paragraph 12(3)(b) to be produced if the transaction is an exempted occasional transaction.

13 Beneficial ownership and control

(1) This paragraph applies when a relevant person is operating the procedures required by paragraph 9 and parts 4, 5 and 6 (as applicable).

(2) A relevant person must, in the case of any customer —

(a) where that customer is not a natural person, identify who is the beneficial owner of the customer;

(b) take reasonable measures to verify the identity of any beneficial owner of the customer, using relevant information obtained from a reliable, independent source; and

(c) subject to paragraphs 21 and 24, determine whether the customer is acting on behalf of another person and, if so, identify that other person, and take reasonable measures to verify that other person's identity using relevant information obtained from a reliable, independent source.

(3) Without limiting sub-paragraph (2), the relevant person must, in the case of a customer that is a legal person or legal arrangement —

(a) verify that any person purporting to act on behalf of the customer is authorised to do so;

(b) identify that person and take reasonable measures to verify the identity of that person using reliable, independent source documents;

(c) in the case of a legal arrangement, identify —

(i) the trustees or any other controlling party;
(ii) any known beneficiaries; and
(iii) the settlor or other person by whom the legal arrangement is made or on whose instructions the legal arrangement is formed;

(d) in the case of a foundation, identify —

(i) the council members (or equivalent);
(ii) any known beneficiaries; and
(iii) the founder and any other dedicator;

(e) obtain information concerning the names and addresses of any other natural persons having power to direct the customer's activities and take reasonable measures to verify that information;

(f) obtain information concerning the person by whom, and the method by which, binding obligations may be imposed on the customer; and

(g) obtain information to understand the ownership and control structure of the customer.

(4) Without limiting sub-paragraph (2), in the case of a customer for a life assurance policy, an insurer must —

(a) identify the beneficiaries of the life assurance policy; and

(b) immediately prior to the making of any payment or loan to a beneficiary of the life assurance policy, verify the identity of each such beneficiary using relevant information obtained from a reliable, independent source; and

(c) subject to paragraph 24(7), determine whether the customer is acting on behalf of another person and, if so, identify that other person, and take reasonable measures to verify that other person's identity using relevant information obtained from a reliable, independent source.

(5) Subject to paragraph 24(7) and without limiting sub-paragraphs (2) and (3), the relevant person must not, in the case of a customer that is a legal person or legal arrangement, make any payment or loan to a beneficial owner of that person or beneficiary of that arrangement unless it has —

(a) identified the recipient of the payment or loan; and

(b) on the basis of materiality and risk of ML/FT, verified the identity of the recipient using relevant information or data obtained from a reliable, independent source.

14 Politically exposed persons

(1) A relevant person must maintain appropriate procedures and controls for the purpose of determining whether any of the following is a PEP —

(a) any customer;

(b) any natural person having power to direct the activities of a customer;

(c) any beneficial owner or known beneficiaries.

(2) A relevant person must maintain appropriate procedures and controls for requiring the approval of its senior management —

(a) before any business relationship is established with;

(b) before any occasional transaction is carried out with; or

(c) before a business relationship is continued with,

a domestic PEP who has been identified as posing a higher risk of ML/FT, or any foreign PEP.

(3) A relevant person must take reasonable measures to establish the source of wealth of a domestic PEP who has been identified as posing a higher risk of ML/FT, or any foreign PEP.

(4) A relevant person must perform ongoing and effective enhanced monitoring of any business relationship with a domestic PEP who has been identified as posing a higher risk of ML/FT, or any foreign PEP.

(5) For the avoidance of doubt, this paragraph does not remove the requirement to conduct enhanced customer due diligence where a PEP has been identified as posing a higher risk of ML/FT.

15 Enhanced customer due diligence

(1) A relevant person must obtain enhanced customer due diligence —

(a) where a customer poses a higher risk of ML/FT as assessed by the customer risk assessment carried out in accordance with paragraph 7; or

(b) in the event of any unusual activity.

(2) A relevant person must consider whether to obtain enhanced customer due diligence in the event of any suspicious activity.

(3) For the avoidance of doubt, if higher risk of ML/FT within the meaning of sub-paragraph (1)(a) is assessed then paragraphs 10(4), 20, 22, 23(5), 24(2), (5) and (7) to (9) do not apply.

(4) Matters that pose a higher risk of ML/FT include but are not restricted to —

(a) a business relationship or occasional transaction with a customer resident or located in a jurisdiction in List A; and

(b) a customer that is the subject of a warning in relation to AML/CFT matters issued by a competent authority or equivalent authority in another jurisdiction.

(5) Matters that may pose a higher risk include but are not restricted to —

(a) activity in a jurisdiction the relevant person deems to be higher risk of ML/FT;

(b) a business relationship or occasional transaction with a customer resident or located in a jurisdiction in List B;

(c) activity in a jurisdiction in List A or B;

(d) a situation that by its nature presents a significant risk of ML/FT;

(e) a business relationship or occasional transaction with a PEP;

(f) a company that has nominee shareholders or shares in bearer form;

(g) the provision of high risk products;

(h) the provision of services to high-net-worth individuals;

(i) a legal arrangement; and

(j) persons performing prominent functions for international organisations.

(6) Except as provided in Part 6, when enhanced due diligence is not obtained or produced either where it is required under sub-paragraph (1) or considered appropriate under sub-paragraph (2) —

(a) the business relationship or occasional transaction must proceed no further; and

(b) the relevant person must consider terminating that relationship and consider making an internal disclosure in accordance with paragraphs 26 and 27.

PART 5 – SPECIFIED NON-PROFIT ORGANISATIONS

16 Application

This Part only applies to specified non-profit organisations.

17 New business relationships of specified non-profit organisations

(1) A specified non-profit organisation must, in relation to each new business relationship, establish, maintain and operate the procedures specified in sub-paragraph (3), which procedures must comply with the other requirements of this paragraph.

(2) The procedures must be undertaken —

(a) before a business relationship is entered into; or

(b) during the formation of that relationship.

(3) The procedures referred to in sub-paragraph (1) are —

(a) the identification of the customer;

(b) the taking of reasonable measures to verify the identity of the customer using reliable, independent sources; and

(c) the obtaining of information on the nature and intended purpose of the business relationship.

(4) A specified non-profit organisation must, in the case of any correspondent non-profit organisation receiving funds on behalf of a customer, identify that correspondent non-profit organisation, and take reasonable measures to verify that correspondent non-profit organisation's identity using relevant information obtained from reliable, independent sources.

(5) Except as provided in Part 6, procedures comply with this paragraph if they require, when satisfactory evidence of identity in accordance with sub-paragraph (1) is not obtained or produced —

(a) the business relationship to proceed no further; and

(b) the specified non-profit organisation to terminate the business relationship and consider making an internal disclosure in accordance with paragraphs 26 and 27.

(6) "**Correspondent non-profit organisation**" for the purposes of sub-paragraph (4) means a non-profit organisation that acts as an intermediary between a specified non-profit organisation and its customers.

18 Continuing business relationships of specified non-profit organisations

(1) A specified non-profit organisation must, in relation to each continuing business relationship, establish, maintain and operate the procedures specified in sub-paragraph (3), which procedures must comply with the requirements of this paragraph.

(2) The procedures must be undertaken during a business relationship as soon as reasonably practicable.

(3) The procedures referred to in sub-paragraph (1) are —

(a) an examination of the background and purpose of the business relationship;

(b) if no evidence of identity was obtained after the business relationship was established, the taking of such measures as will require the production of such information in accordance with paragraph 17(1);

(c) if evidence of identity was obtained under paragraph 17(1), the taking of such measures as will determine whether the evidence of identity obtained under that paragraph is satisfactory; and

(d) if evidence of identity obtained under paragraph 17(1) is not for any reason satisfactory, the taking of such measures as will require the identification of the beneficiaries or the taking of such measures as will produce evidence of identity in accordance with paragraph 17(1).

(4) A specified non-profit organisation —

(a) must keep written records of any examination, steps, measures or determination made or taken under sub-paragraph (1) (which records shall be records to which paragraph 32 applies); and

(b) must, on request, make such findings available to the competent authorities and auditors (if any).

(5) Except as provided in Part 6, procedures comply with this paragraph if they require, when evidence of identity in accordance with paragraph 17(1) is not obtained or produced —

(a) the business relationship to proceed no further; and

(b) the specified non-profit organisation to consider terminating that business relationship and consider making an internal disclosure in accordance with paragraphs 26 and 27.

19 Occasional transactions of specified non-profit organisations

(1) A specified non-profit organisation must, in relation to an occasional transaction, establish, maintain and operate the procedures specified in sub-paragraph (3), which procedures must comply with the requirements of this paragraph.

(2) The procedures specified in sub-paragraph (1) must be undertaken before the occasional transaction is accepted.

(3) The procedures specified in sub-paragraph (1) are —

(a) the identification of the donor of the funds for the transaction; and

(b) the verification of the identity of the donor using reliable, independent sources.

(4) Except as provided in Part 6, procedures comply with this paragraph if they require, when satisfactory evidence of identity in accordance with sub-paragraph (1) is not obtained or produced —

(a) the occasional transaction not to be carried out; and

(b) the specified non-profit organisation to consider making an internal disclosure in accordance with paragraphs 26 and 27.

(5) Sub-paragraph (1) does not require evidence of identity in accordance with paragraph 19(3) to be obtained if the transaction is an exempted occasional transaction.

PART 6 – SIMPLIFIED CUSTOMER DUE DILIGENCE

20. Acceptable applicants

(1) Verification of the identity of a customer for —

(a) a new business relationship in accordance with paragraph 10(1); or

(b) an occasional transaction in accordance with paragraph 12(1) or 19(1),

is not required to be produced if the conditions in sub-paragraph (2) are met.

(2) The conditions referred to in sub-paragraph (1) are that —

(a) the identity of the customer is known to the relevant person;

(b) the relevant person knows the nature and intended purpose of the business relationship or occasional transaction;

(c) the relevant person has not identified any suspicious activity; and

(d) the relevant person has satisfied itself that —

(i) the customer is a trusted person; or

(ii) the customer is a company listed on a recognised stock exchange or a wholly owned subsidiary of such a company in relation to which the relevant person has taken reasonable measures to establish that there is effective control of the company by an individual, group of individuals or another legal person or legal arrangement (which persons are treated as beneficial owners for the purposes of this Code); and

(iii) the customer does not pose a higher risk of ML/FT.

21 Persons in a regulated sector acting on behalf of a third party

(1) This paragraph only applies to a regulated person holding a financial services licence issued under section 7 of the *Financial Services Act 2008* to carry on regulated activities under Class 1 (deposit taking), Class 2 (investment business), Class 3 (services to collective investment schemes) or Class 8 (money transmission services) of the Regulated Activities Order 2011[20].

(2) Where the regulated person determines that a customer is acting on behalf of another person who is an underlying client of the customer, the regulated person need not comply with paragraph 13(2)(c) if the following conditions are met —

(a) the regulated person has satisfied itself that the customer is a person specified in sub-paragraph (6);

(b) the customer has identified and verified the identity of the underlying client in accordance with paragraphs 10 to 13 and has no reason to doubt those identities;

(c) the regulated person and the customer know the nature and intended purpose of the business relationship;

(d) the customer has identified the source of funds of the underlying client;

(e) the regulated person has not identified any suspicious activity; and

(f) written terms of business are in place between the regulated person and the customer in accordance with sub-paragraph (3).

(3) The written terms of business required to be in place in accordance with sub-paragraph (2)(f) must in all cases require the customer to —

[20] SD 0884/11 as amended by SD 0373/13

(a) supply to the regulated person immediately on request, information on the identity of the underlying client, copies of the evidence verifying the identity of the underlying client and all other due diligence information held by the customer in respect of the underlying client in any particular case;

(b) inform the regulated person specifically of each case where the customer is not required or has been unable to verify the identity of the underlying client;

(c) inform the regulated person if the customer is no longer able to comply with the provisions of the written terms of business because of a change of the law applicable to the customer; and

(d) do all such things as may be required by the regulated person to enable the regulated person to comply with its obligations under sub-paragraph (2).

(4) In satisfying the conditions under sub-paragraph (2), the regulated person must take reasonable measures to ensure that —

(a) the evidence produced or to be produced is satisfactory; and

(b) the customer due diligence procedures of the customer are fit for purpose.

(5) The regulated person must take reasonable measures to satisfy itself that —

(a) the procedures for implementing this paragraph are effective by testing them on a random and periodic basis no less than once every 12 months; and

(b) the written terms of business confer the necessary rights on the regulated person.

