Montserrat Financial Services Commission

Guidance for the Prevention and Detection of Money Laundering and Terrorist Financing for High Value Dealers

Issued: 20.May.2024

Sector Specific Guidance for High Value Dealers

Contents

Foreword

A. What is Money Laundering?

Money Laundering is the process by which funds derived from criminal activity ("dirty money") are given the appearance of having been legitimately obtained, through a series of transactions in which the funds are 'cleaned'. Its purpose is to allow criminals to maintain control over those proceeds and, ultimately, provide a legitimate cover for the source of their income.

For money laundering to take place, first, there must have been the commission of a serious crime (also referred to as a predicate offence) which resulted in benefits/gains (illegal funds) to the perpetrator. The perpetrator will then try to disguise the fact that the funds were generated from criminal activity through various processes and transactions which may also involve other individuals, businesses and companies.

There is no one single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g., cars or jewellery) to passing money through legitimate businesses and "shell" companies. Money laundering can take many forms, but for high value dealers (HVDs) it can involve:

- exchanging cash for high value items that can be easily transferred and sold on, sometimes at a loss, such as jewellery or vehicles
- exchanging cash for large quantities of lower value items that can be sold onwards easily such as alcohol
- exchanging cash for high value assets that are then returned and clean cash refunded.

Tax evasion is a criminal offence that can lead to money laundering. For example, sale or purchase of high value goods for cash can be under reported to avoid paying VAT or corporation tax.

A.1 The Stages of Money Laundering

The money laundering process is generally described as taking three stages. It is important to remember that the three stages are not necessarily sequential. For example, the laundering of the proceeds of corruption typically commences at the layering stage as the proceeds are already in the banking system and diverted through layering out of the hands of the rightful

owner.

A.1.1 Placement

Criminally derived funds are brought into the financial system. In the case of drug trafficking, and some other serious crimes, such as robbery, the proceeds usually take the form of cash which needs to enter the financial system. Examples of placement are depositing cash into bank accounts or using cash to purchase assets. Techniques used include Structuring – breaking up a large deposit transaction into smaller cash deposits and Smurfing – using other persons to deposit cash.

A.1.2 Layering

This takes place after the funds have entered into the financial system and involves the movement of the funds. Funds may be shuttled through a complex web of multiple accounts, companies, and countries in order to disguise their origins. The intention is to conceal and obscure the money trail in order to deceive Law Enforcement Agencies and to make the paper trail very difficult to follow.

A.1.3 Integration

The money comes back to criminals “cleaned”, as apparently legitimate funds. The laundered funds are used to fund further criminal activity or spent to enhance the criminal's lifestyle.

Criminals may use services to assist in investment in legitimate businesses or other forms of investment, to buy a property, set up a trust, acquire a company, or even settle litigation, among other activities.

Successful money laundering allows criminals to use and enjoy the income from the criminal activity without suspicion.

B What is Financing of Terrorism?

Financing of Terrorism is the process by which funds are provided to an individual or group to fund terrorist activities. Unlike money laundering, funds can come from both legitimate sources

as well as from criminal activity. Funds may involve low dollar value transactions and give the appearance of innocence and a variety of sources. Funds may come from personal donations, profits from businesses and charitable organizations e.g., a charitable organization may organise fundraising activities where the contributors to the fundraising activities believe that the funds will go to relief efforts abroad, but, all the funds are actually transferred to a terrorist group.

Funds may come, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

Unlike money laundering, which precedes criminal activity, with financing of terrorism you may have fundraising or a criminal activity generating funds prior to the terrorist activity actually taking place.

However, like money launderers, terrorism financiers also move funds to disguise their source, destination and purpose for which the funds are to be used. The reason is to prevent leaving a trail of incriminating evidence - to distance the funds from the crime or the source, and to obscure the intended destination and purpose.

A person or an entity commits an offence of Terrorist Financing if they;

- fund-raise or are involved in fund-raising, use, or intend to use, or possess money or other property for the purposes of terrorism
- conceal, transfer or remove from a jurisdiction, any money or other property used to finance terrorism
- facilitate the retention or control of money, which is destined for, or is the proceeds of terrorism
- do not comply with a prohibition imposed by a freezing order or enable any other person to contravene the freezing order
- make available funds or economic resources, directly or indirectly to a designated person, or deal with funds or economic resources which are owned, held, or controlled by a designated person.

1 Introduction

Criminals have responded to the anti-money laundering and terrorist financing measures introduced over the past years by the traditional financial sector and have sought other means to convert their proceeds of crime.

In their own response to the changing landscape of money laundering and terrorist financing, inter-governmental and international standard setting organisation, notably the Financial Action Task Force (FATF) has extended the scope of recommended prevention measures. FATF recommendations now include Anti-Money Laundering and Combating Terrorist Financing responsibilities to a group of businesses and professions collectively named as Designated Non-Financial Businesses and Professions (referred to as DNFBPs). This group includes those businesses which deal in goods of high value.

Dealers in high value goods provide a useful store of value and may form part of a criminal lifestyle. Goods are generally luxury items that could be potentially sold on through the black market, for example jewellery, antiques and high-performance cars.

The continuing ability of Montserrat's financial services industry to attract legitimate customers with funds and assets that are clean and untainted by criminality depends, in large, upon the island's reputation as a sound, well-regulated jurisdiction. Any dealer in high value goods in Montserrat that assists in laundering the proceeds of crime, or financing of terrorism, whether:

- with knowledge or suspicion of the connection to crime; or
- in certain circumstances, acting without regard to what it may be facilitating through the provision of its services, will face the loss of its reputation and damage the integrity of Montserrat's professional and financial services industry as a whole and may risk prosecution for criminal offences.

Cash is the mainstay of much recognised criminal activity. For the criminal it has the obvious advantage of leaving no discernable audit trail and is their most reliable and flexible method of payment. Cash is also a weakness for criminals. Whilst they hold the cash they are more at risk of being traced to the predicate offence. Cash seizure powers also means they are more at risk

of money being taken away by law enforcement. The focus of preventative measures with regard to high value dealers is on the acquisition of high value goods using cash.

2 Purpose of this Guidance Document

The purpose of this document is to provide industry specific guidance for High Value Dealers on their legal obligations to deter and detect money laundering and financing of terrorist activities.

The guidance

- Outlines the legislation on anti-money laundering (AML) and countering of terrorist financing (CTF) measures
- Explains the requirements of Montserrat's AML Regulations and AML Code 2024 and how these should be used in practice.
- Provides specific good practice guidance on AML/CTF procedures.
- Assists High Value Dealers in designing and putting in place the systems and controls necessary to lower the risk of their business being used by criminals to launder money or finance terrorism.

Reference is made throughout this document to AML/CTF. The Regulations refer to Anti Money Laundering and Countering of Terrorist Financing and other bodies tend to use AML/PTF, Anti Money Laundering and the Prevention of Terrorist Financing. The two pieces of terminology are interchangeable.

3 Status of this Guidance

The objective of this guidance document is to supplement, with specific reference to High Value Dealers, The Proceeds of Crime Act, Cap. 04.04, ("POCA") The Anti-Money Laundering and Terrorism Financing Regulations ("AML Regulations") and the Anti-Money Laundering and Terrorist Financing Code 2024, ("Code").

In case of doubt between this document and the Code, the Code will take precedence.

This guidance uses plain language to explain the most common situations under the specific laws and related regulations which impose AML/CTF requirements. It is provided as general information only. It is merely guidance and not a substitute for legal advice, nor intended to

replace the POCA or the Regulations.

This Guidance is intended for use by senior management and compliance staff of a business dealing in high value goods to assist in the development of systems and controls. It is not intended to be used as an internal procedure manual.

4 Montserrat Financial Services Commission as the Supervisory Authority

The Regulations seek to reduce businesses' vulnerability to being used for money laundering or terrorist financing.

In accordance with Regulation 18 of the AML Regulations, the Commission has been appointed the sole supervisory authority of all DNFBP, for the purposes of Section 157 (2) of the POCA.

As the Supervisor, the Commission is required to:

- Establish and maintain a Register of all Non-Financial Service Providers (NFSPs). The Register will include Dealers in High Value Goods.
- Monitor compliance with the Regulations.
- Take appropriate enforcement action.

5 Businesses and Individuals within the Scope of this Guidance

5.1 Overview of the Sector

This guidance is applicable to all "High Value Dealers" which accept cash payments of at least EC$35,000 or the equivalent in another currency whether the transaction is executed in a single operation or in several linked operations. This includes when a customer deposits cash directly into your bank account, or when they pay cash to a third party for your benefit.

There are a number of sub sectors in the High Value Dealers (HVD) sector and include: Alcohol, Art & Antiques, Auction, Caravans, Motorhomes & Static Vans, Cars, Cash & Carry or Wholesaler, Cash & Carry or Wholesaler – Alcohol, Commercial Vehicles, Electronic Goods, Food, High-End Retail, Household, Sports & Guns, Jewellery, Pharmaceutical or Chemicals,

Recycling, Textiles & Clothing, Vehicles other, etc.

5.1.1 Cash: Definition

The Regulations Part 1 (2) (1) defines cash to be

a) Notes and Coins
b) Postal Orders
c) Travellers Cheques

A relevant cash payment is deemed to be:

- a single cash payment of EC$35,000 or more for goods.
- several cash payments for a single transaction totalling EC$35,000 or more, including a series of payments and payments on account.
- cash payments totalling EC$35,000 or more which appear to have been broken down into smaller amounts so that they come below the relevant cash payment limit.

The thresholds quoted may be reached in respect of a single transaction or there may be several linked transactions for the same customer that together will exceed the threshold value.

These obligations apply to businesses operating in Montserrat. The requirements are the responsibility of the employer, but employees are required to report internally suspicious transactions in accordance with the employer's compliance programme.

5.2 Obligations Under the Regulations

- Put in place adequate documented policies, procedures and controls to guard against being exploited by criminals taking into account the risks posed by the nature, scale and complexity of the business.
- Set up procedures to undertake customer due diligence including risk assessing the customer and verifying the identity of any customer who offers cash above the threshold values, as well as other customers where there is a suspicion of money laundering.
- Inform staff of their obligations and responsibilities and those of the business, and train staff as to how to recognise and report suspicious activity.
- Appoint a Money Laundering Reporting Officer (MLRO) to whom staff can report their

suspicions and who will be responsible for making any disclosures to Montserrat's Financial Intelligence Unit (FIU)

- Appoint a Money Laundering Compliance Officer (MLCO) (who may also be the MLRO) for overseeing compliance with the requirements of the Regulations and acting as liaison point with the FIU.
- Monitor the activity of the customer throughout the relationship.
- Retain all relevant records including copies of the identification evidence obtained and all transactions or activity carried out for customers.
- Co-operate with the FIU as requested in anti-money laundering or terrorist financing investigation.

6 Legislation

This section provides a brief overview only of the legislation and regulations.

6.1 Legislation, Regulations and The Code

The Proceeds of Crime Act, 04.04 was amended in 2010, 2011, 2013, 2014, 2015 and 2023.

