The Turks and Caicos Islands Financial Services Commission

Handbook for the Prevention and Detection of Money Laundering and the Financing of Terrorism for High Value Dealers

Issued February 2014

Sector Specific Guidance High Value Dealers

Contents

1 Introduction

Criminals have responded to the anti-money laundering and prevention of financing measures introduced over the past decade 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 organisations, notably the Financial Action Task Force (FATF) and the Caribbean FATF (CFATF) styled body have 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 DNFBP). 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. Good 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 the Turks and Caicos Islands 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 the Turks and Caicos Islands 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 the Turks and Caicos Islands professional and financial services industry as a whole, and may risk prosecution for criminal offences.

Cash is the mainstay of much organised 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 prevention of terrorist financing (PTF) measures
- Explains the requirements of the Turks and Caicos Islands Money Laundering Regulations 2010 and the Turks and Caicos Islands AML Code 2011 and how these should be used in practice.
- Provides specific good practice guidance on AML/PTF 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/PTF and AML/CTF. The Regulations refer to Anti Money Laundering and Prevention of Terrorist Financing and other bodies tend to use AML/CTF - Anti Money Laundering and Countering (or Combating) 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 Ordinance, ("The POCO") The Anti-Money Laundering and Prevention of Terrorism Regulations 2010 ("The Regulations") and the Anti-Money Laundering and Prevention of Terrorist Financing Code 2010. ("The 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/PTF requirements. It is provided as general information only. It is not legal advice, and is not intended to replace The POCO or to replace 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 procedures manual.

4 The Turks and Caicos Islands 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 23 of the Regulations, The Commission has been appointed the sole supervisory authority of all DNFBP, for the purposes of Section 148F (2) of the POCO

As the Supervisor, the Commission is required to:

- Establish and maintain a Register of all DNFBPs. 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 greater than US$50,000 or in the case of dealers in precious stones US$15,000.[1]

Types of High Value Dealers include (but not exclusively) jewellers, car, boat and art dealers.

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

In any currency

The thresholds[2] quoted above 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 the Turks and Caicos Islands. 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.[3]

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 customer where there is a suspicion of money laundering.

[1] The Regulations Part 1 (2) (1)
[2] $50,000 and $15,000: See definition – Section 5.1
[3] See Section 11 of this document.

- Inform staff of their obligations and responsibilities and those of the business, and train staff in 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 the Turks and Caicos Islands 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 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[4] 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.

6.1 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

[4] Also referred to as a Predicate Crime

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.

6.1.1 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 a number of other persons to deposit cash in amounts below any reporting thresholds.

6.1.2 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 and to make the paper trail very difficult to follow.
The buying and then selling of a high value asset is a good example of the layering stage of money laundering.

6.1.3 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, such as the acquisition of high value goods.
Successful money laundering allows criminals to use and enjoy the income from the criminal activity without suspicion.

The FATF, has found that globally, High Value Dealers are susceptible to being used not only in the layering and integration stages of money laundering, as has been the case historically, but also as a means to disguise the origin of funds before placing them into the financial system.

7 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.

8 Turks and Caicos Islands Legislation

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

8.1 Legislation, Regulations and The Code

The Proceeds of Crime Ordinance was amended in 2009, 2010, 2011, and 2013.

- Proceeds of Crime Ordinance Chapter 3.15 (as amended) (The Principal Ordinance)
- The Anti-Money Laundering and Prevention of Terrorist Financing Regulations 2010
- The Anti-Money Laundering and Prevention of Terrorist Financing Code 2011

8.2 Money Laundering Offences

Money Laundering is dealt with in Part IV Sections 108 – 125 of the Proceeds of Crime Ordinance (POCO)

Establishment Operations and Functions of the Money Laundering Reporting Authority.	**Sections 108 – 114**
Criminal Property	Section 115 – 116
Offences of Concealing, Disguising, Converting, Transferring and removing Criminal Property	Section 117
Offence of Arrangements	Section 118
Offences of Acquisition and Possession of Criminal Property	Section 119
Duty to Disclose Knowledge or Suspicion of Money Laundering	Sections 120 – 122
Offence of Prejudicing Investigations and Tipping Off	Section 123 – 124
Protection of Disclosures	Section 125

8.2.1 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.

9 Registration with the Financial Services Commission

The Turks and Caicos Islands 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[5].

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

9.1 Registration Procedure

Applicants for registration must complete and submit a paper copy of the Application to Register.

The application form is available on the Financial Services Commission website. The form may be prepared electronically and printed.

Applicants are strongly advised to refer to the Guidance Notes to Registration available on the website.

An advance copy of the Application to Register may be submitted by email to the address dnfbp@tcifsc.tc

- A signed paper printed copy of the Application to Register together with supporting documents must be delivered by hand to either the Providenciales or Grand Turk offices of the Commission.