(6) The persons referred to in sub-paragraph (2)(a) are —

(a) a regulated person;

(b) a nominee company of a regulated person where the regulated person is responsible for the nominee company's compliance with the AML/CFT requirements;

(c) a collective investment scheme (except for a scheme within the meaning of Schedule 3 (exempt schemes) to the *Collective Investment Schemes Act 2008*) where the manager or administrator of such a scheme is a regulated person, or where the person referred to in sub-paragraph (2)(a) is an equivalent scheme in a jurisdiction in List C where the manager or administrator of that scheme is a person referred to in sub-paragraph (6)(e);

(d) a designated business;

(e) a person who acts in the course of external regulated business and who is —

(i) regulated under the law of a jurisdiction in List C; and
(ii) subject to AML/CFT requirements and procedures that are at least equivalent to the Code,

but does not solely carry on activities equivalent to either or both of Class 4 (corporate services) or Class 5 (trust services) under the Regulated Activities Order 2011; and

(f) a nominee company of a person specified in (e) where that person is responsible for the nominee company's compliance with the equivalent AML/CFT requirements.

(7) In this paragraph "**underlying client**" includes a beneficial owner of that underlying client.

22 Generic designated business

(1) Subject to sub-paragraph (2), verification of the identity of a customer for a new business relationship in accordance with paragraph 10(1) is not required to be produced if the relevant person is conducting generic designated business.

(2) This paragraph applies if the relevant person —

(a) has identified the customer and the beneficial owners (if any) and has no reason to doubt those identities;

(b) has not identified the customer as posing a higher risk of ML/FT;

(c) knows the nature and intended purpose of the business relationship;

(d) has not identified any suspicious activity; and

(e) has identified the source of funds.

(3) "**Generic designated business**" for the purposes of this paragraph means designated business carried on by a relevant person that does not involve participation in any financial transactions on behalf of the customer. The provision of professional advice or audit services may be examples of generic designated business.

23 Eligible introducers

(1) If a customer is introduced to a relevant person by a third party (the "**introducer**"), the relevant person may, if it thinks fit, comply with this paragraph, instead of paragraphs 10, 12, 17 or 19 (as applicable).

(2) The relevant person must establish, maintain and operate the procedures specified in sub-paragraph (4).

(3) The procedures must be undertaken before a business relationship or occasional transaction is entered into.

(4) The procedures referred to in sub-paragraph (2) are —

(a) the production by the introducer of evidence of identity of the customer in accordance with paragraph 10(1), 12(1), 17(1) or 19(1) (as applicable); or

(b) the taking of such other measures as will produce evidence of identity in accordance with paragraph 10(1), 12(1), 17(1) or 19(1) (as applicable); and

(c) the undertaking of a customer risk assessment in accordance with paragraph 7.

(5) Sub-paragraph (2) does not require verification of identity to be produced if the relevant person —

(a) has identified the customer and the beneficial owner (if any) and has no reason to doubt those identities;

(b) knows the nature and intended purpose of the business relationship;

(c) has not identified any suspicious activity;

(d) has satisfied itself that —

(i) the introducer is a trusted person other than a nominee company of either a regulated person or a person who acts in the course of external regulated business; or
(ii) the relevant person and the customer are bodies corporate in the same group; or

(iii) the transaction is an exempted occasional transaction; and

(e) has satisfied itself that the introducer does not pose a higher risk of ML/FT.

(6) The relevant person must not enter into a business relationship with a customer that is introduced by an introducer unless written terms of business are in place between the relevant person and the introducer and, despite sub-paragraphs (4) and (5), those terms of business require in all cases the introducer to —

(a) verify the identity of all customers introduced to the relevant person sufficiently to comply with the AML/CFT requirements;

(b) take reasonable measures to verify the identity of the beneficial owner (if any);

(c) establish and maintain a record of the evidence of identity for at least 5 years calculated in accordance with paragraph 33(1);

(d) establish and maintain records of all transactions between the introducer and the customer if the records are concerned with or arise out of the introduction (whether directly or indirectly) for at least 5 years calculated in accordance with paragraph 33(1);

(e) supply to the relevant person immediately on request, copies of the evidence verifying the identity of the customer and the beneficial owner (if any) and all other customer due diligence information held by the introducer in any particular case;

(f) supply to the relevant person immediately copies of the evidence verifying the identity of the customer and the beneficial owner (if any) and all other customer due diligence information, in accordance with paragraphs 10(1), 12(1), 17(1) or 19(1) (as applicable), held by the introducer in any particular case if —

(i) the introducer is to cease trading;
(ii) the introducer is to cease doing business with the customer;
(iii) the relevant person informs the introducer that it no longer intends to rely on the terms of business entered into under this paragraph;

(g) inform the relevant person specifically of each case where the introducer is not required or has been unable to verify the identity of the customer or the beneficial owner (if any);

(h) inform the relevant person if the introducer is no longer able to comply with the provisions of the written terms of business because of a change of the law applicable to the introducer; and

(i) do all such things as may be required by the relevant person to enable the relevant person to comply with its obligation under sub-paragraph (8).

(7) A relevant person must ensure that the procedures under sub-paragraph (2) are fit for the purpose of ensuring that the evidence produced or to be produced is satisfactory and that the procedures of the introducer are likewise fit for that purpose.

(8) A relevant person must take measures to satisfy itself that —

(a) the procedures for implementing this paragraph are effective by testing them on a random and periodic basis no less than once every 12 months; and

(b) the written terms of business confer the necessary rights on the relevant person to satisfy the requirements of this paragraph.

(9) In order to rely upon an introducer a relevant person must —

(a) take measures to satisfy itself that the introducer is not itself reliant upon a third party for the evidence of identity of the customer in accordance with paragraphs 10(1), 12(1), 17(1) or 19(1) (as applicable); and

(b) take such measures as necessary to ensure it becomes aware of any material change to the introducer's status or the status of the jurisdiction in which the introducer is regulated.

(10) Except as provided in sub-paragraph (5), procedures comply with this paragraph if they require, when evidence of identity in accordance with paragraphs 10(1), 12(1), 17(1) or 19(1) (as applicable) is not obtained or produced —

(a) the business relationship or occasional transaction to proceed no further; and

(b) the relevant person to consider terminating that business relationship and consider making an internal disclosure in accordance with paragraphs 26 and 27.

(11) The ultimate responsibility for ensuring that customer due diligence procedures comply with the terms of this Code remains with the relevant person and not with the introducer.

(12) In sub-paragraph (5)(d)(ii), "**group**", in relation to a body corporate, means that body corporate, any other body corporate that is its holding company or subsidiary and any other body corporate that is a subsidiary of that holding company, and "**subsidiary**" and "**holding company**" shall be construed in accordance with section 1 of the *Companies Act 1974*[21] or section 220 of the *Companies Act 2006*[22] (as applicable).

24 Miscellaneous

(1) Sub-paragraphs (2) to (6) apply to—

(a) an insurer effecting or carrying out a contract of insurance; and

(b) an insurance intermediary who, in the course of business carried on in or from the Island, acts as an insurance intermediary in respect of the effecting or carrying out of a contract of insurance.

(2) An insurer or insurance intermediary, as the case may be, need not comply with Part 4 and paragraph 23 if the contract of insurance referred to in sub-paragraph (1) is a contract where —

(a) the annual premium is less than €1,000, or a single premium, or series of linked premiums, is less than €2,500; or

(b) there is neither a surrender value nor a maturity value (for example, term insurance).

(3) In respect of a contract of insurance satisfying sub-paragraph (2) an insurer may, having paid due regard to the risk of ML/FT, consider it appropriate to comply with Part 4 and paragraph 23 but to defer such compliance unless a claim is made or the policy is cancelled.

(4) If a claim is made under a contract of insurance referred to in sub-paragraph (1) that has neither a surrender value nor a maturity value (for example on the occurrence of an insured event), and the amount of the settlement is greater than €2,500 the insurer must satisfy itself as to the identity of the policyholder or claimant (if different to the policyholder).

(5) An insurer or insurance intermediary, as the case may be, need not comply with sub-paragraph (4) if settlement of the claim is to —

(a) a third party in payment for services provided (for example to a hospital where health treatment has been provided);

(b) a supplier for services or goods; or

[21] AT 30 of 1974
[22] AT 13 of 2006

(c) the policyholder where invoices for services or goods have been provided to the insurer,

and the insurer believes the services or goods to have been supplied in respect of the insured event.

(6) If a contract of insurance referred to in sub-paragraph (1) is cancelled resulting in the repayment of premiums and the amount of the settlement is greater than €2,500, the insurer or insurance intermediary, as the case may be, must comply with Part 4 and paragraph 23.

(7) In respect of a pension, superannuation or similar scheme that provides retirement benefits to employees, if contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme, the relevant person —

(a) may treat the employer, trustee or any other person who has control over the business relationship, including the administrator or the scheme manager, as the customer; and

(b) need not comply with paragraph 13(2)(c).

(8) A relevant person need not comply with paragraph 13(2)(c) in respect of a customer that is —

(a) a collective investment scheme (except for a scheme within the meaning of Schedule 3 (exempt schemes) to the *Collective Investment Schemes Act 2008*), or an equivalent arrangement in a jurisdiction in List C; and

(b) if the manager or administrator of such a scheme or equivalent arrangement is a regulated person or a person who acts in the course of external regulated business carrying on equivalent regulated activities in a jurisdiction in List C.

(9) The Isle of Man Post Office need not comply with Part 4, if it sees fit, when it —

(a) issues or redeems a postal order up to the value of £50;

(b) issues or administers funds on behalf of other Government departments or statutory boards;

(c) accepts payment for Government utilities or statutory boards up to the value of £650 in cash or £5,000 by other means of payment;

(d) accepts payments on behalf of utilities and telecom service providers up to the value of £650 in cash or £5,000 by other means of payment;

(e) accepts payments on behalf of a third party from customers of that party in respect of provision by that third party of goods or services, provided that the third party has been assessed as posing a low risk of ML/FT, up to the value of £650 in cash or £5,000 by other means of payment; and

(f) accepts donations on behalf of a charity, provided that the charity is registered in the Isle of Man and has been assessed as posing a low risk of ML/FT, up to the value of £650 in cash or £5,000 by other means of payment.

(10) If there is any suspicious activity, sub-paragraphs (2), (5), (7), (8) and (9) cease to apply and the relevant person must make an internal disclosure in accordance with paragraphs 26 and 27.

(11) Subject to sub-paragraph (12), where the relevant person (the "**purchaser**") is acquiring a customer or group of customers from another relevant person (the "**vendor**"), the acquired customer or group of customers will be a new business relationship for the purchaser. In this case, customer due diligence and enhanced customer due diligence of that customer or that group of customers may be provided to the purchaser by the vendor.

(12) Sub-paragraph (11) applies where —

(a) the vendor is —

(i) a regulated person;
(ii) a collective investment scheme (except for a scheme within the meaning of Schedule 3 (exempt schemes) to the Collective Investment Schemes Act 2008) where the manager or administrator of such a scheme is a regulated person, or where the vendor is an equivalent scheme in a jurisdiction in List C where the manager or administrator of that scheme is a person referred to in sub-paragraph (12)(a)(iv);
(iii) a designated business;
(iv) a person who acts in the course of external regulated business and who is —

(A) regulated under the law of a jurisdiction in List C; and

(B) subject to AML/CFT requirements and procedures that are at least equivalent to the Code,

but does not solely carry on activities equivalent to either or both of Class 4 (corporate services) or Class 5 (trust services) under the Regulated Activities Order 2011;

(b) the purchaser —

(i) has identified the customer and the beneficial owner (if any) and has no reason to doubt those identities;
(ii) has not identified the customer as posing a higher risk of ML/FT;
(iii) knows the nature and intended purpose of the business relationship;
(iv) has identified the source of funds;
(v) has not identified any suspicious activity; and
(vi) has put in place appropriate measures to remediate, in a timely manner, any deficiencies in the customer due diligence of the acquired customer or group of customers.

PART 7 – REPORTING AND DISCLOSURES

25 Money Laundering Reporting Officer

(1) A relevant person must appoint a Money Laundering Reporting Officer ("**MLRO**") to exercise the functions conferred by paragraphs 26 and 28.

(2) The MLRO must —

(a) be sufficiently senior in the organisation of the relevant person or have sufficient experience and authority;

(b) have a right of direct access to the directors or the managing board (as the case may be) of the relevant person; and

(c) have sufficient time and resources to properly discharge the responsibilities of the position,

to be effective in the exercise of its functions.

(3) A relevant person may appoint a Deputy Money Laundering Reporting Officer ("**Deputy MLRO**") in order to exercise the functions specified in paragraphs 26 and 28 in the MLRO's absence.