- Proceeds of Crime Act, Cap. 04.04 (the principal legislation)
- The Anti-Money Laundering and Terrorist Financing Regulations 2024
- The Anti-Money Laundering and Terrorist Financing Code 2024

6.2 Money Laundering Offences

Money Laundering is dealt with in Part 6 Sections 116 – 133 of the Proceeds of Crime Act, Cap. 04.04 (POCA).

Criminal Property	**Section 116 – 117**
Offences of Concealing, Disguising, Converting, Transferring and Removing Criminal Property	**Section 118**
Offence of Arrangements	**Section 119**
Offences of Acquisition, Use and Possession of Criminal Property	**Section 120**
Offences of Attempting, Conspiring and Inciting	**Section 121**
Duty to Disclose Knowledge or Suspicion of Money Laundering	**Sections 122 – 123**
Offence of Prejudicing Investigations and Tipping Off	**Section 124 – 125**
Protection of Disclosures	**Section 127**

6.2.1 Non-Compliance with Money Laundering Regulations

Non-compliance with obligations under the AML/CFT laws and regulations may result in criminal and or administrative sanctions.

Penalties include fines and terms of imprisonment, and sanctions include possible revocation of licenses, issuance of directives and court orders.

7 Registration with the Financial Services Commission

Montserrat Financial Services Commission is the sole supervisory authority for Designated Non-Financial Businesses and Professions. High Value Dealers are included within the definition of DNFBPs.

As Supervisor the Commission must establish and maintain a register of DNFBPs.

7.1 Registration Procedure

- Applicants for registration must complete and submit a paper copy of the Application to Register.
- The application form is available from the Financial Services Commission and may be prepared electronically and printed for submission to the Commission.
- An advance copy of the Application to Register may be submitted by email to the address: info@fsc.ms.
- A signed paper printed copy of the Application to Register together with supporting documents must be delivered by hand to the offices of the Commission.
- The application must fulfill the following requirements (as prescribed by Regulation 20 of the AML/TF Regulations):
- be in writing and in the form specified by the Supervisor (typed);
- be signed by the applicant or by a person acting on the applicant's behalf;
- be accompanied by such documents or information as may be specified on the application form or by the Supervisor.

7.1.1 Supporting Documents

The Application to Register and the Guidance Notes describe the documents which must be provided to verify information:

- Biographical affidavit form (complete with two (2) forms of IDs) to be completed by all shareholders, directors, management and senior officers with decision making powers.
- Personal Questionnaire to be completed by all shareholders and directors.
- Incorporation certificate if incorporated as a company.

Every effort will be made by the Commission to reduce the amount of verification documentation which must be provided, wherever possible, by utilising information and documentation already provided or available to the Commission.

Documents which must be submitted as verification by individuals/companies must be certified by one of; a Notary Public, Justice of the Peace, or Commissioner of Oaths, as a true copy of the original.

7.1.2 Receipt of Registration Application by the Commission

The Commission undertakes to acknowledge receipt within two to five working days of receiving the Application to Register.

The Commission will advise, by a letter to the applicant, within 30 days of receipt, of the outcome of the application unless additional information is requested. The response shall be one of:

- Registration Confirmed
- Registration Refused
- A request for further information or documentation. (In such cases the Commission shall keep the applicant advised of progress.

7.1.3 Refusal of a Request for Registration

A refusal of the Application will be in written form and will state the grounds for refusal.

The grounds upon which the Commission may refuse an Application for Registration are one or

more than one of the following criteria:

a) The applicant does not comply with Regulation 20 (3).

b) The applicant fails to provide any information or documents required by the Supervisor under Regulation 20 (3).

c) The Supervisor is of the opinion that –

- The applicant does not intend to carry on the relevant business for which it seeks registration.
- The business or any of its directors, senior officers or owners does not satisfy the Supervisors fit and proper criteria.
- It is contrary to the public interest for the business to be registered.

For full details of grounds for refusal please refer to the Regulations which can be found in Regulation 22 of the AML/CFT Regulations.

7.1.4 Registration Refused: Right to Appeal

In the event that an application to register is refused by the Commission, the applicant may submit an appeal, within 28 days of the date of the refusal, to the Court for leave to appeal against the decision. The decision of refusal of the application to register made by the Commission will remain intact during the period of the appeal and until otherwise directed by the Court.

For further details on the conditions for appeal, please refer to section 171 of the POCA.

7.1.5 Forms

The following forms to be used can be accessed on the FSC website at fscmontserrat.org.

7.1.6 Continuing Registration and Material Changes

Subsequent to the initial submission, registration is an on-going process. Renewals of existing successful applications will take place on the third anniversary of the original approval, i.e. registration is valid for a one-year period.

All individuals and businesses are required to register as soon as they begin to provide the services designated for their business or profession.

If at any time after registration there are material changes to the information supplied as part of the application, or it becomes apparent that there is a significant inaccuracy in the details provided, the business must notify the Commission, as soon as possible, of the changes occurring or the inaccuracy being discovered.

If a business does not notify the Commission of any material changes or inaccuracies in the details provided for registration, it will be in breach of the Regulations and may be subject to civil penalties or prosecution.

7.1.7 Offence - Failure to Register

A business shall not carry out a relevant business as a Designated Non-Financial Business and Profession until registered with the FSC.

Failure to register when required may result on summary conviction to imprisonment for a term of twelve months, or a fine of $20,000 or both. On conviction on indictment to imprisonment for a term of three years or to a fine of $75,000 or to both.

For further details on failure to register, please refer to section 158 of the Act.

8 Vulnerabilities and Risks for High Value Dealers

Cash remains the mainstay of much serious organised criminal activity. It has the obvious advantage that it leaves no audit trail and is the most reliable. Criminals tend to use large denominations of currency as it is the easiest to transport and conceal. Consequently, businesses should always exercise additional vigilance when accepting large numbers of high value notes.

Those in receipt of large sums of cash have a problem with how to dispose of it. The objective of the first stage of money laundering – placement – is to move the criminal cash into the financial system. It is extremely difficult to place large amounts of cash into the banking system without raising suspicions. Serious organised criminals frequently launder cash through legitimate and quasi legitimate businesses, typically those with a high cash turnover. The businesses are often owned or part owned by the criminals or by close associates although legitimate businesses may also be duped into providing the means for laundering criminal proceeds. Retail businesses that genuinely accumulate and bank large amounts of cash are natural targets for laundering the cash

through genuine purchases.

Businesses who find themselves in financial difficulties may also be targeted by criminals. Cash may be placed into the banking system by persuading the owners or managers to deposit criminal money along with their normal takings. The business then transfers the criminal money to the money launderer's account taking a cut along the way.

Money launderers normally want to move funds quickly in order to avoid detection. This is more easily done in large one-off transactions. The purchase of high value goods, with great portability, paid for in cash, represents an attractive target for money launderers. Luxury goods paid for with cash that can be easily sold (even at a loss) for "clean money" is especially attractive.

Equally an asset may be purchased to support a certain lifestyle (e.g. a high performance car or yacht). Alternatively, an asset may be purchased as a form of long-term investment (e.g. jewellery, an antique or work of art etc.).

8.1 Gold and Precious Metals

Criminal funds can be used to purchase gold, which is then exported to other jurisdictions and sold, thus legitimising the funds as the proceeds of sale. The use of gold is attractive for many reasons; it is the only raw material comparable to money. It is a universally accepted medium of exchange which is traded on the world markets and the launderer can remain anonymous.

8.2 Precious Stones and Jewellery

Precious stones and jewellery are easily transportable and highly concentrated forms of wealth.

8.3 The Motor Trade

Vehicles may be either the source of the laundered money or the means by which other illegal income is laundered. Money launderers often make contacts within trades in which the use of cash is accepted such as dealers in expensive cars.

9 Anti-Money Laundering Systems and Controls

9.1 Corporate Governance

Corporate governance is the system by which businesses are directed and controlled and the business risks managed. Money laundering and terrorist financing are risks that must be managed in the same way as other business risks.

9.2 Responsibilities of the Board

It is the responsibility of the Board, or senior management, or the owner(s) to ensure that the organisational structure of the business effectively manages the risks it faces.

Part 2, Section 5 of the Code provides the principal responsibilities of the Board. Senior Management, the Money Laundering Compliance Officer and the Money Laundering Reporting Officer will assist the Board in fulfilling these responsibilities.

Larger and more complex business may also require dedicated risk and internal audit functions to assist in the assessment and management of money laundering and terrorist financing risk.

9.3 Responsibilities of Senior Managers

Senior managers are responsible for making sure that the business has carried out a risk assessment for its business and has policies, controls and procedures to help reduce the risk that criminals may exploit the business for financial crime. They are also responsible for approving that risk assessment. The policies, controls and procedures must address the level of risk that the business may encounter in different circumstances.

You must also take account of the size and nature of your business and put in place additional measures to ensure your policies, controls and procedures are being complied with throughout your organisation (including by subsidiaries, branches and agents).

9.4 Policies, Systems and Controls

Establish and Maintain Systems and Controls

Businesses must establish and maintain systems and controls to prevent and detect money laundering and terrorist financing that enable the business to;

- Apply appropriate customer due diligence (CDD) policies and procedures that take into account vulnerabilities and risk. Policies and procedures must include;

- The development of clear customer acceptance policies and procedures.
- Identifying and verifying the identity of the applicant of the business.

- Report to Montserrat's Financial Intelligence Unit when it knows or has reasonable grounds to know or suspect that another person is involved in money laundering or terrorist financing, including attempted transactions.
- Ensure that relevant employees are;
  - adequately screened when they are initially employed,
  - aware of the risks of becoming concerned in arrangements involving criminal money and terrorist financing,
  - aware of their personal obligations and the internal policies and procedures concerning measures to combat money laundering and terrorist financing, and
  - provided with adequate training.

In maintaining the required systems and controls, a firm must ensure that the systems and controls are implemented and operating effectively.

A firm must also have policies and procedures in place to address specific risks associated with non-face to face business relationships or transactions, which should be applied when conducting due diligence procedures.

9.4.1 Internal Controls

A firm must take into account situations that, by their nature, can present a higher risk of money laundering, terrorist financing or proliferation financing, and take enhanced measures to address them. The specific measures depend on the type of customer, identity of the customer, business relationship, jurisdiction, product or transaction, especially large or complex transactions or unusual patterns of activity that have no apparent economic or lawful purpose. Conversely, the measures that you put in place to manage risks associated with lower-risk customers should be less onerous. The risk assessment that you conduct will underpin the nature of your measures for mitigating and managing money laundering, terrorist financing and proliferation financing risks.

The firm must ensure that when new products, business practices or technology are adopted, appropriate measures are taken to assess and if necessary, mitigate any money laundering, terrorist financing or proliferation financing risks that may arise.

A firm must specify the undertaking of additional measures, where appropriate, to prevent the use for money laundering, terrorist financing or proliferation financing of transactions which might favour anonymity. This could include putting in place additional due diligence measures.

When designing systems to identify and deal with suspicious activity, there are some warning signs of potentially suspicious activity that your systems should be capable of picking up and flagging for attention. You will always need to consider the circumstances of each case, which you will need to assess on an individual basis.

