GUIDANCE NOTES ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING AND TERRORIST FINANCING IN THE CAYMAN ISLANDS

Issued by the Cayman Islands Monetary Authority
Pursuant to section 34 of the Monetary Authority Law (2016 Revision)

December 13th 2017

These Guidance Notes replace the (previous) Guidance Notes issued in August 2015 (the "August 2015 GNs").

This document is intended to provide general guidance to Financial Service Providers ("FSPs"). It should therefore, not be relied upon as a source of law. Reference for that purpose should be made to the appropriate statutory provisions. However, FSPs should be aware of the enforcement powers of the Supervisory Authorities under the Anti-Money Laundering Regulations (2017 Revision) ("AMLRs") as they relate to supervisory or regulatory guidance.

Contact:
Cayman Islands Monetary Authority
Elizabethan Square
P.O. Box 10052
Grand Cayman KY1-1001
Cayman Islands

Tel:345-949-7089 Fax: 345-945-6131
Website:www.cimoney.com.ky Email: CIMA@cimoney.com.ky

FOREWORD

The Cayman Islands, being one of the leading international financial centres, has framed its regulatory system around international standards of supervision and co-operation with overseas regulatory authorities in the fight against financial crime. The Islands seek to maintain their position as a premier jurisdiction, while at the same time ensuring that their institutions can operate in a competitive manner.

The Cayman Islands Monetary Authority ("Monetary Authority") is particularly aware of the global nature of the fight against money laundering, terrorist financing and other financial crime, and the consequent need for all jurisdictions to operate their Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") and regulatory regimes co-operatively and compatibly with each other. This is both to limit opportunities for "regulatory arbitrage" by criminals and to promote an internationally level playing field for legitimate businesses.

These Guidance Notes provide guidelines that should be adopted by FSPs in order to maintain the integrity of the Cayman Islands' financial sector in respect of preventing and combating money laundering ("ML") and terrorist financing ("TF").

These Guidance Notes are based on the AML/CFT legislation of the Cayman Islands and reflect, so far as applicable, the 40 Recommendations and guidance papers issued by the Financial Action Task Force ("FATF").

The Monetary Authority stands ready to discuss individual cases with FSPs to assist in the practical implementation of these Guidance Notes. We hope that you find the enclosed guidance of assistance.

Cindy Scotland
Managing Director

CONTENTS

GUIDANCE NOTES ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING AND TERRORIST FINANCING IN THE CAYMAN ISLANDS

PART I

AML/CFT FRAMEWORK OF THE CAYMAN ISLANDS

Section 1

SCOPE AND GENERAL MATTERS

A. INTRODUCTION

1. Money Laundering is a global phenomenon that affects all countries to varying degrees. By its very nature it is a hidden activity, and therefore the scale of the problem, and the amount of criminal money being generated and laundered either locally or globally each year is impossible to measure accurately. Failure to prevent the laundering of the proceeds of crime allows criminals to benefit from their actions, making crime a more attractive proposition.

2. Having an effective AML / CFT regime has become a major priority for all jurisdictions from which financial activities are carried out. Being used for Money Laundering ("ML"), Terrorist Financing ("TF") and Proliferation Financing ("PF") exposes FSPs to significant operational, regulatory, legal and reputational risks. The adoption and effective implementation of appropriate control processes and procedures by FSPs is not only a principle of good business but is also an essential tool to avoid involvement in ML, TF and PF.

3. It is important that the management of FSPs view prevention of ML, TF and PF as part of their risk management strategies and not simply as a stand-alone requirement that is being imposed by the legislation. ML, TF and PF prevention should not be viewed in isolation from an institution's other business systems and needs.

4. The AMLRs require relevant financial businesses to establish systems to detect ML/TF, and therefore assist in the prevention of abuse of their financial products and services. This is in FSPs' own commercial interest, and it also protects the reputation of the Cayman Islands.

B. PURPOSE AND SCOPE

1. These Guidance Notes are applicable to all persons conducting relevant financial business as defined under the Proceeds of Crime Law (2017 Revision) ("PoCL" or the Law"). For the purpose of this document, the term FSPs refers to all the persons carrying on relevant financial business specified in the Law.

2. These Guidance Notes are designed to assist FSPs in complying with the AMLRs. They are intended to supplement the AMLRs and the Law by clarifying and explaining the general requirements of the AMLRs. It is expected therefore, that all FSPs will pay due regard to the Guidance Notes in developing an effective AML/CFT framework suitable to their business. If an FSP appears not to be doing so, the relevant Supervisory Authority will seek an explanation and may conclude that the FSP is carrying on business in a manner that may give rise to enforcement actions under the applicable legislation.