26 Reporting procedures

A relevant person must establish, document, maintain and operate reporting procedures that, in relation to its business in the regulated sector, will —

(a) enable all its directors or, as the case may be, partners, all other persons involved in its management, and all appropriate employees and workers to know to whom they should report any knowledge or suspicion of ML/FT activity;

(b) ensure that there is a clear reporting chain under which that knowledge or suspicion will be passed to the MLRO;

(c) require reports to be made to the MLRO ("**internal disclosures**") of any information or other matters that come to the attention of the person handling that business and which in that person's opinion gives rise to any knowledge or suspicion that another person is engaged in ML/FT activity;

(d) require the MLRO to consider any report in the light of all other relevant information available to the MLRO for the purpose of determining whether or not it gives rise to any knowledge or suspicion of ML/FT activity;

(e) ensure that the MLRO has full access to any other information that may be of assistance and that is available to the relevant person; and

(f) enable the information or other matters contained in a report ("**external disclosure**") to be provided as soon as is practicable to a constable who is for the time being serving with the Financial Crime Unit if the MLRO knows or suspects that another is engaged in ML/FT activity.

27 Internal disclosures

(1) Where a relevant person identifies any suspicious activity in the course of a business relationship or occasional transaction the relevant person must —

(a) consider obtaining enhanced customer due diligence in accordance with paragraph 15; and

(b) make an internal disclosure in accordance with the procedures established under paragraph 26.

(2) Where a relevant person identifies any unusual activity in the course of a business relationship or occasional transaction the relevant person must —

(a) perform appropriate scrutiny of the activity;

(b) obtain enhanced customer due diligence in accordance with paragraph 15; and

(c) consider whether to make an internal disclosure in accordance with the reporting procedures established under paragraph 26.

28 External disclosures

(1) Where an internal disclosure has been made, the MLRO must assess the information contained within the disclosure to determine whether there are reasonable grounds for knowing or suspecting that the activity is related to ML/FT.

(2) The MLRO must make an external disclosure in accordance with the reporting procedures established under paragraph 26 as soon as is practicable to a constable who is for the time being serving with the Financial Crime Unit if the MLRO —

(a) knows or suspects; or

(b) has reasonable grounds for knowing or suspecting,

that another is engaged in ML/FT.

PART 8 – COMPLIANCE

29 Monitoring and testing compliance

A relevant person must maintain appropriate procedures for monitoring and testing compliance with the AML/CFT requirements, having regard to ensuring that —

(a) the relevant person has robust and documented arrangements for managing the risks identified by the business risk assessment conducted in accordance with paragraph 6 for compliance with those requirements;

(b) the operational performance of those arrangements is suitably monitored; and

(c) prompt action is taken to remedy any deficiencies in arrangements.

30 New staff appointments

A relevant person must establish, maintain and operate appropriate procedures to enable the relevant person to satisfy itself of the integrity of new directors, officers or partners (as the case may be) of the relevant person and of all new appropriate employees and workers.

31 Staff training

A relevant person must provide or arrange education and training, including refresher training, at least annually, for all directors, officers or, as the case may be, partners, all other persons involved in its management, all key staff and appropriate employees and workers to ensure that they are aware of —

(a) the provisions of the AML/CFT requirements;

(b) their personal obligations in relation to the AML/CFT requirements;

(c) the reporting procedures established under paragraph 26;

(d) the relevant person's policies and procedures for AML/CFT;

(e) the relevant person's customer due diligence, record-keeping and other procedures;

(f) the recognition and handling of transactions and attempted transactions that may give rise to an internal disclosure;

(g) their personal liability for failure to report information or suspicions in accordance with internal procedures, including the offence of tipping off; and

(h) new developments, including information on current techniques, methods and trends in ML/FT.

32 Record keeping

A relevant person must keep —

(a) a copy of the documents obtained or produced under parts 3 to 6, and paragraphs 37 and 39 or information that enables a copy of such documents to be obtained;

(b) a record of all transactions carried out in the course of business in the regulated sector, including identification information, account files, business correspondence records and the results of any analysis undertaken; and

(c) such other records as are sufficient to permit reconstruction of individual transactions and compliance with this Code.

33 Record retention

(1) A relevant person must keep the records required by this Code for at least 5 years—

(a) in the case of records required by paragraph 32(b), from the date of the completion of the transaction; and

(b) in other cases, from the date when —

(i) all activities relating to an occasional transaction or a series of linked transactions were completed; or
(ii) in respect of other activities —

(A) the business relationship was formally ended; or

(B) if the business relationship was not formally ended, when all activities relating to the transaction were completed.

(2) Without limiting sub-paragraph (1), if —

(a) a report has been made to a constable under paragraphs 26(1)(f) and 28;

(b) the relevant person knows or believes that a matter is under investigation by a competent authority; or

(c) the relevant person becomes aware that a request for information or an enquiry is underway by a competent authority,

the relevant person must retain all relevant records for as long as required by the constable or competent authority as the case may be.

34 Record format and retrieval

(1) In the case of any records required to be established and maintained under this Code —

(a) if the records are in the form of hard copies kept in the Island, the relevant person must ensure that they are capable of retrieval without undue delay;

(b) if the records are in the form of hard copies kept outside the Island, the relevant person must ensure that the copies can be sent to the Island and made available within 7 working days; and

(c) if the records are not in the form of hard copies (such as records kept on a computer system), the relevant person must ensure that they are readily accessible in or from the Island and that they are capable of retrieval without undue delay.

(2) A relevant person may rely on the records of a third party in respect of the details of payments and transactions by customers if it is satisfied that the third party will —

(a) produce copies of the records on request; and

(b) notify the relevant person if the third party is no longer able to produce copies of the records on request.

35 Registers of internal and external disclosures

(1) A relevant person must establish and maintain separate registers of —

(a) all internal disclosures; and

(b) all external disclosures.

(2) The registers of internal disclosures and external disclosures may be contained in a single document if the details required to be included in those registers under sub-paragraph (3) can be presented separately for internal disclosures and external disclosures upon request by a competent authority.

(3) The registers must include details of —

(a) the date on which the report is made;

(b) the person who makes the report;

(c) for internal disclosures, whether it is made to the MLRO or deputy MLRO;

(d) for external disclosures, the constable's name; and

(e) information sufficient to identify the relevant papers.

36 Register of money laundering and financing of terrorism enquiries

(1) A relevant person must establish and maintain a register of all ML/FT enquiries made of it by law enforcement or other competent authorities.

(2) The register must be kept separate from other records and include —

(a) the date of the enquiry;

(b) the nature of the enquiry;

(c) the name and agency of the enquiring officer;

(d) the powers being exercised; and

(e) details of the accounts or transactions involved.

PART 9 – MISCELLANEOUS

37 Foreign branches and subsidiaries

(1) A relevant person must ensure that any branch or subsidiary in a jurisdiction outside the Island takes measures consistent with this Code and guidance issued by a competent authority for AML/CFT, to the extent permitted by that jurisdiction's laws.

(2) If the minimum measures for AML/CFT in such a jurisdiction differ from those required by the law of the Island, the relevant person must ensure that any branch or subsidiary in that jurisdiction applies the higher standard, to the extent permitted by that jurisdiction's laws.

(3) The relevant person must inform the relevant competent authority when a branch or subsidiary is unable to take any of the measures referred to in sub-paragraphs (1) or (2) because it is prohibited by the laws of the jurisdiction concerned.

(4) In this paragraph "**subsidiary**", in relation to a relevant person, means a legal person more than half of whose equity share capital is owned by the relevant person.

38 Shell banks

(1) A relevant person must not enter into or continue a business relationship or occasional transaction with a shell bank.

(2) A relevant person must take adequate measures to ensure that it does not enter into or continue a business relationship or occasional transaction with a respondent institution that permits its accounts to be used by a shell bank.

39 Correspondent services

(1) This paragraph applies to a business relationship or occasional transaction, as the case may be, which involves correspondent services or similar arrangements.

(2) A relevant person must not enter into or continue a business relationship or occasional transaction to which this paragraph applies with a financial institution or designated business in another jurisdiction unless it is satisfied that the respondent institution or designated business does not permit its accounts to be used by shell banks.

(3) Before entering into a business relationship or occasional transaction to which this paragraph applies, a relevant person must —

(a) obtain sufficient information about the respondent institution or designated business to understand fully the nature of its business;

(b) determine from publicly available information —

(i) the reputation of the respondent institution or designated business;
(ii) the quality of the supervision to which it is subject; and
(iii) whether it has been subject to investigation or regulatory action in respect of ML/FT;

(c) assess the AML/CFT procedures and controls maintained by the respondent institution or designated business, and ascertain that they are adequate and effective;

(d) ensure that the approval of the relevant person's senior management is obtained; and

(e) clearly understand the respective responsibilities of the relevant person and the respondent institution or designated business with respect to AML/CFT measures.

(4) If a business relationship or occasional transaction to which this paragraph applies involves a payable-through account, a relevant person must be satisfied that the respondent institution or designated business —

(a) has taken measures that comply with the requirements of the FATF Recommendations 10 and 11 (customer due diligence and record keeping) with respect to every customer having direct access to the account; and

(b) will provide the relevant person on request with relevant evidence of identity of the customer.

40 Fictitious, anonymous and numbered accounts

(1) Subject to sub-paragraph (2), a relevant person must not set up or maintain an anonymous account or an account in a name that it knows, or has reasonable cause to suspect, to be fictitious for any new or existing customer.

(2) Sub-paragraph (1) does not apply for an account already maintained where the account is included in the list kept by the Insurance and Pensions Authority specifically for this purpose.

PART 10 – OFFENCES AND REVOCATIONS

41 Offences

(1) A person who contravenes requirements of this Code is guilty of an offence and liable —

(a) on summary conviction to custody for a term not exceeding 12 months or to a fine not exceeding £5,000, or to both;

(b) on conviction on information, to custody not exceeding 2 years or to a fine, or to both.

(2) In determining whether a person has complied with any of the requirements of this Code, a court may take account of —

(a) any relevant supervisory or regulatory guidance given by a competent authority that applies to that person; or

(b) in a case where no guidance falling within (a) applies, any other relevant guidance issued by a body that regulates, or is representative of, any trade, business, profession or employment carried on by that person.

(3) In proceedings against a person for an offence under this paragraph, it is a defence for the person to show that it took all reasonable measures to avoid committing the offence.

(4) If an offence under this paragraph is committed by a body corporate or foundation and it is proved that the offence —

(a) was committed with the consent or connivance of; or

(b) was attributable to neglect on the part of,

an officer of the body, the officer, as well as the body, is guilty of the offence and liable to the penalty provided for it.

(5) If an offence under this paragraph is committed by a partnership that does not have legal personality, or by an association other than a partnership or body corporate, and it is proved that the offence —

(a) was committed with the consent or connivance of; or

(b) was attributable to neglect on the part of,

a partner in the partnership or (as the case may be) a person concerned in the management or control of the association, the partner or (as the case may be) the person concerned, as well as the partnership or association, is guilty of the offence and liable to the penalty provided for it.

(6) In this paragraph "officer" also includes —

(a) a director, manager or secretary;

(b) a person purporting to act as a director, manager or secretary; and

(c) a member, if the affairs of the body are managed by its members.

42 Revocations

The following are revoked —

(a) Money Laundering and Terrorist Financing Code 2013 ; and

(b) Money Laundering and Terrorist Financing (Amendment) Code 2013 .

MADE 26 FEBRUARY 2015

J P WATTERSON
Minister for Home Affairs

EXPLANATORY NOTE

(This note is not part of the Code)

This Code revokes and replaces the Money Laundering and Terrorist Financing Code 2013. This Code is made jointly under section 157 of the Proceeds of Crime Act 2008 and section 68 of the Terrorism and Other Crime (Financial Restrictions) Act 2014. It contains provisions in line with the Financial Action Task Force's Recommendations on preventing money laundering and the financing of terrorism. Failure to comply with the requirements of this Code is an offence

Appendix B

Proceeds of Crime (Business in the Regulated Sector) Order 2014

Statutory Document No. 2015/0073

Proceeds of Crime Act 2008

PROCEEDS OF CRIME (BUSINESS IN THE REGULATED SECTOR) ORDER 2015

Approved by Tynwald: 17 March 2015
Coming into Operation: 1 April 2015

The Department of Home Affairs makes the following Order under paragraph 3 of Schedule 4 to the Proceeds of Crime Act 2008.

1 Title

This Order is the Proceeds of Crime (Business in the Regulated Sector) Order 2015.

2 Commencement

If approved by Tynwald, this Order comes into operation on 1 April 2015[1].

3 Amendment of Schedule 4 to the Proceeds of Crime Act 2008

For paragraph 1 (business in the regulated sector) of Schedule 4 to the Proceeds of Crime Act 2008 substitute the text set out in the Schedule to this Order.

4 Revocation

The Proceeds of Crime (Business in the Regulated Sector) Order 2013 is revoked[2].

[1] Tynwald approval is required by section 223 of the Proceeds of Crime Act 2008.
[2] SD 2013/0097.