Issues which may be covered in an internal controls system include;

9.4.1.1 Customer Due Diligence

- Have in place a proforma to gather core due diligence information which must be used in all high value transactions.
- The level of personnel permitted to exercise discretion on the risk based application of regulations and under what circumstances.
- Monitor and review instances where exemptions are granted to policies and procedures or where controls are overridden.
- When outsourcing of CDD obligations or reliance upon third parties will be permitted and under what conditions.
- How the business will restrict transactions being conducted where CDD has not been completed.
- The circumstances in which delayed CDD is permitted.
- Some types of high value dealers could consider having a contract or commercial arrangement with their customers so that high value payments can be anticipated in advance.
- A business must also have policies and procedures in place to address specific risks associated with non-face to face business relationships or transactions, which should be applied when conducting due diligence procedures.

9.4.1.2 Handling Transactions

- When cash payments will be accepted.

- When payments will be accepted from or made to third parties

9.4.1.3 Identifying and Reporting Suspicious Activity

- The manner in which disclosures are to be made to the MLRO.
- Implementation of a system of recording all transactions above their relevant thresholds on their accounting systems. Recording must include linked transactions for the same customer.
- Consideration of a "till alert" for potential high value transactions or having a policy of only permitting the MLRO or other specified members of staff to deal with high value cash transactions.
- Liaise closely with the Commission and the FIU on matters concerning vigilance, systems and controls.

9.4.2 Monitoring Compliance

All employees involved in the day-to-day business should be made aware of the policies and procedures in place in their business to prevent money laundering and financing of terrorism risks. It is essential for businesses to evaluate compliance by staff with policies and procedures, in particular, CDD, record keeping and suspicious transactions reporting. Best practice indicates that internal testing should be carried out by someone other than the Compliance Officer, to avoid potential conflict since the Compliance Officer is responsible for implementation of the Compliance Programme, its measures and controls.

Staff should be made aware that deliberate non-compliance with procedures for dealing with high value goods will be treated as a disciplinary matter.

Monitoring compliance will assist a firm to assess whether the policies and procedures that have been implemented are effective in managing the risk of money laundering and terrorist financing.

Procedures to be undertaken to monitor compliance may involve:

- Checking records to evidence that ID has been taken and other customer due diligence checks have been carried out when required.

- File checklists to be completed before opening or closing a relationship or single transaction.
- An MLRO's log of situations brought to their attention including queries from staff and reports made.
- How the business rectifies lack of compliance when identified.
- How lessons learnt will be communicated back to staff and fed back into the risk profile of the business.
- If the Compliance Officer is also the most senior employee (person at the highest level in the organization) additional care must be exercised to test compliance with your obligation in respect of AML/CFT obligations.
- Such reviews (whether they may be internal or external) must be documented and made available to the Financial Services Commission.

9.4.3 Compliance Programme

The Compliance Programme is a written document explaining the system of internal procedures, systems and controls which are intended to make the business less vulnerable to money laundering and the financing of terrorism. The Compliance Programme encapsulates the guidance provided in the section policies, systems and controls.

Policies and procedures must relate to:

- Governance and Responsibilities of the Board
- Anti-Money Laundering System and Controls
- Risk Assessment and Management
- Customer Due Diligence
- Identifying and Reporting Suspicious Activity
- The Monitoring and Management of Compliance including the Roles and Responsibilities of the MLCO and MLRO
- Record Keeping

These policies, procedures and controls, must be communicated to employees, and fully implemented. Where appropriate, depending upon the size of the business, the programme should be approved by the Board and/or Senior Management.

The Compliance Programme must be reviewed at a minimum of every two years, or more frequently if the initial and on-going business risk assessment warrants or if there are changes to Legislation, Regulations or The Code.

A well-designed, applied and monitored regime will provide a solid foundation for compliance with the AML/CFT laws. As not all individuals and entities operate under the same circumstances, compliance procedures will have to be tailored to fit individual needs. It should reflect the nature, size and complexity of the operations as well as the vulnerability of the business to money laundering and terrorism financing activities.

10 Risk Based Approach

A risk-based approach is where you assess the risks that your business may be used for money laundering, terrorist financing or proliferation financing and put in place appropriate measures to manage and reduce those risks. An effective risk-based approach will identify the highest risks of money laundering, terrorist financing and proliferation financing that your business faces allowing you to effectively manage and mitigate these risks.

Several features of the high value dealer sector make it attractive to criminals, such as the anonymity of cash, the one-off nature of many transactions and the ease of carrying high value goods across borders.

10.1 Overview

Systems and controls will not detect and prevent all money laundering or terrorist financing. A risk-based approach will, however, serve to balance the cost burden placed on individual business and on their customers with a realistic assessment of the threat of a business being used in conjunction with money laundering or terrorist financing by focusing where it is needed and has the most impact.

The possibility of being used to assist with money laundering and terrorist financing poses many risks to businesses including;

- Criminal and disciplinary sanctions for the business and for individual employees.
- Civil action against the business as a whole and against individuals.

- Damage to reputation leading to loss of business.

These risks must be identified and mitigated as any other risk which the business faces. Such an approach;

- Recognises that the money laundering and terrorist financing threats businesses face vary across customers, jurisdictions, services and delivery channels.
- Allows businesses to differentiate between customers in a way that matches risk in a particular business.
- Establishes minimum standards, allows businesses to apply its own approach to systems and controls and other arrangements in particular circumstances.
- Helps to produce a more cost-effective system.

10.2 Key Concepts

The business portfolio risk assessment will depend on the business's size, type of customers and the practice area it engages in.

Identifying, assessing and understanding money laundering and terrorist financing risks is an essential part of developing an effective AML/CTF regime. It assists in prioritisation and the efficient use of resources. Once risks are understood businesses may apply AML/CTF measures in a way that ensures they are commensurate with those risks.

Assessing Money Laundering and Terrorist Financing Risks are viewed at two levels. Firstly, at the business portfolio level and secondly at the individual customer level. The notes in this section can be applied at both the portfolio and customer level.

A risk assessment views risk as a function of three factors, threat, vulnerability and consequence.

10.2.1 Threat

A threat is a person, group of people, an activity or object which may do harm to the business. In the money laundering/terrorist financing context this includes criminals, terrorist groups, and their facilitators.

10.2.2 Vulnerabilities

In risk assessment vulnerability comprises of those things that can be exploited by the threat or that may support or facilitate those activities.

Looking at vulnerabilities as distinct from threat means focusing upon the factors that represent weaknesses in anti-money laundering and prevention of terrorist financing systems or controls, for example a particular service or product which has certain features which make them attractive for money laundering or terrorist financing purposes.

10.2.3 Consequence

Consequence refers to the impact or harm that money laundering or terrorist financing may cause. The consequences may be short or long term, ranging from prosecution of the individuals concerned, and reputational damage to the business or forfeiture of laundered assets.

Assessing consequences may be challenging, given the lack of clear data and experiences. It is not always necessary to assess consequences in a sophisticated manner, but a high-level understanding of the impact and consequences should be assessed as a benchmark of what may happen.

The key is that any risk assessment adopts an approach that attempts to distinguish the extent of different risks to assist in prioritising mitigation efforts.

10.2.4 Sources of Risk

Sources may be organised into three groupings described below.

10.2.4.1 Country / Geographic Risk

There is no universally agreed definition that prescribes whether a particular country or geographic area represents a higher risk.

Country risk in conjunction with other risk factors provides useful information as to potential money laundering and terrorist financing risks. Money laundering and terrorist financing risks have the potential to arise from almost any source, such as the domicile of the customer, the location of the transaction, and the source of the funding. Countries that pose a higher risk include:

- Countries subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (UN), Office of Financial Sanctions Implementation (OFSI) and Office of Foreign Assets Control (OFAC). In addition, in some circumstances, countries subject to sanctions or measures similar to those issued by bodies such as the UN, but that may not be universally recognised, may be taken into account by a legal professional because of the standing of the issuer of the sanctions and the nature of the measures.
- Countries identified by credible sources as generally lacking appropriate AML/CFT laws, regulations and other measures.
- Countries identified by credible sources as being a location from which funds or support are provided to terrorist organizations.
- Countries identified by credible sources as having significant levels of corruption or other criminal activity.

10.2.4.2 Customer Risk

Determining the potential money laundering or terrorist financing risks posed by a customer, or category of customers, is critical to the development and implementation of an overall risk-based framework. Based on its own criteria, a business should seek to determine whether a particular customer poses a higher risk and the potential impact of any mitigating factors on that assessment. Application of risk variables may mitigate or exacerbate the risk assessment.

Behaviours of customers which may indicate higher risk include:

- An unwillingness to produce evidence of ID or the production of unsatisfactory evidence of ID
- Where the customer is, or appears to be, acting on behalf of another person, an unwillingness to give the name(s) of the person(s) they represent.
- A willingness to bear very high or uncommercial penalties or charges.
- Situations where the source of funds cannot be easily verified.

How the customer comes to the business may also affect the risk:

- Occasional or one-off transactions as opposed to business relationships.
- Introduced business, depending on the effectiveness of the due diligence carried out by the introducer.
- Non face to face transactions.

Risk posed by the products/services the customer is using:

- Do the products allow facilitate payments to third parties?
- Is there a risk of inappropriate assets being placed with, or moving through the business?

Categories of customers whose activities may indicate a higher risk include:

- Brand new customers carrying out large one-off transactions.
- Customers that are not local to the business and for which there is no rational explanation.
- Customers engaged in a business which involves significant amounts of cash
- Politically Exposed Persons (PEPs) are considered as higher risk customers (see section 13.13)
- Customers where the structure or nature of the entity or relationship makes it difficult to identify in a timely fashion the true beneficial owner or controlling interests, such as the unexplained use of legal persons or legal arrangements, nominee shares or bearer shares.
- Customers based in, or conducting business in or through a high risk jurisdiction or a jurisdiction with known higher levels of corruption, organised crime or drug production/distribution.

10.3 Money Laundering Compliance Officer and Money Laundering Reporting Officer.

10.3.1 Overview

Section 8 of the AML Code provides detailed explanation of the roles of the responsibilities of the Money Laundering Compliance Officer (MLCO) and Money Laundering Reporting Officer (MLRO).

The MLCO is required to:

- Develop and maintain systems and controls (including policies and procedures) for both anti-money laundering and prevention of terrorist Financing in line with evolving requirements;
- Undertake regular reviews (including testing) of compliance with policies and procedures to counter money laundering and the financing of terrorism;
- Report periodically to and advise senior management on anti-money laundering and terrorist financing compliance issues that need to be brought to its attention;
- Respond promptly to requests for information made by the Commission or the FIU.

10.3.2 Criteria

Depending upon the size and organisational structure of the business the same person may operate as both the MLCO and the MLRO. In the case of a sole trader the owner adopts, by default, the role of both MLCO and MLRO.

The important factor is the nomination of an individual(s) who will then be expected to take advantage of any available training provided by the Commission, as well as making their own arrangements to up-skill the individual, by means of the various sources of professional qualification.

10.3.2.1 Positioning the MLCO and MLRO within the Organisational Structure.

The appointed person must possess sufficient independence to perform the role objectively having unfettered access to all business lines, support departments and information necessary. Businesses must assess and implement their own approach to the two roles of MLCO and MLRO, within the existing organisational structure and the level of AML/CTF risk assessed.