9.1.1 Supporting Documents

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

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 must be certified by one of; a Notary Public, Justice of the Peace, or Commissioner of Oaths, as a true copy of the original.

9.1.2 Receipt of Registration Application by the Commission

[5] The Regulations Schedule 2

The Commission undertakes to acknowledge receipt within two 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.

9.1.3 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 25.

b) The applicant fails to provide any information or documents required by the Supervisor under Regulation 25 (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.

9.1.4 Registration refused: Right to Appeal

In the event that an Application to Register is refused, the applicant may submit an appeal addressed to the Managing Director of the Commission, and submitted by email to;

dnfbp@tcifsc.tc

9.1.5 Forms

The following forms are must be used and can be accessed by following the link in the FSC website.

9.1.6 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 three 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 within 30 days 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.

9.1.7 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.[6]

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.

10 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

[6] POCO Sections 148H (1) and (2)

Criminals tend to use as 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 of 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 the 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 life style (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.).

10.1.1 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.

10.1.2 Precious stones and jewellery

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

10.1.3 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.

11 Anti-Money Laundering Systems and Controls

11.1 Compliance programme

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.

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 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.

11.2 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.

11.3 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.
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.

11.4 Policies, systems and controls[7]

11.4.1 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 and
    - Identifying and verifying the identity of the applicant of the business.
- Report to the Turks and Caicos Islands 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.

11.4.2 Internal Controls

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

11.4.2.1 Customer Due Diligence

- Have in place a proforma to gather core due diligence information which must be used in all high value transactions.

[7] The Code Part 2

- 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.

11.4.2.2 Handling Transactions

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

11.4.2.3 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 if staff to deal with high value cash transactions.
- Liaise closely with the Commission and the FIU on matters concerning vigilance, systems and controls.

11.4.3 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.

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.

12 Risk Based Approach[8]

12.1 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.
- While establishing 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.

12.2 Key Concepts

[8] Reference the guidance provided in Part 2 of the Code.

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

The notes in this section can be applied at both the portfolio and customer level.

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.

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

12.2.1 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.

12.2.2 Vulnerabilities

In risk assessment vulnerability comprise 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 focussing 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.

12.2.3 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 to the individuals concerned, and reputational damage to the business or forfeiture of laundered assets.

Assessing consequence may be challenging, given the lack of clear data and experiences. It is not always necessary to assess consequence in a sophisticated manner, but a high level understanding of the impacts 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.

12.2.4 Sources of risk

Sources may be organised into three groupings described below.

12.2.4.1 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). 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[9] 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.

12.2.4.2 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 customer's may indicate higher risk.

- 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 affect the risk.

- Occasional or one-off transactions as opposed to business relationships.

[9] Credible sources refer to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publically and widely available. In addition to the FATF and FATF styled regional bodies such sources may include but are not limited to, supra-national; or international bodies such as the International Monetary Fund, the World Bank, and the Egmont Group of Financial Intelligence units, as well as relevant national government bodies and non-governmental organisations. The information provided by these credible sources does not have the effect of law or regulation and should not be viewed as an automatic determination that something is of higher risk.

- 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[10] (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.

12.3 Money Laundering Compliance Officer and Money Laundering Reporting Officer.[11]

[10] See specific section of the Handbook – Politically Exposed Persons
[11] Section 8 of the Code.

12.3.1 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.

The MLRO is required to:

- Assess internal suspicious activity reports and submit suspicious activity reports when required to the Turks and Caicos Islands Financial Intelligence Unit.

12.3.2 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 Commission issued guidance notes in May 2013 with regard to the appointment of the Money Laundering Reporting Officer and Money Laundering Compliance Officer. However at this early stage of Supervision by the Commission the strict criterion for acceptance as MLRO and MLCO is not followed at the present time in its entirety.

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.

12.3.2.1 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/PTF risk assessed.

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

- Sufficient resources including sufficient time.
- A sufficient level of authority within the business.
- Regular contact with the Board or senior management.
- Sufficient knowledge and experience in AML and PTF matters
- Local residency and be employed by the business[12].

12.4 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.

[12] See Section 12.4 Outsourcing

13 Customer Due Diligence (CDD)[13]

13.1 Introduction

High Value Dealers which accept cash payments of greater than US$50,000 or in the case of dealers in precious stones US$15,000, must apply Customer Due Diligence prior to entering into the transaction or relationship.[14]

Part III 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: This is the obtaining of reputable documentation[15] 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 recognisable government prepared document e.g Passport.
If a prospective cannot satisfactorily satisfy usual due diligence measures for example unable to identify and verify a customer's identity or obtain sufficient information about the nature and

[13] Part III of the Code
[14] The Regulations Part 1 (2) (1)
[15] Part III of The Code provides extensive information on acceptable documentation.

purpose of a transaction, then the transaction must not be carried out the business relationship must not be established.