MADE 17 FEBRUARY 2015

JUAN WATTERSON
Minister for Home Affairs

SCHEDULE

[Article 3]

AMENDMENT OF SCHEDULE 4 TO THE PROCEEDS OF CRIME ACT 2008

«1 Business in the regulated sector

(1) A business is in the regulated sector to the extent it consists of —

(a) business carried on by a building society within the meaning of section 7 of the *Industrial and Building Societies Act 1892*;

(b) business carried on by a society (other than a building society or credit union) registered under the *Industrial and Building Societies Act 1892*;

(c) any activity carried on for the purpose of raising money authorised to be borrowed under the *Isle of Man Loans Act 1974*;

(d) the business of an estate agent within the meaning of the *Estate Agents Act 1975*;

(e) the provision by way of business of audit services in respect of a body corporate;

(f) the business of an external accountant, where "**external accountant**" means any person who, by way of business, provides accountancy services to third parties. However, "external accountant" does not include accountants employed by —

(i) public authorities; or
(ii) undertakings which do not by way of business provide accountancy services to third parties;

and, for the avoidance of doubt, does not include an employed person whose duties relate solely to the provision of accountancy services to his or her employer;

(g) any activity which is specified in sub-paragraph (h) that is undertaken by —

(i) an advocate within the meaning of the *Advocates Act 1976*;
(ii) a registered legal practitioner within the meaning of the *Legal Practitioners Registration Act 1986*;
(iii) a notary public within the meaning of the *Advocates Act 1995* and the *Notaries Regulations 2000*[3] ; or

[3] SD 671/00 as amended by SD 0850/02

(iv) any other legal professional who by way of business provides legal services to third parties,

except for any such persons who are employed by public authorities or undertakings which do not by way of business provide legal services to third parties;

(h) when undertaken by a person referred to in subparagraph (g) —

(i) managing any assets belonging to a client;
(ii) the provision of legal services which involves participation in a financial or real property transaction (whether by assisting in the planning or execution of any such transaction or otherwise) by acting for, or on behalf of, a client in respect of —

(A) the sale or purchase of land;

(B) managing bank, savings or security accounts;

(C) organising contributions for the promotion, formation, operation or management of bodies corporate;

(D) the sale or purchase of a business; or

(E) the creation, operation or management of a legal person or legal arrangement;

(i) insurance business within the meaning of the *Insurance Act 2008*;

(j) the business of acting as an insurance manager for or in relation to an insurer within the meaning of the *Insurance Act 2008*;

(k) the business of insurance intermediary within the meaning of the *Insurance Act 2008*;

(l) any activity permitted to be carried on by a licence holder under a casino licence granted under the *Casino Act 1986* or on premises in respect of which a temporary premises certificate is in issue under Part IIA of that Act;

(m) a collective investment scheme within the meaning of section 1 of the *Collective Investment Schemes Act 2008*;

(n) the business of a bookmaker within the meaning of the *Gaming, Betting and Lotteries Act 1988*;

(o) the business of providing online gambling within the meaning of section 1 of the *Online Gambling Regulation Act 2001*;

(p) the business of engaging in any regulated activity within the meaning of the *Financial Services Act 2008*;

(q) investment business within the meaning of section 3 of the *Financial Services Act 2008* and Class 2 of Schedule 1 to the Regulated Activities Order 2011[4] whether or not exclusions or exemptions contained within the Order or the Financial Services (Exemptions) Regulations 2011[5] apply;

(r) corporate services or trust services within the meaning of section 3 of the *Financial Services Act 2008* and Classes 4 and 5 of Schedule 1 to the Regulated Activities Order 2011 whether or not exclusions or exemptions for that class contained within the Order or the Financial Services (Exemptions) Regulations 2011 apply;

(s) deposit taking within the meaning of section 3 of the *Financial Services Act 2008* and Class 1 of Schedule 1 to the Regulated Activities Order 2011 whether or not exclusions or exemptions for that class contained within the Order or the Financial Services (Exemptions) Regulations 2011 apply;

(t) business carried on by a society registered as a credit union within the meaning of the *Credit Unions Act 1993*;

(u) acting as a retirement benefits schemes administrator within the meaning of Part 6 of the *Retirement Benefits Schemes Act 2000*;

(v) acting by way of business as the trustee of a retirement benefits scheme within the meaning of the *Retirement Benefits Schemes Act 2000*;

(w) any activity carried on for the purpose of raising money by a local authority;

(x) the business of a *bureau de change*;

(y) the business of the Post Office in respect of any activity undertaken on behalf of the National Savings Bank;

(z) any activity involving money (including any representation of monetary value) transmission services or cheque encashment facilities;

(aa) the provision of safe custody facilities for cash or liquid securities on behalf of other persons;

[4] SD 0884/11 as amended by SD 0373/13.
[5] SD 0885/11 as amended by SD 0374/13.

(bb) the business of dealing in goods of any description (including dealing as an auctioneer) whenever a transaction involves accepting a total cash payment of euro 15,000 or more;

(cc) administering or managing money on behalf of other persons;

(dd) services to collective investment schemes as defined in section 3 of the *Financial Services Act 2008* and Class 3 of Schedule 1 to the Regulated Activities Order 2011 whether or not exclusions or exemptions for that class contained within the Order or the Financial Services (Exemptions) Regulations 2011[6] apply;

(ee) any business involving the issuing and managing of means of payment (including but not limited to credit and debit cards, cheques, traveller's cheques, money orders, bankers' drafts and electronic money);

(ff) subject to paragraph (4), the business of lending including, but not limited to, consumer credit, mortgage credit, factoring and the finance of commercial transactions in respect of products other than consumer products for and on behalf of customers;

(gg) subject to paragraph (4), the business of providing financial leasing arrangements in respect of products other than consumer products for and on behalf of customers;

(hh) subject to paragraph (4), the business of providing financial guarantees and commitments in respect of products other than consumer products for and on behalf of customers;

(ii) subject to paragraph (5), the provision of safe custody facilities, deposit boxes or other secure storage facilities suitable for high-value physical items or assets, jewellery, precious metals and stones, bullion or documents of title;

(jj) the business of a tax adviser as defined by the *Income Tax Act 1970*;

(kk) the activity of a specified non-profit organisation;

(ll) the business of a payroll agent;

(mm) the business of issuing, transmitting, transferring, providing safe custody or storage of, administering, managing, lending, buying, selling, exchanging or otherwise trading or intermediating convertible virtual currencies, including crypto-currencies or similar concepts where the concept is accepted by persons as a means of payment for goods or services, a unit of account, a store of value or a commodity;

[6] SD 0885/11.

(nn) the business of selling or supplying controlled machines within the meaning of the *Gaming (Amendment) Act 1984*.

(2) A business is not in the regulated sector by reason of the provisions of subparagraph (1)(h)(i) in relation to managing any assets belonging to a client where those assets only represent advance payment of fees.

(3) A business is not in the regulated sector by reason of the provisions of subparagraphs (1)(p) or (r) in relation only to the service of the conveyance of letters, documents or parcels or communication by post or any other means.

(4) A business is not in the regulated sector by reason only of the provisions of subparagraphs (1)(ff), (gg) or (hh) if the lending, leasing or provision of guarantees or commitments (as the case may be) is made by —

(a) a parent undertaking to a subsidiary of that parent undertaking;

(b) a subsidiary of a parent undertaking to the parent undertaking; or

(c) a subsidiary of a parent undertaking to another subsidiary of that parent undertaking.

(5) A business is not in the regulated sector by reason only of the provisions of subparagraph (1)(ii) if the services provided are —

(a) the storage of goods such as luggage, household items or motor vehicles;

(b) the storage of non-physical property such as computer data;

(c) the secure transportation of high value items;

(d) the offering of safe custody on an occasional or very limited basis, such as hotels providing a safe for use by guests; or

(e) legal professionals storing legal documents other than documents of title.

(6) For the purposes of subparagraph (1) —

"higher risk jurisdiction" is a jurisdiction which the business in the regulated sector determines presents a higher risk of money laundering, the financing of terrorism or of proliferation having considered any relevant guidance;

"payroll agent" is a person that is involved with the payment of earnings to or for the benefit of any individual, where the payroll agent is not that individual's employer, but does not include services provided by technical service providers, which support the provision of payment services, without the technical services provider entering at any time into possession of the funds to be transferred;

"specified non-profit organisation" means a body corporate or other legal person, the trustees of a trust, a partnership, other unincorporated association or organisation or any equivalent or similar structure or arrangement, established solely or primarily to raise or distribute funds for charitable, religious, cultural, educational, political, social or fraternal purposes with the intention of benefiting the public or a section of the public and which has —

(a) an annual or anticipated annual income of £5,000 or more; and

(b) remitted, or is anticipated to remit, at least 30% of its income in any one financial year to one or more ultimate recipients in or from one or more higher risk jurisdictions;

"technical service provider" means a person that supports the provision of payment services by providing services including (but not limited to) services of the following kinds, but that does not, at any time, possess the funds to be transferred —

(a) the processing and storage of data;

(b) trust and privacy protection services;

(c) data and entity authentication;

(d) information technology and communication network provision; and

(e) the provision and maintenance of terminals and devices used for payment services.

(7) For the purposes of subparagraph (4) —

"parent undertaking" means an undertaking which, in relation to another undertaking (a "subsidiary") —

(a) owns or controls, whether directly or indirectly, shares or other interests in the subsidiary together aggregating in excess of 50 per cent of the votes exercisable at general or other meetings of the subsidiary on any or all matters;

(b) has a right to appoint or remove a majority of its board of directors, or other governing body;

(c) has the right to exercise a dominant influence over the subsidiary —

(i) by virtue of the provisions contained in the subsidiary's constitutional documents, or
(ii) by virtue of a control contract; or

(d) controls, alone or pursuant to an agreement with other persons, a majority of the voting rights in the subsidiary; and

"undertaking" means a natural person, body corporate, trustees of a trust, partnership, foundation or unincorporated association.

(8) For the purpose of subparagraph (7) —

(a) an undertaking is taken to have the right to exercise a dominant influence over another undertaking only if it has a right to give directions with respect to the operating and financial policies of that other undertaking with which its directors are, or governing body is, obliged to comply whether or not they are for the benefit of that other undertaking;

(b) a "control contract" means a contract in writing conferring a dominant influence right which —

(i) is of a kind authorised by the constitutional documents of the undertaking in relating to which the right is exercisable; and
(ii) is permitted by the law under which that undertaking is established; and

(c) any undertaking which is a subsidiary of another undertaking is also a subsidiary of any further undertaking of which that other is a subsidiary.».

EXPLANATORY NOTE

(This note is not part of the Order)

This Order replaces paragraph 1 of Schedule 4 to the Proceeds of Crime Act 2008 (the Act). That paragraph sets out the list of businesses that are businesses in the regulated sector for the purposes of the Act. The substituted paragraph 1 updates the list to ensure that all relevant persons are subject to the anti-money laundering and control of terrorist financing provisions of the Act.

The main change made in the substituted paragraph 1 is the inclusion of certain categories of business that pose a higher potential money laundering and terrorist financing risk. This change will aid the Island in meeting its obligations under international requirements.

Appendix C

LIST C: Equivalent Jurisdiction List

Below is a list of countries which the Island has judged to have equivalent AML/CFT controls to our framework. Customers resident in, or carrying on business from, countries on this list may be subject to simplified due diligence concessions as outlined in Part 6 of the Code.

Australia	Japan
Austria	Jersey
Belgium	Liechtenstein
Bermuda	Luxembourg
British Virgin Islands	Malta
Canada	Mauritius
Cayman Islands	Monaco
Cyprus	Netherlands
Denmark	New Zealand
Finland	Norway
France	Portugal
Germany	Singapore
Gibraltar	South Africa
Guernsey	Spain
Hong Kong	Sweden
Iceland	Switzerland
Ireland	Taiwan
Italy	United Kingdom
	United States

Appendix D(a)

LIST A: High Risk Jurisdiction List

This Appendix covers countries and territories that are to be treated as countries and territories that do not apply, or insufficiently apply, the FATF Recommendations. Consequently, business relationships and occasional transactions with persons or legal arrangements resident or located in such jurisdictions pose a higher risk and must be subject to enhanced customer due diligence.

This Appendix provides details of FATF statements or statements made by other relevant international bodies, with respect to inadequate implementation of anti-money laundering and counter the financing of terrorism standards in such jurisdictions.

This Appendix is not intended to provide an exhaustive list and no conclusion should be drawn from the omission of a particular jurisdiction. Furthermore, there may be additional jurisdictions where the FATF Recommendations are not applied or insufficiently applied in respect of particular transactions or business relationships.

This Appendix will be updated as and when the IOMFSA becomes aware of necessary amendments.