Organisational matters to be considered are such that the MLRO/MLCO must have;

- Adequate resources including sufficient time.
- An appropriate level of authority within the business.
- Regular contact with the Board or senior management.
- Adequate knowledge and experience in AML and CTF matters.
- Local residency and be employed by the business.

10.4 Outsourcing

Depending upon the nature and the size of the business the roles of the MLCO and the MLRO may require additional support and resources. Where a business elects to bring in additional support or to delegate areas of the MLCO or MLRO functions to third parties, the MLCO and MLRO shall remain directly responsible for their respective roles, and senior management will remain responsible for overall compliance with the Regulations and The Code.

Any arrangement to outsource its compliance function must have the prior approval of the Commission and be covered by way of a contractual agreement in which defined responsibilities must be clearly stated and acknowledged by all parties.

11 High Value Dealer Risk

A high value dealer selling wholesale alcohol with overseas clients presents a completely different risk to a high street jeweller in a small town. However, both may be targeted by criminals if they have little or no controls in place.

The environment you do business in affects the individual customer's risk assessment. If you have many high net-worth customers or deal with people from a particular country or region, this will influence the business wide risk assessment. You should also be aware of the risk of transactions being used for tax evasion, for example dealing in goods where tax has not been declared or understated.

11.1 Risks Your Business May Face

Assessing the risks your business faces will help you understand those risks and how they may change over time, or in response to the steps you take. This will help you design the right systems to spot suspicious activity and ensure that staff are aware of what sort of indicators of possible money laundering they may encounter.

The risks your business may face depends on factors including the nature of the business, how it is structured (e.g., branch network), the areas it operates in, who your customers are, where they are from and the vulnerability of your services or transactions to financial exploitation.

Specific risks in relation to high value dealers are covered in section 8. For each of these areas you must consider how your business could be exposed and put in place policies, controls and procedures to effectively address these. This generalised list is not exhaustive and will depend on individual business circumstances. An effective risk-based approach will require you to identify the risks facing your business, in view of your business' individual characteristics.

11.2 Business Risk Profile

Assessing your business's risk profile will help you design the right systems that will spot suspicious activity and ensure that staff are aware of what sort of money laundering activities they are likely to encounter.

A high value dealer that buys bulk, low value goods presents a different risk profile to a high value dealer that sells high-end luxury cars.

Cash is a key component in organised criminal activity and criminals may try to dispose of cash through the purchase of goods. Because of this, high value dealers must be vigilant to high risk areas.

You should assess the risks to your own business and consider what is high risk in your own policies, controls and procedures. The following is not an exhaustive list of risk indicators:

- assets that are particularly high value and easily portable such as jewellery
- high risk goods that are commonly used to evade tax such as alcohol or tobacco
- businesses with no security or insurance for large volumes of cash
- businesses that have no established presence
- a business you deal with is not applying the standard of due diligence you would expect
- a business wants to use cash for an "off the record" sale
- the customer asks for delivery in an unusual manner or to an address that is not their own
- the customer appears to be breaking down the transaction to fall below the $10,000 limit
- use of cash with no apparent commercial or personal rationale beyond anonymity
- purchasing goods or quantities which are inconsistent with business or personal needs

Low risk indicators should also be included in your risk assessment. The following is not an

exhaustive list of low risk indicators and may not represent low risk in all cases. You must consider this list with regard to your own business practices and risk assessment:

- perishable goods that have a limited life
- local customers that fit with the area and your normal trade models
- highly regulated commodities such as guns.

The risk profile depends on the nature of the business, branch network, customers, and activities. For each of these areas exposure should be considered. For example:

- how risk management procedures will be applied to a network of branches or other services your business may offer e.g., foreign currency exchange
- how management and maintain records and the type of records will be applied
- if a random number of customer files were selected, would all selected files contain a risk assessment and adequate customer due diligence for the customer and beneficial owners
- whether a system is in place to identify where individuals, departments or branches are not implementing risk management procedures
- being able to demonstrate that all staff have been trained on the regulations and provided with ongoing training on recognising and dealing with suspicious transactions
- are staff able to identify the MLRO, what the firm's policies are and where they can be found.

11.3 Risk Assessment

Risk assessment identifies the risks a business is exposed to. A firm should be able to understand all the ways that its business could be exposed to money laundering, terrorism financing and proliferation financing risks, and design systems to deal with them.

A firm must:

- ensure its risk assessment identifies and monitors the risks of money laundering, terrorist financing and proliferation financing that are relevant to its business including those posed by:
    - customers and any underlying beneficial owners (see sector guidance on customer due diligence on who is the beneficial owner) and financing methods
    - services or transactions provided by your business
    - delivery channels, for example cash over the counter, wire transfer or cheque

- geographical areas of operation, including sending money to, from or through high risk third countries, for example **countries identified by HM Treasury, FCDO or FATF** as having deficient systems to prevent money laundering, terrorist financing or proliferation financing.
- size and nature of your business

The risk assessment must be in writing (this should be in a digital format) and kept up to date. It needs to reflect changes in the business and the environment that it does business. At least an annual review of the risk assessment is recommended, and any revisions noted in the document.

The risk assessment must be given to the FSC when requested, as well as the information on which the risk assessment was based and any records required to be kept, under regulation 13.

The business-wide risk assessment must take account of the full range of circumstances associated with your business model. The risk assessment must consider the risk factors relating to:

- Its customers
- the countries or geographic areas it operates in
- its products or services
- its transactions
- its delivery channels.

The risk assessment should also include the following non-exhaustive list:

- delivery channels: the way the customer comes to the business affects the risk for
  - non face-to-face customers
  - face to face customers
  - occasional transactions, as opposed to ongoing business
- does the pattern of behaviour, or changes to it, pose a higher risk?
- if you accept customer introductions from an agent or third party, have you accepted customers from this source before?
- are customers companies, partnerships, trusts or some combination of these?
- do you undertake business in areas with a highly transient population?
- is the customer base stable or does it have a high turnover?
- do you act for international customers or customers you do not meet?

- do you accept business from abroad?
- do you act for entities that have a complex ownership structure or a cross border element?
- do you accept payments that are made to or received from third parties?
- do your customers fall into categories which indicate that they should be looked at more carefully than other customers that present a low apparent risk of money laundering, terrorist financing, and proliferation financing – for example:
    - customers carrying out large, one-off cash transactions
    - customers that are not local to the business
    - individuals in public positions and/or locations that carry a higher exposure to the possibility of corruption, including politically exposed persons (see sector guidance on politically exposed persons)
    - complex business ownership structures with the potential for concealing beneficiaries?

Other situations that may present a higher risk and need to be considered in your risk assessment are covered in the enhanced due diligence at Appendix B and levels of risk connected with politically exposed persons.

11.4 Internal Controls and Procedures

Once the risks of money laundering, terrorist financing and proliferation financing associated with the business has been identified and assessed, appropriate controls and procedures to reduce and manage them must be established. They will help to decide the appropriate level of due diligence to apply to each customer and beneficial owner. It's likely that there will be a standard level of due diligence that will apply to most customers (who will present a relatively low risk of money laundering and terrorist financing), based on your business' risk assessment.

Procedures should be easily accessible to staff and detailed enough to allow staff to understand and follow them easily. They should set out:

- the types of customers and transactions that you consider to be lower risk and why they qualify for simplified due diligence and those that are higher risk and merit closer scrutiny;
- how to carry out customer due diligence, the identification requirements for customers and beneficial owners and how to carry out enhanced due diligence on higher risk customers;
- any other patterns or activities that may signal that money laundering, terrorist financing or

proliferation financing is a real risk in connection with an individual customer/transaction;

- how to identify politically exposed persons and what to do when one is identified, in particular, how to identify their source of wealth and source of funds;
- what to do if you are dealing with an individual subject to the sanctions regime or who is based in a jurisdiction of concern;
- how to keep records, and where and for how long they should be kept;
- how and when to conduct ongoing monitoring of transactions and customers;
- clear staff responsibilities and the name and role of the MLRO/MLCO;
- how to audit and monitor the policies and procedures and the internal controls in place to ensure that the policies and procedures are followed correctly by staff;
- how to report suspicious activity to the MLRO, and how the MLRO should make a report to the FIU;
- how and when staff are trained and how that training is recorded.

Examples of risk-based controls could include:

- introducing a customer identification and verification programme that varies depending on the assessed level of risk
- requiring additional customer identity evidence in higher risk situations
- reviewing low risk customers and applying more due diligence where changes are apparent which alter the risk profile associated with a customer
- varying the level of monitoring of customer transactions and activities depending on the assessed level of risk or activities that might be unusual or suspicious.

This list is not exhaustive and should not be treated as a checklist. You could also have other risk-based controls depending on the circumstances of your business.

Identifying a customer or transaction as high risk does not automatically mean that they are involved in money laundering, terrorist financing or proliferation financing. Similarly, identifying a customer or transaction as low risk does not mean that they are not involved in money laundering, terrorist financing or proliferation financing.

The risk assessment of a customer must reflect the risk of that particular customer, your business-wide risk assessment, and take into account risks highlighted by the FSC. Declining a business

relationship should be a last resort, when you have concluded that it is not possible to effectively manage the money laundering, terrorist financing or proliferation financing risks associated with a particular customer.

11.5 Effectiveness of Controls

Managing the money laundering, terrorist financing and proliferation financing risks to your business is an ongoing process, not a one-off exercise.

The risk assessment procedures and controls, such as internal compliance audits, must be documented as this helps to keep them under regular review. There should be a process for monitoring whether the processes are working effectively, whether updates are required, for example to reflect changes in the business environment, such as new product types or business models.

12 Customer Due Diligence (CDD)

12.1 Introduction

High Value Dealers which accept cash payments of greater than $35,000 (in any currency), must apply Customer Due Diligence prior to entering into the transaction or relationship.

Part 3 of the Code provides extensive detail on the requirements of Customer Due Diligence. Customer due diligence has two elements:

- Identifying the customer.
- Understanding sufficiently about the customer to assess that the transaction and the funding is from a legitimate source.

Identification itself also has two elements:

- Identity information provided by the customer which distinguishes one person from another; e.g name, date of birth, gender and country of birth, etc.
- Verification: which is obtaining of reputable documentation which **verifies the information** provided by the customer.

Identity information is usually captured by the completion of an application form (or equivalent)

and followed by the provision of a recognizable, government issued document, e.g. passport.

If a prospective customer cannot satisfy the basic due diligence measures for example unable to identify and verify their identity or provide sufficient information about the nature and purpose of a transaction, then the transaction must not be carried out and the business relationship must not be established.

12.2 When Due Diligence Measures must be Applied

Customer due diligence must be applied when:

- When establishing a business relationship.
- When carrying out an occasional transaction.
- Where there is a suspicion of money laundering or terrorist financing.
- Where there are doubts about previously obtained customer identification information.
- At appropriate times to existing customers on a risk sensitive basis.

However, if it is necessary not to interrupt the normal conduct of business and there is little risk of money laundering or terrorist financing occurring, then verification may take place during the establishment of the business relationship, provided it is done as soon as is practicable after contact is first established.