Businesses must also consider submitting a Suspicious Activity Report to the Financial Intelligence Unit.

13.2 When due diligence measures must be applied.

Customer due diligence must be applied when

- When establishing a business relationship[16]
- When carrying out an occasional transactions
- 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 during the establishment of the business relationship, provided it is done as soon as is practicable after contact is first established.

13.3 Why is it 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

[16] It is recognised that a typical relationship with a High Value customer may be a single transaction. Relationships may extend into multiple transactions over a period of time.

cannot be accepted until identity has been verified and the nature and purpose of the transaction has been checked.

13.3.1 Identifying the customer

Most customers can be expected to present a passport or drivers licence to verify identity. A customer may present a drivers 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[17].

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.

13.3.2 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.

13.3.3 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.

[17] Refer to The Code Part III Customer Due Diligence

13.4 Ascertaining funds and wealth are from a legitimate source.

13.5 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.

13.6 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.

13.6.1 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.

13.7 Occasional transactions

Part 1 Section 4 of the Regulations requires that customer due diligence measures must be applied when a business carries out occasional transactions. Section 4 (1) defines an occasional transaction.

13.8 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. (See Section 15)

13.9 Risk Approach to Customer Due Diligence

Regulation 13 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 lever risk assessment, customer on boarding should include a risk assessment of each customer. Businesses are expected to assess the inherent AML and PTF risk associated with each individual new customer and also re-assess that risk periodically.

13.9.1 Customer Profile

It is necessary to prepare a profile on 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.

13.10 Other Customer Due Diligence Matters

13.10.1Is 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[18].

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.

13.10.2High Risk Customer/ Transactions[19]

There are 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)

[18] The Code Sections 16, 17 and the supporting guidance
[19] Section 13 of the Code

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.

13.11 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.

14 Monitoring Customer Activity[20]

14.1 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.

[20] Part 4 Section 28 of the AML Code

- 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.

14.2 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 rather 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 be either:

- 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.

14.3 Recognising Suspicious Behaviour and unusual instructions.

14.3.1 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?

14.3.2 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 businesses' 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.

14.3.3 Buying in second hand goods

High value dealers who buy-in high value second hand items for trading on 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.

14.3.4 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 $15,000/$50,000 (as appropriate) by credit card cheque and then at the last minute present cash as a means of payment.
- There appear 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

15 Reporting Suspicious Activity and Transactions[21]

15.1 Legislation

Section 120 (1) of The POCO calls for:

Where a person

[21] Part 5 of the AML Code

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 Reporting Authority.

In the Turks and Caicos Islands the reporting authority is the Turks and Caicos Islands Financial Intelligence Unit. (FIU).

15.2 What constitutes knowledge or suspicion

15.2.1 Knowledge

Knowledge means actual knowledge.

15.2.2 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 those particular funds were definitely those arising from the 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.

15.2.3 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 that profession would 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.

15.3 Failure to report

Failing 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.

15.4 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.

15.4.1 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 when a disclosure while waiting for consent and
- 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.

15.5 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.

15.6 Reports to Reporting Authority (FIU)

The MLRO will submit suspicious activity reports to the FIU in writing on the Suspicious Activity Report form electronically via email or they may be delivered by hand. A copy of the SAR form is available via the FIU link on the following website: www.tcipolice.tc or they can be provided by contacting the FIU directly at 649-941-7690 or fcutcipd@tciway.tc

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.

15.7 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 Suspicious Activity Report 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.

15.7.1 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's 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.

15.8 Consent to Activity[22]

15.8.1 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.

15.9 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.

16 Employee Training and Awareness[23]

[22] Section 116 of POCO
[23] The Code Part 6 Section 33

16.1 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.

16.2 Obligations

Businesses must provide their staff with appropriate and proportional training AML/CFT training.[24] 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.

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

[24] Part VI of the Code

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.

16.3 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.

16.4 Scope of Training

Businesses must ensure that relevant employees are made aware of their responsibilities under The POCO, The Regulations and The Code, to report knowledge or suspicion 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
- 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.

16.5 Frequency of training

Businesses should ensure that the frequency of training is sufficient to maintain the knowledge and competence of staff to apply customer due diligence measures appropriately and in accordance with the business's 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 go to www.fatf-gafi.org

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

17 Record Keeping[25]

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

Businesses should ensure that they keep records as specified on Regulation 18

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 or such longer period as the FSC. The records must be kept for 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 with the record keeping requirements of the AML/PTF Regulations and the Code.

[25] The Code Part 7 Sections 34 to 40

18 Appendix A Red Flag Indicators

18.1 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 the 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 checks, 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.

18.2 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.

18.3 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.

18.4 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.