Jurisdiction	Issuing Body	Warning Type	Date of most recent warning
Democratic People's Republic of Korea	FATF	Counter Measures	~~November 2017~~February 2018
Iran	FATF	Enhanced Due Diligence	~~November 2017~~February 2018

FATF Countermeasures

The Non-Cooperative Countries and Territories ("NCCTs") exercise began in 1998 at a time when many countries around the world did not have adequate AML measures in place. The goal of the initiative was to secure the adoption by all financial centres of international standards to prevent, detect and punish money laundering and thereby effectively cooperate internationally in the global fight against money laundering. Financial services businesses will be aware that no countries or territories are currently listed by FATF as non-cooperative.

To ensure continued effective implementation of the reforms enacted, the FATF adopted a monitoring mechanism. This mechanism included the submission of regular implementation reports and a possible follow-up visit to assess progress in implementing reforms and to ensure that stated goals had been fully achieved.

The following are jurisdictions subject to a FATF call on its members and other jurisdictions to apply counter-measures to protect the international financial system from the ongoing and substantial money laundering and terrorist financing risks emanating from the jurisdictions.

Democratic People's Republic of Korea

For statements prior to 2012 please see the FATF website

FATF Statement of 22 June 2012
FATF Statement of 19 October 2012
FATF Statement of 22 February 2013
FATF Statement of 21 June 2013
FATF Statement of 18 October 2013
FATF Statement of 14 February 2014
FATF Statement of 27 June 2014
FATF Statement of 24 October 2014
FATF Statement of 27 February 2015
FATF Statement of 26 June 2015
FATF Statement of 23 October 2015
FATF Statement of 19 February 2016
FATF Statement of 24 June 2016
FATF Statement of 21 October 2016
FATF Statement of 24 February 2017
FATF Statement of 23 June 2017
FATF Statement of 3 November 2017
FATF Statement of 23 February 2018

Enhanced Due Diligence

The following are jurisdictions subject to a FATF call on its members and other jurisdictions to apply enhanced due diligence measures proportionate to the risks arising from the jurisdictions.

Iran

For statements prior to 2012 please see the FATF website

FATF Statement of 22 June 2012
FATF Statement of 19 October 2012
FATF Statement of 22 February 2013
FATF Statement of 21 June 2013
FATF Statement of 18 October 2013
FATF Statement of 14 February 2014
FATF Statement of 27 June 2014
FATF Statement of 24 October 2014
FATF Statement of 27 February 2015
FATF Statement of 26 June 2015
FATF Statement of 23 October 2015
FATF Statement of 19 February 2016
FATF Statement of 24 June 2016
FATF Statement of 21 October 2016
FATF Statement of 24 February 2017
FATF Statement of 23 June 2017

FATF Statement of 3 November 2017
FATF Statement of 23 February 2018

Appendix D(b)

List B: Jurisdictions that May Pose a Higher Risk

This Appendix covers countries and territories that may pose a higher risk of money laundering or terrorist financing. Relevant persons should consider the statements issued as part of their risk assessment and consider whether enhanced due diligence would be appropriate.

Insufficient progress

The FATF statement of 23 February 2018~~FATF statement of 3 November 2017~~identified a number of jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies.

Ongoing process

The FATF statement entitled "Improving Global AML/CFT Compliance: ongoing process",, issued on the 18 February 2010 (updated at each FATF Plenary since, with the latest update being on ~~3 November 2017~~23 February 2018) identifies a number of jurisdictions as having strategic AML/CFT deficiencies for which they have developed an action plan with the FATF. It also identifies a number of jurisdictions as not having made sufficient progress on their action plans agreed with the FATF. Relevant persons' attention is drawn to this statement.

More information on each of the FATF lists is provided below.

Jurisdiction	Issuing Body	Warning Type	Date of most recent warning
~~Bosnia and Herzegovina~~	~~FATF~~	~~Ongoing process~~	~~3 November 2017~~
Ethiopia	FATF	Ongoing process	~~3 November 2017~~ 23 February 2018
Iraq	FATF	Ongoing process	23 February 2018~~3 November 2017~~
Serbia	FATF	Ongoing process	23 February 2018
Sri Lanka	FATF	Ongoing process	23 February 2018~~3 November 2017~~
Syria	FATF	Ongoing process	23 February 2018~~3 November 2017~~
Trinidad and Tobago	FATF	Ongoing process	23 February 2018~~3 November 2017~~
Tunisia	FATF	Ongoing process	23 February 2018~~3 November 2017~~
Vanuatu	FATF	Ongoing process	23 February 2018~~3 November 2017~~
Yemen	FATF	Ongoing process	23 February 2018~~3 November 2017~~

The following jurisdictions listed below have also been identified as those that may pose **a higher risk of money laundering ("ML") or terrorist financing ("TF"). This list is as of ~~December 2017~~April 2018.**

Jurisdiction	Risk Type	Jurisdiction	Risk Type
Afghanistan	ML & TF	Mali	ML & TF
Angola	TF	Mozambique	ML
Algeria	TF	Myanmar	ML
Bangladesh	TF	Nepal	ML
Benin	ML	Niger	ML & TF
Bolivia	ML	Nigeria	TF
Burkina Faso	ML & TF	North Korea	TF
Burundi	TF	Pakistan	TF
Cambodia	ML	Palestinian Territory	TF
Cameroon	TF	Panama	ML
Central African Republic	TF	Paraguay	ML
Chad	TF	Philippines	TF
Colombia	TF	Sao Tome and Principe	ML
Côte d'Ivoire	TF	Saudi Arabia	TF
Democratic Republic of the Congo	TF	Sierra Leone	ML
Egypt	TF	Somalia	TF
Eritrea	TF	Sri Lanka	ML
Ethiopia	TF	South Sudan	TF
Gambia	TF	Sudan	ML & TF
Guinea	TF	Syria	TF
Guinea Bissau	ML & TF	Tajikistan	ML
Haiti	ML & TF	Tanzania	ML
India	TF	Tunisia	TF
Indonesia	TF	Turkey	TF
Iraq	TF	Ukraine	TF
Israel	TF	Uganda	ML & TF
Kenya	ML & TF	Vanuatu	ML
Laos	ML	Venezuela	TF
Lebanon	ML & TF	Vietnam	ML
Lesotho	ML	Yemen	TF
Liberia	ML	Zambia	ML
Libya	TF	Zimbabwe	TF
Madagascar	TF		

Appendix E

Eligible Introducers Certificate (includes terms of business)

EIC 1.1 - ELIGIBLE INTRODUCER'S CERTIFICATE

Customer name (in full)	

Name of Accepting Business	
Name of Eligible Introducer	
Eligible Introducer's contact details	Address:
Telephone:	E-mail:
Eligible Introducer's Regulatory / Supervisory / Professional Body	

The Eligible Introducer certifies that it is one of the following:-
(Please tick the applicable box)

1	A regulated person*	
2	An advocate within the meaning of the Advocates Act 1976, a registered legal practitioner within the meaning of the Legal Practitioners Registration Act 1986, or an accountant carrying on business in or from the Isle of Man, where the professional body's rules embody requirements and procedures equivalent to the Anti-Money Laundering and Terrorist Financing Code 2015 ("the Code").	
3	A person who acts in the course of external regulated business and is regulated under the law of a jurisdiction in List C of the Code, unless the relevant person has reason to believe that the jurisdiction in question does not apply, or insufficiently applies, the FATF recommendations in respect of the business of that person. Specify which country ……	
4	A body corporate within the same group as the customer(s)	

* - Please refer to the Notes and Guidance at EIC 6.1 to 6.4

EIC 1.2 - ELIGIBLE INTRODUCER'S CERTIFICATE (CONT'd)

The Eligible Introducer also certifies that in respect of this customer it has obtained the verification required to satisfy the requirements of the Code and this Handbook. The information disclosed for this customer by the Eligible Introducer accurately reflects the information held and is being given for business opening and maintenance purposes only. The Eligible Introducer undertakes to supply suitably certified copies*, originals of the verification documentation or copies of verified electronic documents* forthwith upon request. The Eligible Introducer confirms that he/she will comply with the requirements of paragraph 23(6) and 23(8) of the Code. The Eligible Introducer also confirms that it is not itself reliant upon a third party for the evidence of identity of the customer.

Signature*:	
Full Name:	
Official Position:	
Date:	
Contact details of Signatory:	Address:
Telephone:	E-mail:

Please identify the number of supplementary pages being submitted.

EIC 2 ☐ EIC 3 ☐ EIC 4 ☐ EIC 5 ☐

* - Please refer to the Notes and Guidance at EIC 6.1 to 6.4

EIC 2.1 – IDENTIFICATION INFORMATION

Name of Eligible Introducer	

Customer name (in full)	
Details of associated entities or relationships* (which are part of the same structure) **Please provide a structure chart if available.**	

To be completed for customers who are individuals or partners in a partnership only
(Please complete section below and attach additional copies of this sheet as required)

	Individual 1	**Individual 2**
Legal name, any former names and any other names used		
Gender, nationality, date and place of birth, national identification number		
Permanent residential address including post code. (PO Box only address is insufficient)		
Does the Eligible Introducer consider the related party to be, or associated with, a Politically Exposed Person*?	Yes ☐ No ☐	Yes ☐ No ☐

To be completed for applicants for business who are legal persons or legal arrangements.

Name of entity / any trading names / name of trust		
Official identification number where applicable		
(if a legal person): Date and country of incorporation and registration number		Are bearer shares* currently in issue? Yes ☐ No ☐

EIC 2.2 – IDENTIFICATION INFORMATION (CONT'd)

(if a legal person): Whether listed and where		
(if a legal person): Registered office address, place of business and mailing address if different		
(if a legal arrangement): Date of establishment, legal jurisdiction and if applicable registration number and business address		
Type of trust / foundation / company*		Is it a trading entity? Yes ☐ No ☐
Name of regulator if applicable		

Initials of signatory completing EIC1

☐

Date

* - Please refer to the Notes and Guidance at EIC 6.1 to 6.4

EIC 3.1 – RELATED PARTIES

Name of Eligible Introducer	

Customer name (in full)	

Names of Directors / Trustees (or equivalent if a foundation) (including those who are officers of the Eligible Introducer)

Full name	
Full name	
Full name	
Full name	
Full name	
Full name	

Details of all principal(s)* including beneficial owners but excluding officers of the Eligible Introducer

	1	**2**
Legal name, any former names and any other names used		
Gender, nationality, date and place of birth, national identification number		
Permanent residential address including post code. (PO Box only address is insufficient)		
Role* of principal and date relationship commenced		
Does the Eligible Introducer consider the related party to be, or associated with, a Politically Exposed Person*?	Yes ☐ No ☐	Yes ☐ No ☐

* - Please refer to the Notes and Guidance at EIC 6.1 to 6.4

Initials of signatory completing EIC ☐

Date

EIC 3.2 – RELATED PARTIES (CONT'd)

Name of Eligible Introducer	

Customer name (in full)	

Details of all principal(s)* including beneficial owners but excluding officers of the Eligible Introducer

(Please complete section below and attach additional copies of this sheet as required)

	3	4
Legal name, any former names and any other names used		
Gender, Nationality, date and place of birth, national identification number		
Permanent residential address including post code. (PO Box only address is insufficient)		
Role* of principal and date relationship commenced		
Does the Eligible Introducer consider the related party to be, or associated with, a Politically Exposed Person*?	Yes ☐ No ☐	Yes ☐ No ☐

Initials of signatory completing EIC1

☐

Date

* - Please refer to the Notes and Guidance at EIC 6.1 to 6.4

EIC 4.1 – RELATIONSHIP INFORMATION

Name of Eligible Introducer	

Customer name (in full)	

To be completed for all customers

Purpose / intended nature of business relationship* (please provide a full description)	
Expected type, volume and value of activity	
Activity providing the source of funds for the relationship and geographical sphere of the activity	
Source of funds*	
Source of wealth (if held)* (please identify the period over which this has been derived)	

Should the space provided be insufficient, please continue using EIC 5.1.

* - Please refer to the Notes and Guidance at EIC 6.1 to 6.4

Initials of signatory completing EIC1
Date

EIC 5.1 – ADDITIONAL INFORMATION

Name of Eligible Introducer	

Customer name (in full)	

This section is to be used by the accepting business to identify any additional information or documentation that they require over and above the stated minimum and/or for the Eligible Introducer to provide additional information to supplement the details already provided.

Initials of signatory completing EIC1
Date

* - Please refer to the Notes and Guidance at EIC 6.1 to 6.4

EIC 6.1 – ADDITIONAL INFORMATION

This Eligible Introducer's Certificate aims to streamline and provide a standard format for the use of the Eligible Introducer system. It was prepared by the Isle of Man Financial Services Authority in conjunction with the Isle of Man Joint Anti-Money Laundering Advisory Group ("JAMLAG").