12.3 Why it is Necessary to Apply CDD Measures

Undertaking satisfactory customer due diligence prior to entering into a relationship or undertaking a high value transaction will help to provide necessary safeguards. Customers arriving without notice may not have the necessary ID to hand to enable the customer due diligence checks to be undertaken. Customers must be advised that high value cash payments cannot be accepted until identity has been verified and the nature and purpose of the transaction has been checked.

12.3.1 Identifying the Customer

Most customers can be expected to present a passport or drivers licence to verify identity. A customer may present a driver's licence to verify residential address, however, this cannot be accepted if it has already been used to verify identity. In these cases, a current utility bill or bank statement showing the residential address can be used.

When accepting such evidence from a customer, it is important that staff make sufficient

checks on the evidence provided to satisfy them that it is valid, it does indeed relate to that customer and that it all makes sense on a cumulative basis.

12.3.2 Checks on Photo ID

Checks on photo ID may include:

- A visual likeness against the customer;
- Whether the date of birth on the evidence matches the apparent age of the customer;
- Whether the document is still current;
- Whether the spelling of names is the same as on other documents provided by the customer.

12.3.3 Checks on Documentary Evidence of Address

Checks on documentary evidence of address may include:

- Whether the address matches that given on the photo ID (if quoted on ID document);
- Whether the name of the customer matches with the name on the photo ID;
- Whether the document is current and;
- If the evidence contains a date of birth, whether this also matches up with the ID evidence received.

12.4 Ascertaining Funds and Wealth are from a Legitimate Source.

12.4.1 Source of Funds

The source of funds for each applicant customer must be established.

Source of funds is regarded as the activity which generates the funds for the transaction e.g. a customer's occupation or business activities. Information concerning the geographical sphere of the activities may also be relevant.

This Guidance stipulates record keeping requirements for transaction records which require information concerning the remittance of funds also to be recorded (e.g. the name of the bank and the name and account number of the account from which the funds were remitted). This is the source of transfer and must not be confused with source of funds.

12.4.2 Source of Wealth

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

In determining source of wealth, it will often not be necessary to establish the monetary value of an individual's net worth.

12.4.3 Regular Customers whose Identity has Already been Verified.

Regular customers whose identity has already been verified and whose details have not changed need not be re-verified whenever further transactions are to take place. However, the identification information must have been retained and it must still be relevant and up to date. To ensure that this is the case, businesses may wish to consider offering a loyalty card through which special offers can be obtained or early notification of sales can be advised. This will enable the customer's name, address and occupation to be kept up to date.

12.5 Occasional Transactions

Part 2 Section 5 of the Regulations requires that customer due diligence measures must be applied when a business carries out occasional transactions. Schedule 1 (7) of the Regulations defines an occasional transaction.

12.6 Attempted Transactions

If a customer attempts a transaction and for whatever reason it is not completed and if it is considered suspicious then it must be reported to the FIU.

12.7 Risk Approach to Customer Due Diligence

Regulation 12 requires that the extent of customer due diligence measures must be decided on a risk sensitive basis depending upon the type of customer, business relationship or transaction.

Businesses must be able to demonstrate that the due diligence measures that have been applied are

appropriate in view of the risk of, money laundering and terrorist financing faced by each business.

Using the risk characteristics identified following the business level risk assessment, customer on boarding should include a risk assessment of each customer. Businesses are expected to assess the inherent AML and CTF risk associated with each individual new customer and also re- assess that risk periodically.

12.7.1 Customer Profile

It is necessary to prepare a profile for each customer on the basis of expected activity and transactions.

The customer profile must contain sufficient information to identify:

- A pattern of expected business activity and transactions within each customer relationship; and
- Unusual, complex or higher risk activity and transactions that may indicate money laundering or terrorist financing activity.

12.8 Other Customer Due Diligence Matters

12.8.1 Is the Customer Acting for a Third Party?

Reasonable measures must be taken to determine whether the customer is acting on behalf of a third party.

Such cases will include where the customer is an agent of the third party who is the beneficiary and who is providing the funds for the transaction. In cases where a third party is involved, information on the identity of the third party and their relationship with the customer must be obtained.

In deciding who the beneficial owner is in relation to a customer who is not a private individual, (e.g., a company or trust) it is essential to look behind the corporate entity to identify those who have ultimate control over the business and the company's assets, with particular attention paid to any shareholders or others who inject a significant proportion of the capital or financial support.

Reference should be made to the Code for further information on the concept of beneficial ownership.

Particular care should be taken to verify the legal existence and trading or economic purpose of corporates and to ensure that any person purporting to act on behalf of the company is fully authorized to do so.

12.8.2 High Risk Customer/ Transactions

There are several customers and types of transactions, services and products which may pose higher risk to a business.

Where a relationship or transaction is assessed as presenting a higher risk, businesses must perform appropriate Enhanced Due Diligence (EDD).

Where a relationship or transaction involves a Politically Exposed Person (PEP) then it must always be considered to present a higher risk.

A business must apply one or more enhanced due diligence measures with higher risk customer relationships. The nature of the measures to be applied will depend on the circumstances of the relationship or transactions and the factors leading to the relationship being considered as higher risk.

Enhanced due diligence measures include:

- Requiring higher levels of management approval for higher risk new customer relationships.
- Obtaining further Customer Due Diligence (CDD) information (identification information and relationship information, including further information on the source of funds and source of wealth), from customer or independent sources, such as the internet, public and commercially available databases.)
- Taking additional steps to verify the CDD information obtained.
- Commissioning due diligence reports from independents experts to confirm the veracity of CDD information held.
- Requiring more frequent review of customer relationships.

- Requiring the review of customer relationship to be undertaken by the compliance function, or other employees not directly involved in managing the client relationship; and
- Setting lower monitoring thresholds for transactions connected with the customer relationship.

12.9 Politically Exposed Persons (PEPs)

Corruption by some high-profile individuals, generally referred to as PEPs inevitably involves serious crime, such as theft or fraud and is of global concern. The proceeds of such corruption are often transferred to other jurisdictions and concealed through private companies, trusts or foundations, frequently under the names of relatives or close associates. Such situations may involve the acquisition of high value goods.

By their very nature, money laundering investigations involving the proceeds of corruption generally gain significant publicity and are therefore very damaging to the reputation of both businesses and jurisdictions concerned, in addition to the possibility of criminal charges.

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

The risk of handling the proceeds of corruption, or becoming engaged in an arrangement that is designed to facilitate corruption is greatly increased when the arrangement involves PEP. Where the PEP also has connections to countries or business sectors where corruption is widespread, the risk is further increased.

PEP status itself does not of course, incriminate individuals or entities. It will however put an applicant for business or customer into a higher risk category.

13 Monitoring Customer Activity

13.1 Introduction

It is accepted that most of the activity involving high value goods is by way of single transactions however it is not uncommon that ongoing relationships may develop.

Businesses must, as part of its on-going customer due diligence procedures, establish appropriate customer activity and transaction monitoring procedures to monitor customer relationships and put in place procedures to identify and scrutinise complex, and/or unusual higher risk activity.

Monitoring must consist of:

- Scrutiny of transactions, including where necessary the source of funds to ensure that the transactions are consistent with the business's knowledge of the customer, their business and risk profile.

- Ensuring that the documents, data, or information held evidencing the customer's identity is up to date.

The extent to which scrutiny of transactions and knowledge of customer enquiries are undertaken should be determined using the risk-based approach and must be applied in accordance with the risks that are assessed to be present in relation to the customer, products, transactions, delivery channels and geographical locations involved.

High value dealers should bear in mind that it is not only new clients who may attempt to launder funds through their business. Regular and established customers may also become involved with criminal activity or may have deliberately sought to build up a relationship of trust before using the business for criminal purposes.

The due diligence that has been obtained and kept up to date in respect of all established and regular customers should be used to provide answers to the following questions on each occasion that a new transaction takes place.

- Is the transaction reasonable in the context of the normal business and expectations for that customer?
- Is the size and frequency consistent with the customer's normal purchase or for that type of customer?
- Has the pattern of transactions changed since the business relationship was established?
- Has there been a significant or unexpected improvement in the customer's financial position? – particularly where they are unable to provide any plausible explanation for where the money

came from.

13.2 Approach to Monitoring

For the purposes of this section "monitoring" does not oblige businesses to function as, or assume the role of, a law enforcement or investigative authority vis-a-vis his or her customer. It refers to maintaining awareness throughout the course of work for a customer to money laundering or terrorist financing activity and/or changing risk factors.

The more a business knows about its customers and develops an understanding of the instructions, the better placed it will be to assess risks.

- A monitoring system should take into account its business risk assessment
- The size and complexity of the business
- The nature of its services and transactions.
- Where it is possible to establish appropriate standardised parameters by unusual activity by comparing activity or customer profiles with that of similar peer group of customers and
- The monitoring procedures that already exist to satisfy other business needs.

The monitoring system should:

- Flag up transactions and/or activities for further examination.
- Make available reports or information which is reviewed promptly and by the right person.
- Enable appropriate action to be taken on the findings of any further examination.

Monitoring can either be:

- In real time, in that transactions and/or activities can be reviewed as they take place or are about to take place, or
- After the event, through some independent review of the transactions and/or activities that a customer has undertaken.

Businesses should also assess the adequacy of any systems, controls and processes on a periodic basis. Monitoring programs can fall within the system and control framework developed to manage the risk of the business. The results of the monitoring should also be documented.

In summary monitoring is not a mechanical process and does not necessarily require sophisticated

electronic systems. The scope and complexity of the process will be influenced by the business's business activities, and whether the business is large or small. The key elements of any system are having up to date customer information, on the basis of which it will be possible to spot the unusual, and asking pertinent questions to prompt the reasons for unusual transactions or activities in order to judge whether they may represent something suspicious.

13.3 Recognising Suspicious Behaviour and Unusual Instructions

13.3.1 Linked Transactions

High value dealers must have some means of identifying linked cash transactions for the same customer. Staff will need to be trained to recognise customers who return for repeat purchases over a short period of time and pay for goods in cash that have been broken down into a number of separate operations with the possible aim of avoiding identification or due diligence checks.

To assist this exercise, businesses may wish to consider offering a loyalty card through which special offers can be obtained or early notification of sales can be advised.

Businesses must have adequate systems in place to identify transactions in deciding whether there is a risk that transactions are being deliberately split into separate operations. The business needs to consider the circumstances of the transactions. For example:

- Are a number of transactions carried out for the same customer within a short space of time?
- Could a number of customers be carrying out transactions on behalf of the same individual or group of individuals?

13.3.2 Goods that are Returned for Refund

Returning high value goods paid for in cash and obtaining a refund by way of a cheque enables the laundering of dirty money by exchanging it for a legitimate retailer's cheque. Suspicions may be raised in the following circumstances.

- The customer enquires about the business' refund policy prior to purchasing.
- The customer seeks a refund for spurious reasons.
- The customer seeks the repayment in the form of a cheque when the purchase or deposit was made in cash.

13.3.3 Buying in Second-Hand Goods

High value dealers who buy-in high value second-hand items for trading should be vigilant to avoid handling stolen property. A money launderer who has exchanged criminal cash for a high value asset and then trades it in has a cheque that can be paid into his bank account. He has therefore effectively "placed" and "integrated" the laundered money. Jewellers, art and antique dealers should use their networking to exchange information when stolen goods are being offered around for sale.