These notes and the definitions below are intended to provide guidance to assist the Eligible Introducer in completing the required forms and to enable greater consistency to be achieved.

"Associated entities or relationships"

Other business relationships established by the Eligible Introducer with the accepting business which are associated with the applicant for business or any of its principals.

"Bearer Shares"

Should bearer shares be subsequently issued (after the opening of the account) such that the "Yes" box needs ticking in EIC 2.1, an updated form should be supplied to the accepting financial services business without delay.

"Certified copy"

An officer or authorised signatory of a regulated financial service business will be a suitable certifier. An acceptable "certified copy" document should be an accurate and complete copy of the original such that the certifier will sign and date the copy document (printing his name clearly in capitals underneath) and clearly indicate his position or capacity on it and provide his contact details. The certifier must state that it is a true copy of the original as per Section 4.10 of the AML/CFT Handbook.

"Paragraphs 23(6) and 23(8) Isle of Man's Anti-Money Laundering and Countering the Financing of Terrorism Code 2015"

Paragraph 23(6) of the Code reads as follows:

The relevant person must not enter into a business relationship with a customer that is introduced by an introducer unless written terms of business are in place between the relevant person and the introducer and, despite sub-paragraphs (4) and (5), those terms of business require in all cases the introducer to —

(a) verify the identity of all customers introduced to the relevant person sufficiently to comply with the AML/CFT requirements;
(b) take reasonable measures to verify the identity of the beneficial owner (if any);
(c) establish and maintain a record of the evidence of identity for at least 5 years calculated in accordance with paragraph 33(1);
(d) establish and maintain records of all transactions between the introducer and the customer if the records are concerned with or arise out of the introduction (whether directly or indirectly) for at least 5 years calculated in accordance with paragraph 33(1);
(e) supply to the relevant person immediately on request, copies of the evidence verifying the identity of the customer and the beneficial owner (if any) and all other customer due diligence information held by the introducer in any particular case;
(f) supply to the relevant person immediately copies of the evidence verifying the identity of the customer and the beneficial owner (if any) and all other customer due diligence information, in accordance with paragraphs 10(1), 12(1), 17(1) or 19(1) (as applicable), held by the introducer in any particular case if —
    (i) the introducer is to cease trading;
    (ii) the introducer is to cease doing business with the customer;
    (iii) the relevant person informs the introducer that it no longer intends to rely on the terms of business entered into under this paragraph;

(g) inform the relevant person specifically of each case where the introducer is not required or has been unable to verify the identity of the customer or the beneficial owner (if any);
(h) inform the relevant person if the introducer is no longer able to comply with the provisions of the written terms of business because of a change of the law applicable to the introducer; and
(i) do all such things as may be required by the relevant person to enable the relevant person to comply with its obligation under sub-paragraph (8).

Paragraph 23(8) of the Anti-Money Laundering and Counter the Financing of Terrorism Code 2015 reads as follows:

A relevant person must take measures to satisfy itself that —
(a) the procedures for implementing this paragraph are effective by testing them on a random and periodic basis no less than once every 12 months; and
(b) the written terms of business confer the necessary rights on the relevant person to satisfy the requirements of this paragraph

"Politically Exposed Person"

Politically Exposed Person is 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. "Politically Exposed Persons" include senior political figures and their immediate family, and close associates. Please see Paragraph 14 of the Code and Section 4.16 of the AML/CFT Handbook for further guidance.

"Principal(s)"

Includes the natural person who ultimately owns or controls the applicant for business or on whose behalf a transaction or activity is being conducted.
For a trust, this also would also include the:
(a) the trustee(s) or other persons controlling or having power to direct the activities of the applicant in line with the guidance for individuals and legal persons.
(b) any person(s) whose wishes the trustees may be expected to take into account;
(c) any other parties including the protector(s) and enforcer(s);
(d) any person(s) purporting to act on behalf of the trustee(s)
(e) any person(s) by whom binding obligations may be imposed on the applicant and verify that that person is authorised to do so;
(f) the settlor(s) (or other person making the arrangement) i.e. the initial settlors and any persons subsequently settling funds into the trust;
(g) beneficiaries at the time they come to benefit from the trust.
(h) any potential beneficiaries that the trustee has identified as presenting higher risk, including those presenting increased money laundering, terrorist financing, reputational or other risk.

For a legal person, this also includes:
Where a legal person is not listed on a recognised stock exchange or is not a wholly owned subsidiary of such a listed entity -
(a) any natural person who ultimately owns or controls (whether directly or indirectly) 25% or more of the shares or voting rights in the legal person.
(b) any person(s) having power to direct the activities of the legal person. This includes 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) any person(s) purporting to act on behalf of the legal person or by whom binding obligations may be imposed on the legal person.

For all legal persons -

(a) any natural person (whether as an individual, group of individuals or through another legal person or legal arrangement) who exercises effective control of the company or over the management of the company. This includes persons with less than 25% of the shares or voting rights but who nevertheless hold a controlling interest.

(b) In respect of foundations, this also includes:
- the registered agent;
- founder(s);
- dedicator(s);
- assignee(s);
- all known beneficiaries and potential beneficiaries presenting a higher risk;
- 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).

"Purpose / intended nature of business relationship" A sufficient description should be provided of the reason for the business relationship. For example: provision of current account facilities to the entity; investment of cash assets in equity

"Regulated person" **regulated person**" means —

1. any person holding a financial services licence issued under section 7 of the *Financial Services Act 2008*[1];
2. any person authorised under section 8 the *Insurance Act 2008*;
3. any person registered under section 25 of the *Insurance Act 2008*;
4. a retirement benefits schemes administrator registered under section 36 of the *Retirement Benefits Schemes Act 2000*[2]; or

i. a person holding an online gambling licence issued under section 4 of the *Online Gambling Regulation Act 2001*[3];

"Related Parties" This includes Directors, Trustees and all principals* where the applicant for business is a company, trust or foundation.

"Role This might include, for example: a shareholder, beneficiary, settlor, partner etc.

"Signature" This must be signed by an authorised signatory of the Eligible Introducer. A business name is not acceptable.

"Source of funds" This relates to the source of the customer's funds that will be involved in the transaction with the accepting business as per Section 4.13 of the AML/CFT Handbook.

[1] AT 8 of 2008
[2] AT 14 of 2000
[3] AT 10 of 2001

"Source of wealth"	The origins of a customer's financial standing or total net worth i.e. those activities which have generate a customer's funds and property as per section 4.13 of the AML/CFT Handbook.
"Type of trust / foundation / company"	For example: private limited company, public limited company, limited partnership, discretionary trust, fixed interest trust, testamentary trust.

Please refer to the accepting business should you have any doubt or queries about completing the Eligible Introducer Certificate Forms.

Appendix F

Acceptable Applicants Certificate

ACCEPTABLE APPLICANT'S CERTIFICATE

For Use with Direct Customer

Name of Customer _____

Address of Customer _____

_____

I/We confirm that I/We am/are one of the following persons *[Please tick as appropriate]*

1. A holder (or nominee company of a holder) of a financial services licence issued under section 7 of the Financial Services Act 2008 ☐
2. A person (or nominee of) authorised under section 8 of the Insurance Act 2008 ☐
3. Any person (or nominee of) registered under section 25 of the Insurance Act 2008 ☐
4. A retirement benefits schemes administrator (or nominee of) who is registered under section 36 of the Retirement Benefits Schemes Act 2000. ☐
5. A person (or nominee of) holding an online gambling licence issued under section 4 of the Online Gambling Regulation Act 2001. ☐
6. An advocate within the meaning of the Advocates Act 1976, a registered legal practioner within the meaning of the Legal Practitioners Registration Act 1986 or an accountant carrying on business in or from the Isle of Man. ☐
7. A person (or nominee of) who acts in the course of external regulated business and is regulated under the law of a jurisdiction in List C ☐
8. A company listed on a recognised stock exchange or a wholly owned subsidiary of such a company ☐

I/We confirm that I/We am/are overseen for AML/CFT compliance by:

Name of professional body or regulator (if applicable) _____

Jurisdiction of professional body or regulator (if applicable)_____

Signature _____

Job/position _____

Date_____

Appendix G

Acting "on Behalf of" Certificate (includes terms of business)

AOB 1.1 - ACTING ON BEHALF OF CERTIFICATE

To be completed by the regulated person:

Name of Regulated Person:	

In order to use the concession we can confirm that we hold a financial services licence covering Class 1 (deposit taking), Class 2 (investment business), Class 3 (services to collective investment schemes) or Class 8 (money transmission) services of the Regulated Activities Order 2011. We also confirm the following:

Item	Yes	No
The nature / intended purpose of the relationship with the underlying clients is known to us.		
We have not identified any suspicious activity.		
Written terms of business are in place covering all areas of paragraph 21 (3) of the Code.		
The CDD procedures of this customer are fit for purpose.		
The procedures of the customer will be tested at least annually.		

If, "no" is answered to any of these points the concession is no longer applicable to be used by the regulated person.

Signature:	
Full Name:	
Official Position:	
Date:	
Contact details of Signatory:	Address:
Telephone:	Email:

To be completed by the customer:

Name of Customer:	
Customer's contact details:	Address:
Telephone:	E-mail:
Customer's Regulatory or Supervisory body:	

The Customer certifies that it is an "allowed business" and is one of the following:
(Please tick the applicable box)

1	A regulated person.*	
2	A nominee company of a regulated person where the regulated person is responsible with the nominee's compliance with the AML/CFT requirements.	
3	A collective investment scheme (except a scheme within the meaning of Schedule 3 (exempt schemes) to the Collective investment Schemes Act 2008) where the manager or administrator of such scheme is a regulated person, or where the person is an equivalent scheme in a jurisdiction in list C where the manager or administrator is an external regulated business.	
4	A designated business.	
5	A person who acts in the course of external regulated business and is regulated under the law of a jurisdiction in List C and subject to AML/CFT requirements and procedures that are at least equivalent to the Code (but does not solely carry on activities equivalent to either or both of Class 4 (corporate services) or Class 5 (trust services) under the Regulated Activities Order 2011.	
6	A nominee company of an external regulated business where the regulated person is responsible with the nominee's compliance with the AML/CFT requirements.	

* Please see 1.2 for further guidance.

AOB 1.1 - ACTING ON BEHALF OF CERTIFICATE

To be completed by the customer:

The customer also certifies the following:

Item	Yes	No
The customer confirms that it will comply with the requirements of paragraph 21(3) and 21(5)* of the Code.		
It has obtained customer identification information on the underlying client (in accordance with Paragraphs 10-13 of the Code)		
It has verified the underlying client's identity (in accordance with Paragraphs 10-13 of the Code) and has no reason to doubt the identities.		
The customer undertakes to supply information on the identity of the underlying client, suitably certified copies* or originals of the verification documentation forthwith upon request.		
It has obtained details relating to the purpose / intended nature of business relationship with the underlying client.		
The source of funds of the underlying client have been identified.		

If, "no" is answered to any of these points the concession is no longer applicable to be used by the Regulated Person.

* Please see 1.2 for further guidance.

Signature:	
Full Name:	
Official Position:	
Date:	
Contact details of Signatory:	Address:
Telephone:	E-mail:

AOB 1.2 - ACTING ON BEHALF OF CERTIFICATE – ADDITIONAL INFORMATION

This acting on behalf of certificate aims to streamline and provide a standard format for the use of the concession in paragraph 21 of the Code.

These notes and the definitions below are intended to provide guidance to assist the parties in completing the required forms and to enable greater consistency to be achieved.

"Certified copy"

An officer or authorised signatory of a regulated financial service business will be a suitable certifier. An acceptable "certified copy" document should be an accurate and complete copy of the original such that the certifier will sign and date the copy document (printing his name clearly in capitals underneath) and clearly indicate his position or capacity on it and provide his contact details. The certifier must state that it is a true copy of the original as per Section 4.10 of the AML/CFT Handbook. Please see the main body of the Handbook in relation to the use of electronic verification.

"Paragraphs 21(3) and 21(5) Isle of Man's Anti-Money Laundering and Countering the Financing of Terrorism Code 2015"

Paragraph 21(3) of the Code reads as follows:

The written terms of business required to be in place in accordance with sub-paragraph (2)(f) must in all cases require the customer to —

(a) supply to the regulated person immediately on request, information on the identity of the underlying client, copies of the evidence verifying the identity of the underlying client and all other due diligence information held by the customer in respect of the underlying client in any particular case;

(b) inform the regulated person specifically of each case where the customer is not required or has been unable to verify the identity of the underlying client;

(c) inform the regulated person if the customer is no longer able to comply with the provisions of the written terms of business because of a change of the law applicable to the customer; and

(d) do all such things as may be required by the regulated person to enable the regulated person to comply with its obligations under sub-paragraph (2).