13.3.4 Recognising Other Potentially Suspicious Transactions or Activity

- Reluctance to make personal contact.
- Reluctance to provide the required identification information or evidence of the customer.
- The size of the purchase is out of line with the appearance/age of the customer.
- Customers who initially indicate that they will be paying for goods over EC$37,500 (or the equivalent in any currency) by credit card or cheque and then at the last minute present cash as a means of payment.
- There appears to be no genuine reasons for paying large sums of money in cash.
- Cash is unusual for that type of customer.
- Customers purchasing goods which are available nearer home at a similar price.
- Purchases by businesses where the level of cash activity is higher than the underlying business would justify.

14 Reporting Suspicious Activity and Transactions

14.1 Legislation

Section 122 (1) of the POCA prescribes:

"Where a person:-

a) knows or suspects or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering; and
b) the information or other matter on which his knowledge or suspicion is based or which gives reasonable grounds for such knowledge or suspicion, came to him in the course of a relevant business;

he shall disclose the information or other matter as soon as is practicable after it comes to him to the relevant Money Laundering Reporting Officer or to the Financial Intelligence Unit (FIU).

14.2 What Constitutes Knowledge or Suspicion

14.2.1 Knowledge

Knowledge means actual knowledge.

14.2.2 Suspicion

The test for whether a person holds a suspicion is a subjective one. If someone thinks a transaction is suspicious they are not expected to know the exact nature of the criminal offence or whether those particular funds were arising from a crime? They may have noticed something unusual or unexpected and, after making enquiries, the facts do not seem normal or make commercial sense. There does not have to be evidence that money laundering is taking place for there to be a suspicion.

If someone has not yet formed a suspicion, but they have cause for concern, a business may choose to ask the customer or others more questions. The choice depends upon what is already known, and how easy it is to make enquiries.

14.2.3 Reasonable Grounds to Suspect

A person would commit an offence even if they did not know that or suspect that a money laundering offence was being committed, if they had reasonable grounds for knowing or suspecting that it was.

If there are factual circumstances from which an honest and reasonable person, engaged in a similar business, should have inferred knowledge or formed the suspicion that another was engaged in money laundering or that there was knowledge of circumstances which would put a reasonable person to enquiry, it is important that staff do not turn a blind eye to information that comes to their attention.

Reasonable enquiries should be made, such as a professional in a particular profession based upon their qualifications, experience and expertise might be expected to make in such a

situation within the normal scope of their customer relationship.

Exercising a healthy level of professional scepticism should be adopted. If in doubt a professional should exercise a level of caution and report to the businesses MLRO.

14.3 Failure to Report

Failure to report to the FIU, knowledge or suspicion of crime proceeds or terrorist property is a criminal offence. If such a transaction is allowed to continue despite there being reasonable grounds to believe that the funds are criminal proceeds or terrorists' funds and a report is not submitted to the FIU then an offence of money laundering or financing of terrorism may have been committed.

14.4 Reporting Procedures

Suspicious activity reports should be made as soon as practicable after it has been determined that there are reasonable grounds to suspect money laundering, terrorist financing or any criminal activity is involved. Making a report takes precedence over customer confidentiality considerations. However, there is no obligation to report information that does not relate to the suspicious circumstances.

It is the responsibility of the Money Laundering Reporting Officer to submit Suspicious Activity Reports to the FIU.

The relationship between reporting entities and the FIU is a key one, because the FIU can only perform its analytical function to produce financial intelligence if the various reporting entities report the critical information they have.

14.4.1 Internal Reporting Procedures

Businesses need to have a system clearly setting out the requirements to submit an internal SAR. These may include:

- The circumstances in which a disclosure is likely to be required;
- How and when information is to be provided to the MLRO;
- Resources which can be used to resolve difficult issues around making a disclosure;

- How and when a disclosure is made to the FIU;
- How to manage a customer relationship when a disclosure is made while waiting for consent from the FIU as to whether to continue the business relationships;
- The need to be alert to tipping off issues.

Once employees have reported their suspicions under internal procedures to the MLRO, they have fully satisfied their statutory obligations.

14.5 Evaluation of SARS by MLRO

In order to demonstrate that a report is considered in light of all relevant information when evaluating a suspicious activity report, the MLRO may:

- Review and consider transaction patterns and volumes, previous patterns of instructions, the length of the business relationship and CDD information; and
- Examine other connected accounts or relationships. Connectivity can arise through commercial connections, such as transactions to or from other customers or common introducers, or through connected individuals, such as third parties, common ownership of entities or common signatories.

However, the need to search for information concerning connected accounts or relationships should not delay the making of a report to the FIU.

14.6 Reports to FIU

The MLRO will submit Suspicious Activity Reports (SARs) to the FIU in writing or electronically via email or they may be delivered by hand. A copy of the SAR form is available by contacting the Commission on 664-491-6887/8 or info@fsc.ms or they can be provided by contacting the FIU directly at 664-491-2766 or fcimni@live.co.uk.

A SAR must be made as soon as it is reasonably practicable to do so once knowledge or suspicion, or reasonable grounds to know or suspect, has been formulated. As such it must be made either before a transaction occurs, or afterwards, if knowledge or suspicion is formulated with the benefit of hindsight after a transaction or activity occurs.

Businesses should keep comprehensive records of suspicions and disclosures because disclosure of

a suspicious activity or transaction is a defence to criminal proceedings. Such records may include notes which contain:

- on-going monitoring undertaken and concerns raised by fee earners and staff;
- discussions with the MLRO regarding concerns;
- advice sought and received regarding concerns;
- why the concerns did not amount to a suspicion and a disclosure was not made;
- copies of any disclosures made;
- conversations with FIU, insurers, supervisory authorities etc. regarding disclosures made; and
- decisions not to make a report to FIU which may be important for the MLRO to justify his position to law enforcement.

14.7 Tipping Off

Care should be taken to ensure that the customer does not become aware (i.e. is not tipped off) about the reporting of suspicion. Further enquiries do not need to be made to back up suspicion. These will be made by the authorities. If the suspicion has arisen before the transaction has been completed, consent to complete the transaction must be obtained from the FIU.

When a SAR has been submitted to the FIU, no member of staff may disclose that such a Report or the content of such Report to any person including the customer. It is an offence to deliberately tell any person, including the customer, that the business has filed a suspicious transaction report about the customer's activities/transactions.

14.7.1 Normal Enquiries

High value dealers should never be afraid to ask questions in respect of unusual circumstances. Many of these questions can be posed as genuine commercial enquiries to ensure that the customer obtains the best advice in the circumstances. Where the answers or reaction from the customer do not pass the "does it make sense test" and a suspicion of money laundering or criminal activity is formed a suspicious activity report should be made to the FIU.

It is not tipping-off to include a paragraph about a business' obligations under the money laundering legislation in any business-related communication with the customer.

In circumstances where a SAR has been filed with the FIU, but CDD procedures are incomplete, the risk of tipping-off a client (and its advisers) may be minimised by: ensuring that employees undertaking due diligence enquiries are aware of tipping-off provisions and are provided with adequate support, such as specific training or assistance from the MLRO; obtaining advice from the FIU where a financial services business is concerned that undertaking any additional due diligence enquiries will lead to the customer being tipped-off; and obtaining advice from the FIU when contemplating whether or not to ask for non-routine information or questions in relation to such customers.

14.8 Consent to Activity

14.8.1 Pre-Transaction Consent

When a SAR is made before a suspected transaction or event takes place FIU consent must be obtained before the event occurs. Consent will only be given in respect of that particular transaction or activity and future transactions or activity should continue to be monitored and reported as appropriate.

In the vast majority of instances in which a SAR for consent is made to the FIU, consent to continue an activity or to process a suspected transaction will be provided within seven days of receipt of a report. Whilst this is what generally occurs in practice, the FIU is not obliged under the legislation to provide consent within a particular timeframe, or at all. In particular, consent may be delayed where information is required by the FIU from an overseas financial intelligence unit.

14.9 Terminating the Relationship

A business is not obliged to continue relationships with customers if such would place them at commercial risk. However, to avoid prejudicing an investigation, the FIU may request that a relationship is not terminated.

If a business, having filed a SAR, wishes to terminate a relationship or transaction, and is concerned that, in doing so, it may prejudice an investigation resulting from the report, it should seek the consent of the FIU to do so. This is to avoid the danger of tipping off.

15 Employee Training and Awareness

15.1 Overview

Awareness training and training of staff is one of the best ways of managing money laundering and terrorist financing risks.

Training should be delivered to all senior management, customer facing staff and those involved in transaction processing or monitoring. Employees should be trained in what they need to do to carry out their particular role in the organisation. All customers facing staff will require training in relation to recognising and handling suspicious transactions.

Money Laundering Reporting Officers and Money Laundering Compliance Officers, senior managers and others involved on ongoing monitoring of business relationships and other internal control procedures will need different training tailored to their particular functions.

Where businesses have a number of sites which do not all accept High Value Payments (HVPs) they should introduce a policy of not accepting HVPs. In addition to the policy, businesses must also introduce sufficient controls to ensure HVPs are not accepted at any of their unregistered sites. For example, businesses should ensure that all staff are aware of the business's policy and carry out management checks to ensure such payments do not occur by mistake.

15.2 Obligations

Businesses must provide their staff with appropriate and proportional AML/CFT training. There must be a commitment to having appropriate controls to include both training and awareness. This requires a business-wide effort to provide all relevant employees with at least general information on AML/CFT laws, regulations and internal policies. To satisfy a risk-based approach, particular attention should be given to risk factors or circumstances occurring in the entity's own business.

Employers are encouraged to produce continuing education programs on AML/CFT and the risk-based approach.

Applying a risk-based approach to the various methods available for training however, gives each business flexibility regarding the frequency, delivery mechanisms and focus of such training. Business management should review their own staff and available resources and implement

training programs that provide appropriate AML/CFT information that is:

- Tailored to the relevant staff responsibility (*e.g.* customer contact or administration). At the appropriate level of detail (*e.g.* considering the nature of services provided by the legal professional).
- At a frequency suitable to the risk level of the type of work undertaken by the legal professional.
- Used to assess staff knowledge of the information provided.

15.3 Vetting of Staff

A strong control environment will have appropriately vetted staffs that are:

- Alert to money laundering and terrorist financing risks.
- Well trained in the identification of unusual or higher risk activities or transactions, which may indicate money laundering or terrorist financing activity.

The effective application of even the best designed control systems can be quickly compromised if staff lacks competence or probity, are unaware of or fail to apply systems and controls and are not adequately trained. In particular, sales staff will provide the business with its strongest defence or weakest link.

A business should also encourage its sales staff and other staff to "think risk" as they carry out their duties within the legal and regulatory framework governing money laundering and terrorist financing.

15.4 Scope of Training

Businesses must ensure that relevant employees are made aware of their responsibilities under the POCA, the AML/CFT Regulations and the AML/CFT Code, to report knowledge of or suspicion of AML/CFT to the MLRO and to apply customer due diligence measures.