Paragraph 21 (5) of the Code reads as follows:

The regulated person must take reasonable measures to satisfy itself that —

(a) the procedures for implementing this paragraph are effective by testing them on a random and periodic basis no less than once every 12 months; and

(b) the written terms of business confer the necessary rights on the regulated person.

"Regulated person"	(a) any person holding a financial services licence issued under section 7 of the *Financial Services Act 2008*[46]; (b) any person authorised under section 8 the *Insurance Act 2008*; (c) any person registered under section 25 of the *Insurance Act 2008*; (d) a retirement benefits schemes administrator registered under section 36 of the *Retirement Benefits Schemes Act 2000*[47]; or (e) a person holding an online gambling licence issued under section 4 of the *Online Gambling Regulation Act 2001*[48];
Signature"	This must be signed by an authorised signatory of the Customer and the Regulated person
"Source of funds"	This relates to the source of the underlying client's funds as per Section 4.13 of the AML/CFT Handbook.

[46] AT 8 of 2008
[47] AT 14 of 2000
[48] AT 10 of 2001

Appendix H
Wire Transfers

Wire transfer regulations

The EU's legislation which had implemented measures to prevent electronic transfers of funds ("wire transfers") being abused for money laundering or the financing of terrorism was strengthened with effect from 26 June 2017 when Regulation (EU) 2015/847 repealed and replaced Regulation (EU) No 1781/2006.
It was published in the Official Journal of the European Union (OJ L 141) on 5 June 2015. It is available at:

http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32015R0847&qid=1500371387186

The new EU Regulation implements FATF Recommendation 16 within the EU.

The Regulation provides for EU Member States to establish agreements with territories outside the EU with whom they share a monetary union and payment and clearing systems for them to be treated as if they were part of the Member State concerned, so that the reduced information requirement can apply to payments passing between that Member State and its associated territory (but not between any other Member State and that territory). In the case of the UK, such arrangements include the Isle of Man and the Channel Islands.

The Regulation requires the ordering financial institution to ensure that all wire transfers carry specified information about the originator (Payer) who gives the instruction for the payment to be made and the Payee who receives the payment. The core requirement is that the Payer information consists of name, address, account number, official personal document number, customer identification number or date and place of birth; and that the Payee information consists of name and account number. There are also requirements imposed on any intermediary payment service provider. However, there are a number of permitted variations and concessions and those relevant to the Handbook are set out in below.

To maintain the position where wire transfers between the Island and the UK can be treated as if they were transfers within the UK, Regulation (EU) 2015/847 was applied (with appropriate modifications) as part of the law of the Island by the European Union (Information Accompany Transfers of Funds) Order 2016 as amended by the European Union (Information Accompanying Transfers of Funds) (Amendment) Order 2017. The text of the EU Regulation as modified in its application to the Island is attached to the amendment Order. The Information Accompanying Transfers of Funds Regulations 2016 were made to implement the Order. These Isle of Man Regulations contain enforcement provisions and sanctions for non-compliance, and came into force on 26 June 2017.

References to the British Islands in this Section are to an area that comprises the United Kingdom, the Bailiwick of Guernsey, the Bailiwick of Jersey and the Isle of Man. To ensure that the data protection position is beyond any doubt, it may be advisable for a payer Payment Service Provider ("PSP") to ensure that terms and conditions of business include reference to the information that will be provided.

Scope of the Regulation

The Regulation is widely drawn and intended to cover all types of funds transfer falling within its definition as made "by electronic means" other than those specifically exempted wholly or partially by the Regulation. For British Islands based PSPs it therefore 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.

The Regulation specifically exempts transfers where both Payer and Payee are PSPs acting on their own behalf, i.e. this will apply to MT 200 series payments via SWIFT. This exemption will include MT 400 and MT 700 series messages when they are used to settle trade finance obligations between banks.

The UK credit clearing system is out of scope of the Regulation as it is paper based and hence transfers are not carried out "by electronic means". Cash and cheque deposits over the counter via bank giro credits are not therefore affected by the Regulation.

Pre-conditions for making payments

Relevant persons must ensure that the Payer information conveyed in the payment relating to account holding customers is accurate and has been verified. The verification requirement is deemed to be met for account holding customers of the relevant person whose identity has been verified in accordance with the Code. No further verification of such account holders is required, although relevant persons may wish to exercise discretion to do so in individual cases.

Before undertaking one-off payments in excess of €1,000 on the instructions of non-account holding customers, a relevant person must verify identity and either date of birth or address in accordance with Article 5.2 of the Regulation. Evidence of verification must be retained with the customer information in accordance with Record Keeping Requirements under part 8 of this Handbook. For non-account based transfers of €1,000 and under, relevant persons are not required by the Regulation to verify the Payer's identification, except when several transactions are carried out which appear to be linked and exceed €1,000. NB, even in cases where the Regulation does not require verification, the customer information must be obtained and it may be advisable for the relevant person to verify the identity of the Payer in all cases.

Information Requirements

Complete payer information:
Except as permitted below, complete Payer information must accompany all wire transfers. Effectively, the complete requirement applies where the destination PSP is

located in a jurisdiction outside the British Islands. Complete Payer information consists of: name, address and account number.

(a) Address ONLY may be substituted with the Payer's official personal document number, date and place of birth, national identity number or customer identification number. In the event a Payee PSP demands the Payer's address, where one of the alternatives had initially been provided, the response to the enquiry should point that out. Only with the Payer's consent or under judicial compulsion should the address be additionally provided.
(b) Where the payment is not made from a payment account, the requirement for an account number must be substituted by a unique transaction identifier which permits the payment to be traced back to the Payer. The Regulation defines a unique identifier as "a combination of letters, numbers or symbols, determined by the payment service provider, 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."
(c) The extent of the information supplied in each field will be subject to the conventions of the messaging system in question and is not prescribed in detail in the Regulation.
(d) The account number could be, but is not required to be, expressed as the IBAN (International Bank Account Number).
(e) Where a bank is itself the Payer, as will sometimes be the case even for SWIFT MT 102 and 103 messages, this Guidance considers that supplying the Bank Identifier Code (BIC) constitutes complete Payer information for the purposes of the Regulation, although it is also preferable for the account number to be included where available. The same applies to Business Entity Identifiers (BEIs), although in that case the account number should always be included. As the use of BICs and BEIs is not specified in the Regulation, there may be requests from Payee PSPs for address information.
(f) Where payment instructions are received manually, e.g. over the counter, the Payer name and address (or permitted alternative) should correspond to the account holder. Any request to override customer information should be processed within a rigorous referral and approval mechanism to ensure that only in cases where a relevant person is entirely satisfied that the reason is legitimate should the instruction be exceptionally dealt with on that basis. Any suspicion of improper motive by a customer must be reported to the relevant person's MLRO.

Reduced Payer Information:
Where the PSPs of both Payer and Payee are located within the British Islands, wire transfers need be accompanied only by the Payer's account number or by a unique identifier which permits the transaction to be traced back to the Payer.

However, if requested by the Payee's PSP, complete information must be provided by the Payer's PSP within 3 working days, starting the day after the request is received by the Payer's PSP. ("Working days" is as defined in the jurisdiction of the Payer's PSP).

Complete Payee information:
Except as permitted below, complete Payee information must accompany all wire transfers. Effectively, the complete requirement applies where the destination PSP is

located in a jurisdiction outside the British Islands. Complete Payee information consists of: name and account number.

Where the payment is not made from a payment account, the requirement for an account number must be substituted by a unique transaction identifier which permits the payment to be traced back to the Payee. The Regulation defines a unique identifier as "a combination of letters, numbers or symbols, determined by the payment service provider, 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."

A table detailing the information needed for different types of payment is below:

Payment type	Payer	Payee
Outside the British Islands, over €1,000	Name Account number/transaction ID Address*	Name Account number/transaction ID
Outside the British Islands, under €1,000	Name Account number/transaction ID	Name Account number/transaction ID
Inside the British Islands	Account number/transaction ID	Account number/transaction ID

* Or official personal document number, customer identification number or date and place of birth.

Batch File Transfers:
A hybrid complete/reduced requirement applies to batch file transfers from a single Payer to multiple Payees outside the British Islands in that the individual transfers within the batch need carry only the Payer's account number or a unique identifier along with complete Payee information, provided that the batch file itself contains complete Payer information.

Payments via Intermediaries:
Intermediary PSPs must ensure that all information received on the Payer and the Payee which accompanies a wire transfer is retained with the transfer. A requirement to detect 'missing information (see Checking Incoming Payments) applies in the same way as for transfers of funds received direct by the Payee PSP.

Checking Incoming Payments

Relevant persons must have effective risk based procedures for checking that incoming wire transfers are compliant with the relevant information requirement. These procedures must include, where appropriate, ex-post monitoring or real time monitoring in order to detect whether the required information on the payer or payee is missing. Additionally, the Regulation requires PSPs to take remedial action when they become aware that an incoming payment is not compliant.

Relevant persons must therefore subject incoming payment traffic to an appropriate level of random sampling to detect non-compliant payments. This sampling should be risk based, for example:

(a) the sampling could normally be restricted to payments emanating from PSPs outside the British Islands where the complete information requirement applies;
(b) the sampling could be weighted towards non FATF member jurisdictions, particularly those deemed high risk under a PSP's own country risk assessment, or by reference to external sources such as Transparency International, or FATF or IMF country reviews;
(c) focused more heavily on transfers from those Payer PSPs who are identified by such sampling as having previously failed to comply with the relevant information requirement;
(d) 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.

If a relevant person becomes aware in the course of processing a payment that it contains meaningless or incomplete information, under the terms of Article 8(1) of the Regulation it should either reject the transfer or ask for complete information on the Payer. In addition, in such cases, a relevant person is required to take any necessary action to comply with any applicable law or administrative provisions relating to money laundering and terrorist financing. Dependent on the circumstances such action could include making the payment or holding the funds and advising the MLRO.

Where a relevant person becomes aware subsequent to processing the payment that it contains meaningless or incomplete information either as a result of random checking or other monitoring mechanisms under its risk based approach, it must:

(a) seek the necessary information on the Payer and/or Payee; and/or,
(b) take any necessary action under any applicable law, regulation or administrative provisions relating to money laundering or terrorist financing.

Where a PSP is identified as having regularly failed to comply with the information requirements, a relevant person must take steps, which may initially include issuing warnings and setting deadlines, prior to either refusing to accept further transfers from that PSP or deciding whether to terminate its relationship with that PSP either completely or in respect of funds transfers.

A relevant persons must consider whether incomplete or meaningless information of which it becomes aware on a funds transfer constitutes grounds for suspicion which would be reportable to its MLRO for possible disclosure to the FIU.

With regard to transfers from PSPs located in non-member countries of FATF, relevant persons should endeavour to transact only with those PSPs with whom they have a relationship that has been subject to a satisfactory risk-based assessment of their AML/CFT culture and policy and who accept the standards set out in the Interpretative Note to FATF Recommendation 16.

It should be borne in mind when querying incomplete payments that some FATF member countries outside the EU may have framed their own regulations to incorporate a threshold of Euro or US Dollars 1000 below which the provision of complete information on outgoing payments is not required. This is permitted by the

Interpretative Note to FATF Recommendation 16. The USA is a case in point. This does not preclude Isle of Man PSPs from calling for the complete information where it has not been provided, but it is reasonable for a risk-based view to be taken on whether, or how far, to press the point.

Links to legislation

European Union (Information Accompanying Transfers of Funds) Order 2016
http://www.tynwald.org.im/links/tls/SD/2016a/2016-SD-0349.pdf

European Union (Information Accompanying Transfers of Funds) (Amendment) Order 2017
http://www.tynwald.org.im/business/opqp/sittings/Tynwald%2020162018/2017-SD-0182.pdf

Information Accompanying Transfers of Funds Regulations 2016
http://www.tynwald.org.im/links/tls/SD/2016a/2016-SD-0350.pdf

Appendix I

Proforma Register of Money Laundering and Financing of Terrorism Disclosures Made to the MLRO or Deputy MLRO

This pro-forma is a guidance document, based on paragraph 35 of the Anti-Money Laundering and Countering the Financing of Terrorism Code ("AML/CFT Code") 2015 which may be used as a template by Relevant Persons.

[Relevant Persons Name]
Register of Internal Money Laundering and Financing of Terrorism Disclosures made to the MLRO or Deputy MLRO.