Training to enable employees to recognise and deal with suspicious transactions should include:

- The identity of the Money Laundering Reporting Officer (MLRO);
- The potential effects on the firm, its employees personally and its clients of any breach in the

law;

- The risks of money laundering and terrorist financing that the business faces;
- The vulnerabilities of the business's products and services;
- The policies and procedures that have been put in pace to reduce and manage the risks;
- Customer due diligence measures and where relevant, procedures for monitoring customers transactions;
- How to recognise potential suspicious activity;
- The procedures for submitting a report to the MLRO;
- The circumstances when consent is to be sought and the procedure to follow;
- Reference to industry guidance and other sources of information, for example, FATF.

15.5 Evidence of Training

A business must keep evidence of its assessment of training needs and the steps taken to meet those needs. You may be asked to produce training records in court.

Training records include:

- a copy of the training materials
- details of who provided training, if provided externally
- a list of persons who have completed training, with dates, and their signatures (confirming their understanding of the obligations) or electronic training records
- a planned training schedule.

15.6 Frequency of Training

Businesses should ensure that the frequency of training is sufficient to maintain the knowledge and competency of staff to apply customer due diligence measures appropriately and in accordance with the business' risk assessments of the products and services they offer.

It is important, as part of ongoing training, to make staff aware of changing behaviour and practices amongst money launderers and those financing terrorism. A range of information on this can be found on the internet, and through the media, for example, the website of the Financial Action Task Force, www.fatf-gafi.org.

Training methods and assessment should be determined by the individual business according to its size, and complexity.

For full details on employee training and awareness, please refer to Part 6 section 38 of the Code.

16 Record Keeping

The record keeping obligations are essential to facilitate effective investigation, prosecution and confiscation of criminal property.

Businesses should ensure that they keep records in the manner as prescribed by Regulation 13

Businesses that operate from temporary sites for example, jewellers at trade shows, must also keep records of where and when these events took place.

Records must be kept in a manner which allows for swift reconstruction of individual transactions and provides evidence for prosecution of money laundering and other criminal activities.

Records may be kept in electronic or written form for a period of five (5) years after the end of the business relationship or completion of a one-off transaction.

If a business outsources record keeping to a third party, the business remains responsible for the record keeping requirements of the AML/CTF Regulations and the Code.

For full details on employee training and awareness, please refer to Part 7, sections 39 to 45 of the Code.

16.1 Minimum Requirements

A business must retain:

- copies of the evidence obtained to satisfy customer due diligence obligations and details of customer transactions for at least five years after the end of the business relationship;
- details of occasional transactions for at least five years from the date of the transaction;
- details of actions taken in respect of internal and external suspicion reports;
- details of information considered by the MLRO in respect of an internal report, where the MLRO officer does not make a suspicious activity report;

- copies of the evidence obtained if you are relied on by another person to carry out customer due diligence, for five years from the date that the third party's relationship with the customer ends, the agreement should be in writing.

A business must also maintain a written record of:

- risk assessment and any changes made;
- policies, controls and procedures and any changes made;
- steps taken to ensure staff are aware of the money laundering and terrorist financing legislation and related data protection requirements, as well as the training given to staff.

17 Appendix A - Red Flag Indicators

17.1 New Customers and Occasional or "One Off" Transactions

- Checking identity is proving difficult.
- The customer is reluctant to provide details of their identity.
- There are no genuine reasons for paying large sums of money in cash.
- Cash payment is only mentioned by the customer at the conclusion of the transaction.
- Instruction on the form of payment changes suddenly just before the transaction goes through.
- The goods purchased and/or the payment arrangements are not consistent with normal practice for the type of customer concerned.
- A cash transaction is unusually large.
- The customer will not disclose the source of the cash.
- The explanation by the business and/or the amounts involved is not credible.
- The customer is buying from an unusual location in comparison to their locations.
- A series of transactions are structured just below the regulatory threshold for due diligence identity checks.
- The method of delivery is unusual, for example, a request for immediate delivery, delivery to an address other than the customers address or the loading of high volume / bulky goods immediately into the customers own transport.
- Transactions having no apparent purpose or which makes no obvious financial sense, or which seems to involve unnecessary complexity.
- Unnecessary routing of funds through third parties.
- Enquires about the business's refund policy.
- Seeks a refund for spurious reasons.
- Seeks repayment in the form of a cheque.
- Customer indiscriminately purchases merchandise without regard for value, size, or colour.
- Purchases or sales that is unusual for client or supplier.
- Unusual payment methods, such as large amounts of cash, multiple or sequentially numbered money orders, traveller's cheques, or cashier's cheques, or payment from third- parties.
- Attempts by client or supplier to maintain high degree of secrecy with respect to the transaction, such as request that normal business records not be kept.
- Customer is reluctant to provide adequate identification information when making a purchase.

- Transactions that appear to be structured to avoid reporting requirements.
- A customer orders item, pays for them in cash, cancels the order and then receives a large refund.
- A customer asking about the possibility of returning goods and obtaining a cheque (especially if the customer requests that cheque be written to a third party).
- Purchase appears to be beyond the means of the client based on his stated or known occupation or income.
- Customer may attempt to use a third party cheque or a third party credit card.
- Transaction lacks business sense.
- Purchases or sales that are not in conformity with standard industry practice.

17.2 Regular and Established Customers

- The transaction is different from the normal business of the customer.
- The size and frequency of the transaction is not consistent with the normal activities of the customer.
- The pattern of transactions has changed since the business relationship was established.

17.3 Examples where Customer Identification Issues have Potential to Indicate Suspicious Activity

- The customer refuses or appears reluctant to provide information requested.
- There appears to be inconsistencies in the information provided by the customer.
- The customers residence is inconsistent with other profile details such as employment.
- An address appears vague or unusual.
- The supporting documentation does not add validity to the other information provided by the customer.
- The customer is in a hurry to rush a transaction through with premises to provide the information later.

17.4 Examples of Activity that Might Suggest Potential Terrorist Activity

- The customer is unable to satisfactorily explain the source of income.
- Frequent address changes.

- Media reports of suspected or arrested terrorists or groups.

18 APPENDIX B – Extended Customer Due Diligence Measures

18.1 Extent of Customer Due Diligence Measures

The extent of customer due diligence measures depends on the degree of risk. It depends on the type of customer, business relationship, product or transaction.

It goes beyond simply carrying out identity checks to understanding the customer being dealt with. This is because even people you already know well may become involved in illegal activity at some time, for example if their personal circumstances change or they face some new financial pressure. The due diligence measures should reduce the risk of this, and the opportunities for staff to be corrupted.

This means that the level of identification, verification and ongoing monitoring that is necessary, depending on the risk you assessed must be considered. The business should be able to demonstrate that the extent of these procedures is appropriate when asked to do so.

Using the risk assessment, should assist to determine the extent of due diligence you will conduct depending on the type of customer you will be checking, i.e., the entity who is making the payment to you or the entity you are paying. The types of checks you undertake will differ for each, as the risks associated with them will vary.

For example, if a customer attempts to make a cash payment with a significant amount of foreign currency when there does not appear to be any reason to do so (e.g., both the business and the customer are based in Montserrat without any immediate ties to the countries), enquiries should be made as to why that may be, and if suspicious, you should consider making a suspicious activity report.

Similarly, if any goods you are purchasing appear to be significantly cheaper than the market rate, enquiries should be made as to why that may be, and if suspicious, consider making a suspicious activity report.

18.2 Simplified Due Diligence

A business may apply a simplified form of due diligence in some cases.

Simplified due diligence is where the business relationship or transaction is considered low risk in terms of money laundering or terrorist financing. It can apply to any person assessed as low risk with some exceptions.

The expected starting level of due diligence is customer due diligence. If you decide that simplified due diligence is sufficient you will need to demonstrate why you have deviated from this. The business will have to risk assess the customer to establish that they are low risk, taking into account relevant factors.

This does not mean a business does not have to do customer due diligence, and it is still required to identify and verify customers' identity and take reasonable measures to verify the beneficial owners' identity. Under simplified due diligence however, the business can change when it is done, how much is done, or the type of measures taken to identify and verify a person. For example:

- verifying the customer or take reasonable measures to verify the beneficial owner's identity:
  - during the establishment of a business relationship or
  - within a reasonable time,
- if applicable, verify the identity when transactions exceed a reasonably low level, use at least one authoritative identity document to verify identity that:
  - demonstrates the person's name, and (at least) either their address or date of birth;
  - contains security features that prevent tampering, counterfeiting and forgery;
  - has been issued by a recognised body that has robust identity proofing measures e.g., passport.
- use information already obtained to determine the nature or purpose of a business relationship without requiring further information, for example, if the customer is a pension scheme you can assume what the purpose of that scheme is;
- adjust the frequency of transaction monitoring such as checks triggered when a reasonable threshold is reached;
- adjust the frequency of customer due diligence reviews, for example, to when a change occurs.

If verification is not immediate your system must be able to pick up on these cases so that verification of identity takes place.

To apply simplified due diligence, you need to ensure that all of the following apply:

- it is supported by your customer risk assessment;
- you take into account relevant information made available;
- enhanced due diligence does not apply;
- monitor the business relationship or transactions to ensure that there is nothing unusual or suspicious from the outset;
- the customer is not established in or operates from a high risk third country identified by the FATF, HM Treasury or FIU;
- the customer is not a politically exposed person, or a family member or known close associate of a politically exposed person;
- the customer is seen face to face;
- the source of funds or wealth are transparent and understood by your business;
- where the customer is not an individual, that there is no beneficial ownership beyond a single legal entity customer;
- where the customer is not an individual, that the legal entity is not registered or administered outside of Montserrat.

To decide whether a customer is suitable for simplified due diligence other factors such as the type of customer, the underlying product or service and the geographical factors, should be considered. One factor, on its own, should not be taken to indicate low risk.

A business must record evidence, as part of its risk assessment, that a customer or service provided is eligible for simplified due diligence. Ongoing monitoring should be conducted in line with a business' risk assessment to ensure that the circumstances on which the original assessment was based has not changed.

Where a person says that they are representing a customer who may considered to be low risk the business should verify that they have the authority to act for the customer or are an employee.

It must not be automatically assumed that a customer is low risk to avoid doing an appropriate level of customer due diligence. Persons or businesses well established in the community, persons of professional standing or persons who are well known, may merit being categorised as low risk but there must evidence to base this decision on.

A business or person who has strong links to the community, is well established with a clear history, is credible and open, does not have a complex company structure, where the source of funds are transparent and where there are no other indicators of higher risk may be suitable, subject to the risk assessment, for simplified due diligence.

Simplified due diligence should be discontinued if:

- there is suspicion of money laundering or terrorist financing;
- there is doubt whether documents obtained for identification are genuine;
- there is doubt whether the person is the one demonstrated by the documentation;
- there is suspicion that the documents obtained for identification maybe lost, stolen or otherwise fraudulently acquired, or;
- circumstances change and the risk assessment no longer considers the customer, transactions or location as low risk.

18.3 Enhanced Due Diligence

Enhanced due diligence applies in situations that are high risk. It means taking additional measures to identify and verify the customer identity and source of funds and doing additional ongoing monitoring.