"A Relevant Person must establish and maintain separate registers of all external disclosures and internal disclosures."
Paragraph 35(1) of the AML/CFT Code 2015

Para 35(3)(a)	***Para 35(3)(b)***	***Para 35(3)(c)***	***Para 35(3)(e)***	
Date on which the report is made	*Person who made the report*	*Whether made to the MLRO or Deputy MLRO*	*Information sufficient to identify the relevant papers*	*Comments and further action#*

 # Guidance: optional field.

Appendix J

Proforma Register of Money Laundering and Financing of Terrorism External Disclosures Made to FIU

This pro-forma is a guidance document, based on sub-paragraph 35 of the Anti-Money Laundering and Countering the Financing of Terrorism Code ("AML/CFT Code") 2015 which may be used as a template by Relevant Persons.

[Relevant Persons Name]

Register of External Money Laundering and Financing of Terrorism Disclosures made to the FIU.

"A Relevant Person must establish and maintain separate registers of all external disclosures and internal disclosures."
Paragraph 35(1) of the AML/CFT Code 2015

Para 35(3)(a)	***Para 35(3)(b)***	***Para 35(3)(d)***	***Para 35(3)(e)***	
Date on which the report is made	*Person who made the report*	*To whom was the report made*	*Information sufficient to identify the relevant papers*	*Comments and further action#*

 # Guidance: optional field.

Appendix K

Proforma Register of Money Laundering and Financing of Terrorism Enquiries

This pro-forma is a guidance document, based on -paragraphs 36 of the Anti-Money Laundering and Countering the Financing of Terrorism Code ("AML/CFT Code") 2015 which may be used as a template by Relevant Persons.

[Relevant Persons Name]
Register of Money Laundering and Financing of Terrorism Enquiries

"A Relevant Person must establish and maintain a register of all money laundering and financing of terrorism enquiries made of it by law enforcement or other competent authorities."
Paragraph 36 of the AML/CFT Code 2015

Para 36(2)(a)	***Para 36(2)(b)***	***Para 36(2)(c)***	***Para 36(2)(d)***	***Para 36(2)(e)***	
Date when the enquiry was received	*Nature of the enquiry*	*Name of the enquiring officer and agency*	*Powers being exercised*	*Details of the accounts or transactions involved (e.g. name of customer, account number and date of transactions*	*Comments and further action#*

 # Guidance: optional field.

Appendix L

Terrorist Financing Typologies and Countering the Financing of Terrorism Guidance

Introduction

The purpose of this document is to provide specific guidance for all businesses in the regulated sector which may be vulnerable to misuse by those who wish to finance terrorism. The document will provide some detail of the ways in which terrorist financing takes place building from the brief definition of the term found at 7.3.2 of the main body of the Handbook. A number of typologies are set out along with a description of countermeasures which businesses in the regulated sector should adopt. This guidance should be read in conjunction with the main body of the Handbook. As with all guidance in the Handbook, this guidance is not law, however it is persuasive. Where a person follows guidance this would tend to indicate compliance with the legislative provisions and vice versa.

What is Terrorist Financing?

Section 7.3.2 of the main body of the Handbook provides a general definition as to what constitutes terrorist financing. The term is a generic one which is not defined in any Isle of Man Statute, but was set out in the United Nations International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention) 1999 and includes the financing of terrorist acts, terrorist organisations or individual terrorists. The various terrorist financing offences can be found in Part III of the Anti-Terrorism and Crime Act 2003. These include the offences of:

- Fund raising (section 7);
- Use and possession (section 8);
- Facilitating funding (section 9);
- Financing travel (section 9A);
- Money laundering (section 10); and
- The Failure to Disclose: regulated sector offence (section 14).

It is particularly important to note that whilst the *mens rea*[49] for the other offences require knowledge or reasonable cause to suspect use for terrorist purposes, the offence of Facilitating funding can also be committed when the *offender has failed to exercise due diligence as to whether it will or may be used for the purposes of terrorism*.

The direct (estimated) costs involved in carrying out terror attacks have been quite widely reported. The table below gives an indication of the approximate costs of some of the more recent high profile attacks.

[49] 'guilty mind', having awareness that the act is criminal

Date	Attack	Country	Estimated Cost
12 October 2000	USS Cole bombing	Aden (Yemen)	USD 10,000
12 October 2002	Bali bombings	Bali	USD 50,000
11 March 2004	Madrid train bombings	Spain	USD 10,000
7 July 2005	London transport bombings	UK	GDP 8,000
13 November 2015	Paris attacks	France	EUR 27,000
14 July 2016	Nice truck attack	France	EUR 2,500
22 May 2017	Manchester Arena bombing	UK	Investigation ongoing
3 June 2017	London Bridge attack	UK	Investigation ongoing

As can be seen the direct cost of each of these attacks is relatively low and appears to be decreasing, particularly with the recent use of unsophisticated, inexpensive but effective *modus operendi*.

Because of the high profile given to the direct costs, it is easy to obscure the bigger picture. The broader operational costs which underpin terrorist activity are significantly higher and include:

- The costs involved in promoting a militant ideology;
- Paying operatives and often their families expenses such as subsistence;
- Death in service – when terrorists die, the terrorist organisation often supports the family;
- Arranging for travel for training and to stage attacks;
- Training new members;
- Buying or renting safe houses;
- Forging documents;
- Paying bribes; and
- Acquiring weapons.

Many of these expenses will, by necessity, be incurred in secret and will therefore incur a “clandestine premium”. In addition, the source of the funds used must be obscured to prevent that source being disrupted. As these operational costs are quite high, terrorist organisations are dependent on a steady, sustained funding stream.

Terrorist Financing Typologies

The following information and typologies have largely been extracted from a recent Financial Action Task Force (“FATF”) report entitled *Emerging Terrorist Financing Risks* dated October 2015 (link below).

http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

The need for terrorist groups to obtain funds, move and use them has always been there, but as terrorist groups have evolved, so too have the methods they use in order to do this. The FATF refer to these recent developments as "emerging TF risks". Although there is much overlap between the methods used by large terrorist organisations, small terrorist cells, lone actors and foreign terrorist fighters ("FTFs"), some distinctly different patterns can be seen which will be outlined below. For more detail on these, please refer to the FATF paper above.

Traditional Terrorist Financing

Fund raising

The mainstream methods used by terrorist organisations to raise funds include the following:

- Private donations by terrorist sympathisers;
- Abuse and misuse of Non-Profit Organisations ("NPOs");
- Criminal activity; and
- Legitimate commercial activity.

Of these, probably the second and fourth may have most relevance to businesses in the regulated sector in the Isle of Man.

Abuse and misuse of NPOs

This is one of the most important methods by which mainstream terrorist organisations use to raise funds. A 2014 FATF study found that the abuse or misuse of NPOs occurred in five different ways:

- Diversion by embedded terrorist sympathisers of donations made to legitimate NPOs to terrorist organisations;
- Exploitation of legitimate NPOs;
- Misuse of the NPO delivery programme to support the terrorist organisation; and
- Creation of sham NPOs.

The study found that NPOs at most risk of terrorist abuse are those engaged in activities which are operating close to an area where terrorist activity is taking place. NPOs that remit funds to counterpart or correspondent NPOs located in such areas are vulnerable to misuse unless effective due diligence is done on the counterpart NPO with proper auditing of how and where the funds are used. The study found that NPOs operating in such areas are at an increased risk of being infiltrated and exploited by terrorist groups, particularly where less-established or start-up charities or NPOs without effective due diligence procedures are involved.

Legitimate commercial activity

A number of law enforcement investigations have found links between genuine commercial enterprises and terrorist organisations where the profits of the business were used to provide finance for the terrorist cause. Examples have included the shipment of used cars to West Africa and to the Middle East with some of the revenue from the sale of those cars being used to support terrorist groups. Corporate services providers who may unwittingly be involved in such commercial activity and banks should be aware of such typologies.

Movement of funds

Any method which can be used to transfer funds is potentially vulnerable to misuse for terrorist financing including the following:

- Fund transfers through banks;
- Money transmission services;
- Physical transportation of cash

Banking

The banking sector remains vulnerable to misuse for terrorist financing as it remains the most efficient and reliable way to transfer funds internationally and several FATF reports have commented on the use of the bank accounts of NPOs to move funds to terrorist organisations. It is attractive to terrorist groups because of the speed and ease by which it can be used to transfer funds within the global financial system. The global banking system is so large that terrorist fund movements have the opportunity to blend in with normal financial activity and avoid attracting attention. Terrorist fund movements may often be relatively small in comparison with legitimate commercial fund movements and therefore not arouse suspicion. Studies have found typologies including the deposit of cash in a personal bank account followed by international fund transfers, the use of legitimate and shell business accounts and the use of debit cards by terrorist groups to withdraw funds from accounts opened by terrorist sympathisers.

Money transmission services

This sector is also vulnerable to misuse for terrorist financing, particularly in those regions where access to banking services is limited. As migrant communities and families rely heavily on money transmission services to send funds home, this provides an opportunity to mingle terrorist financing fund movements with legitimate family transfers making them difficult to detect. Studies have also reported the use of money transmission services to finance foreign terrorist fighters.

Physical transportation of cash

Cash remains the medium most used by terrorist organisations. Funds may be raised in many ways and transferred globally using the international banking system or money transmitters, but they are often converted into cash before being taken into conflict zones and used.

Emerging Terrorist Financing Risks

Foreign terrorist fighters ("FTFs")

In September 2014 the United Nations Security Council defined foreign terrorist fighters as individuals who travel or attempt to travel to a state other than their state of residence or nationality "for the purpose of the perpetration, planning or preparation of or participation in terrorist acts or the providing or receiving of terrorist training".

FTFs are not new, but the conflict in Syria and Iraq has led to a significant escalation in their involvement in terrorist activity. An estimated 30,000 FTFs currently operate in this region. Returning FTFs also represent a new and dangerous threat of terrorist activity in their country of origin. Self-funding by individuals and funding by recruitment and facilitation networks are considered to be the main methods used to raise funds for FTFs.

The funding levels required by FTFs are relatively low and are required to support transportation, accommodation whilst en-route to areas of conflict, outdoor clothing, camping equipment, mobile phones, food and general living expenses.

FTFs often use funds from legitimate sources such as employment income, family support, social assistance, student grants and the sale of personal belongings and assets purchased on credit just before their planned travel. Other typologies include the FTF taking out small short-term loans, often from multiple lenders that they have no intention of ever repaying.

FTFs fund movements usually involve the physical transportation of cash, the use of ATMs to access funds held in bank accounts and money transmission services.

Other methods of raising and moving funds

Newer emerging methods include:

- Fundraising using social media; and
- Crowd funding

To raise funds and

- Virtual currencies;
- Prepaid cards; and
- Internet-based payment services

To transfer and/or access funds.

Countering the Financing of Terrorism Guidance

The key to countering the financing of terrorism is firstly to be aware that it can happen and that it can involve any jurisdiction including the Isle of Man. The above typologies give an indication of the various methods which can be used to raise and remit funds and all businesses in the regulated sector should be aware of them.

Effective implementation of the provisions of the Anti-Money Laundering and Countering the Financing of Terrorism Code 2015 ("the Code") is critical so that activity which leads to a suspicion of terrorist financing is identified and an SAR made promptly to the FIU.

No businesses in the regulated sector are immune from being used for terrorist financing, but the following sectors may be particularly vulnerable:

- Banking sector;
- Money transmission Services;
- Non-profit organisations:
- Corporate service providers.

It is essential that businesses apply effective customer due diligence, not only to determine who their customers are; but also, probably of more importance, to determine the nature and intended purpose of the business relationship. If that business relationship is likely to involve remittance of funds to or business activity in other jurisdictions, further enquiries should be pursued at the onset of the relationship as to the nature, level, frequency and purpose of such remittances or business activity. These enquiries will also form part of the customer risk assessment and if remittances or activity are likely to involve jurisdictions which bear a higher risk of terrorist financing, areas of conflict or neighbouring regions, consideration should be given to raising the risk rating of the customer to higher risk and obtaining enhanced due diligence as per paragraph 15 of the Code. The customer risk assessment and customer due diligence should give the relevant person a baseline view of what is likely to be normal and effective ongoing monitoring should identify unusual or suspicious activity. Remittance of funds to or business activity in higher risk jurisdictions may lead the relevant person to perform further scrutiny and institute further enquiries as to the nature and purpose of those remittances or activity.

Proper screening of the screening of both the customer and any proposed or actual recipient of funds or business services may be appropriate in the circumstances detailed above.

Unusual activity may include, but is not limited to:

- Unusual customer behaviour;
- Cash transfers to higher risk places or transit countries (e.g. Turkey) either through the bank or through Money transmitters;
- Lots of cash transactions;

- Customers who may have banked for a long time, even have a dormant account which has been suddenly reactivated;
- Lots of money for transport expenditure to higher risk locations;
- Consumer loans which are not then repaid;
- Contributions to relevant charities;
- On social media, lots of “new friends” especially over a wide geographical area;
- Funds in from crowd funding or donation sites.