This must be done when:

- it is identified in the business' risk assessment that there is a high risk of money laundering or terrorist financing;
- FIU or other supervisor or law enforcement authority provide information that a particular situation is high risk;
- a customer or any party relevant to the transaction, operates or is established in a high risk third country identified by the FATF, HM Treasury or FIU;
- a person has given you false or stolen documents to identify themselves (immediately consider

reporting this as suspicious activity)

- a customer is a politically exposed person, an immediate family member or a close associate of a politically exposed person
- the transaction is complex or unusually large or with an unusual pattern and has no apparent legal or economic purpose
- a customer is the beneficiary of a life insurance policy or legal arrangement and presents a high risk of money laundering or terrorist financing for any other reason during the course of completing due diligence, the business identifies a customer is a third country national who is applying for residence rights in exchange for transfers of capital, purchase of a property, government bonds or investment in corporate entities.

A business should consider a number of factors in its risk assessment when deciding if enhanced due diligence needs to be applied. The following are some examples of things to take account of.

Customer factors based on information a business has or behaviours indicating higher risk, such as:

- unusual aspects of a business relationship;
- the customer is resident in a high-risk area;
- use of a legal person or arrangement used to hold personal assets;
- a company with nominee shareholders or bearer shares;
- a person or business that has an abundance of cash;
- an unusual or complex company structure given the nature of the type of business;
- searches on a person or associates show, for example, adverse media attention, disqualification as a director or convictions for dishonesty.

How the transaction is paid for or specific requests to do things in a certain way may indicate higher risk, for example:

- the transaction involves private banking;
- the transaction favours anonymity;
- a person is not physically present;
- payment from third parties with no obvious association;
- the transaction involves nominee directors, nominee shareholders or shadow directors or a company formation is in a third country.

When the transaction is related to any of the following, a business must consider whether you should carry out enhanced due diligence:

- oil
- arms and weapons
- precious metals and stones
- tobacco products
- cultural artefacts
- ivory and other items related to protected species

Enhanced due diligence measures must be taken when any business relationship or relevant transaction is established in a high-risk third country.

18.4 Additional Measures to Take

If enhanced due diligence is appropriate, then you must do more to verify identity and scrutinise the background and nature of the transactions, than for standard customer due diligence. How this goes beyond standard due diligence must be made clear in your risk assessment and procedures.

For example:

- obtain additional information or evidence to establish the identity from independent sources, such as more documentation on identity or address or electronic verification alongside manual checks;
- take additional measures to verify the original documents supplied from independent sources, such as more documentation on identity or address or electronic verification alongside manual checks or require that copies of the customer's documentation are certified by a bank, financial institution, lawyer or notary who are competent at document inspection and impostor detection, such as a person from a regulated industry or in a position of trust;
- ensure any information on identity documents is validated by an authoritative source;
- check if the identity is known to be involved with any fraudulent activity or documents; if receiving payment ensure it is made through a bank account in the name of the person you are dealing with;
- take more steps to understand the history, ownership, and financial situation of the parties to

the transaction

- in the case of a politically exposed person establish the source of wealth and source of funds
- carry out more scrutiny of the business relationship and satisfy yourself that it is consistent with the stated purpose.
- measures which must be taken when either party to a business relationship, or relevant transaction is established in a high-risk third country (a business is established in a country if they are incorporated there, is their principal place of business, or they are regulated there as a financial or credit institution; an individual is established in a country if they are resident there):
  - Obtain additional information on the customer and the customer's beneficial owner;
  - Obtain additional information on the intended nature of the business relationship;
  - Obtain information on the source of funds of the customer and of the customer's beneficial owner;
  - Obtain information on the reasons for the transaction;
  - Obtain the approval of senior management for establishing or continuing the business relationship;
  - Enhance monitoring of the business relationship by increasing the number and timing of controls applied, and select patterns of transactions which require further examination;

- The following measures must be taken when the transaction relates to a politically exposed person, a family member or known close associate of a politically exposed person:
  - Obtain senior management approval before establishing a business relationship with that person;
  - Take adequate steps to establish the source of wealth and source of funds that are involved in the proposed business relationship or transaction;
  - Conduct enhanced ongoing monitoring where the business has entered a business relationship.

18.5 Certification

If the original documents are not produced for verification, or cannot be validated with an authoritative source, then you can use a certified document instead.

18.6 Politically Exposed Persons (PEPs)

PEPs are persons that are entrusted with prominent public functions, whether in the Montserrat or abroad. This is because international standards issued by the FATF recognise that a PEP may be in a position to abuse their public office for private gain and a PEP may use the financial system to launder the proceeds of this abuse of office.

The definition does not include:

- middle ranking or more junior officials

In Montserrat, civil servants below Permanent or Deputy Permanent Secretary-level will not normally be treated as having a prominent public function. When assessing whether a person is a PEP, it should be considered whether a person is acting on the instruction of, or on behalf of, a PEP. This is more likely to be the case when the relevant persons hold prominent functions in a third country which presents a relatively higher risk of money laundering.

PEPs include:

- heads of government, ministers and deputy or assistant ministers;
- members of parliament or similar legislative bodies;
- members of the governing bodies of political parties;
- members of supreme courts;
- members of courts of auditors or boards of central banks
- members of the administrative, management or supervisory bodies of state-owned enterprises. This only applies to 'for profit' enterprises where the state has ownership of greater than 50% or where information reasonably available points to the state having control over the activities of such enterprises
- directors, deputy directors and members of the board, or equivalent of an international organisation:
    - includes international public organisations such as the UN
    - does not include international sporting federations.

The Regulations require that family members of PEPs must also have enhanced due diligence measures applied to them. For these purposes, the definition of "family member" includes:

- spouses/civil partners of PEPs
- children of PEPs and their spouses/civil partners
- parents of PEPs

Beyond this definition, firms should take a proportionate and risk-based approach in assessing whether any given individual is a family member of a PEP – it may, for example, be appropriate to treat a wider circle of family members (such as brothers and sisters) as subject to enhanced due diligence measures in cases where a firm has assessed a PEP to present a higher risk.

The Regulations require that close associates of PEPs must also have enhanced due diligence measures applied to them. The definition of "close associate" includes:

- joint legal ownership, with a PEP, of a legal entity or arrangement
- any other close business relationship with a PEP
- sole beneficial ownership of a legal entity or arrangement set up for the benefit of a PEP.

18.6.1 PEP Risk

Enhanced due diligence on PEPs must always be applied to, their family members or known close associates on a risk-sensitive basis. A business must have appropriate risk management systems and procedures in place to determine whether a customer is a PEP or a family member or known close associate of one. The business should take account of:

- its own assessment of the risks faced by its business in relation to PEPs;
- a case-by-case assessment of the risk posed by a relationship with a PEP;

Information is available in the public domain that will help you to identify PEPs. A number of sources can be used, for example:

- ask the customer
- search the internet
- news agencies and sources
- government and parliament websites

If a customer is a PEP, family member or known close associate of one, then you must put in place all of the following enhanced due diligence measures:

- obtain senior management approval before establishing a business relationship with that person;
- take adequate steps to establish the source of wealth and source of funds that are involved in the proposed business relationship or transaction;
- conduct enhanced ongoing monitoring where a business relationship has been entered into.

A business must, however, assess in each case the level of risk that the PEP presents and apply an appropriate level of enhanced due diligence. More frequent and thorough measures should be taken if the PEP is higher risk. Similarly, a reduced level of enhanced due diligence measures can be applied to lower-risk PEPs.

Enhanced due diligence must continue to be applied when the PEP has left the function or position and for a further period of at least 12 months after they cease to hold such a function. Any extension over 12 months will normally only apply to a PEP you have assessed as higher risk. A business should typically cease applying enhanced due diligence measures to such persons 12 months after they cease to hold a prominent public function.

The obligation to apply enhanced due diligence on family members and known close associates, stops as soon as the PEP no longer holds the office unless there are other reasons for treating them as higher risk.

The level of risk of a PEP may vary depending on where they are from and the public accountability they are subject to.

18.7 Identifying Individuals

If the customer is an individual, they must be identified as part of a business' customer due diligence. The customer's private individual's given and family names (s), date of birth and residential address as a minimum.

Documentation purporting to offer evidence of identity may come from a number of sources. These documents differ in their integrity, reliability and independence. Some are issued after due diligence on an individual's identity has been undertaken; others are issued on request, without any such checks being carried out. There is a broad hierarchy of documents:

- certain documents issued by government departments and agencies, or by a court; then
- certain documents issued by other public sector bodies or local authorities; then
- certain documents issued by regulated firms in the financial services sector; then
- those issued by other firms subject to the Regulations, or to equivalent legislation; then
- those issued by other organisations.

A business should verify these using identity evidence that have been issued by a recognised body, for example World-Check, that has robust identity proofing measures, and includes security features that prevent tampering, counterfeiting and forgery with the customer's full name and photo, with a customer's date of birth or residential address such as:

- a valid passport;
- a valid photo card driving licence (full or provisional);
- a national identity card.

When verifying the identity of a customer using documents you must take a copy and keep it on file, however it may be appropriate to also record the details of what identity evidence was presented and the information that was on the document, as well as how this evidence was checked and the outcome of the verification process.

Where the customer does not have one of these documents, the following should be requested:

- a valid and genuine identity document from an authoritative source (without a photo) which includes the customer's full name and also secondary evidence of the customer's address, for example an old-style driving licence or Government issued ID/national ID;
- secondary evidence of the customer's address, that can be verified as true by an authoritative source, for example a utility bill, bank, building society or credit union statement or a most recent mortgage statement.

If the customer's identity are verified by documents, the original documents should be seen, Photocopies should not be accepted, unless certified.

Where an agent, representative or any other person acts on behalf of the customer you must ensure that they are authorised to do so, identify them and verify the identity using documents from a reliable and independent source.

18.7.1 Persons Without Standard Documents

Some persons such as elderly persons or those that cannot manage their own affairs may not be able to produce current standard documents because they have not driven or travelled for some time and have allowed licenses and passports to lapse.

Before accepting non-standard documents, the traditional forms of identification must be exhausted first.

If non-standard documentation is used to confirm the client's identity, measures should be taken to establish whether the documentation is genuine - for example, the use of document references or organisation stamps.

18.7.2 Electronic Verification

Simply carrying out electronic records checks on limited information, such as the name and address of a person who has not been seen, does not mean that the business has verified that the person it is dealing with is who they say they are. A business must ensure that the checks its uses shows that it has identified the customer, verified the identity and that they are, in fact, the same person that is using the services (to protect against impersonation). A business should therefore verify key confidential facts that only the customer may know to establish who they say they are. For example, testing the person using robust information that is not known to be, or likely to be, in the public domain. Manual identity documents can be checked alongside electronic verification where greater risk is indicated. An electronic records check is not always appropriate.

In order to verify an individual's identity electronically, a business must:

- Use a package which addresses the risks detailed in the business' risk assessment and understand how it addresses those risks
- Use multiple positive information sources, such as addresses or bill payment details
- Use negative sources, such as databases identifying identify fraud and deceased persons
- Use data from multiple sources collected over a period of time
- Incorporate checks that assess the strength of the information supplied.

- Ensure that the system is set to fail/refer a customer at a level appropriate to the risk posed by the customer you are carrying out customer due diligence on.
- Retain, or have access to, sufficient records in order to comply with your record keeping requirements, which must take into account events such as an external provider going out of business.