3. It is recognised that FSPs may have systems and procedures in place which, whilst not identical to those outlined in these Guidance Notes, nevertheless impose controls and procedures which are at least equal to, if not higher than, those contained in these Guidance Notes. This will be taken into account by the relevant Supervisory Authority in the assessment of an FSP's systems and controls and compliance with the AMLRs.

4. According to the AMLRs, in determining whether a person conducting relevant financial business has complied with the applicable regulations, the Court considers the guidance issued or adopted by the Supervisory Authorities.

5. FSPs shall be cognizant of the fact that the term 'Money Laundering' under the AMLRs includes terrorist financing. Unless otherwise specified, guidance provided in relation to AML in this document is applicable to CFT. FSPs shall apply these Guidance Notes to new business relationships, existing customers and one-off transactions.

6. Throughout these Guidance Notes there is reference to an 'account' or 'accounts' and procedures to be adopted in relation to them. This is a matter of convenience and has been done for illustrative purposes. It is recognised that these references may not always be appropriate to all types of FSPs covered by the AMLRs. Where there are provisions in these Guidance Notes relating to an account or accounts, these will have relevance to mainstream banking activity but should, by analogy, be adapted appropriately to the situations covered by other relevant business. For example, 'account' could refer to bank accounts, insurance policies, mutual funds or other investment product, trusts or a business relationship etc.

7. This document provides references to external websites (i.e., websites other than the CIMA website) for convenience and informational purposes only. Referenced external websites are not under the control of the Monetary Authority and thus the Monetary Authority is not responsible for the contents of any external website or any link contained in, or any changes or updates to such external websites. The Monetary Authority is not responsible for any transmission received from a referenced external website. The inclusion of a reference site does not imply endorsement by the Monetary Authority of the external website, its content, advertisers or sponsors. External websites may contain information that is copyrighted with restrictions on use/reuse. Permission to use copyrighted materials must be obtained from the original source and cannot be obtained from the Monetary Authority.

C. PART II AND PARTS III TO VIII OF THESE GUIDANCE NOTES

1. This part of these Guidance Notes provides information on the AML/CFT framework of the Cayman Islands. General guidance in relation to the requirements under the AMLRs is provided under Part II of these Guidance Notes. In addition to the general guidance provided under Part II, some sector specific guidance is provided under Part III to Part VIII of these Guidance Notes. As such, FSPs should consider all parts of these Guidance Notes, as appropriate.

D. WHAT IS MONEY LAUNDERING?

1. ML is the process by which the direct or indirect benefit of crime is channelled through the economy/financial system to conceal the true origin and ownership of the proceeds of criminal activities. Generally, to launder criminal proceeds, a money launderer places the funds/proceeds in the financial system without arousing any suspicion, moves it in a series of complex transactions to disguise its original (criminal) source and finally, if successful, integrates it into the economy to make the funds appear to be derived legitimately.

2. For the purpose of these Guidance Notes, FSPs shall refer to the meaning of the term "Money Laundering" provided in the AMLRs.

E. THE NEED TO COMBAT MONEY LAUNDERING

1. In recent years there has been a growing recognition that it is essential in the fight against crime that criminals be prevented, wherever possible, from legitimising the proceeds of their criminal activities by converting funds from "dirty" to "clean".

2. The laundering of the proceeds of criminal activity through the financial system is vital to the success of criminal operations. Those involved must exploit the facilities of the world's financial system if they are to benefit from the proceeds of their activities. The increased integration of the world's financial systems, and the removal of barriers to the free movement of capital, has meant that it is potentially easier for criminals to launder dirty money, and more complicated for the relevant authorities to trace. The long-term success of any of the world's financial sectors depends on attracting and retaining legitimately earned funds. The unchecked use of the financial system for laundering money has the potential to undermine FSPs, and ultimately the entire financial sector.

3. Because of the international nature and both market and geographical spread of business conducted in or from the Cayman Islands, local institutions which are less than vigilant may be vulnerable to abuse by money launderers, particularly in the 'layering' and 'integration' stages (see below). FSPs which, albeit unwittingly, become involved in ML/TF risk the imposition of administrative fines, enforcement actions, prosecution and substantial costs both in management time and money, as well as face the severe consequences of loss of reputation.

F. THE STAGES OF MONEY LAUNDERING

1. There is no single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g. a car, or jewellery), to passing of money through a complex international web of legitimate businesses or 'shell' companies. Initially, however, in the case of drug trafficking and some other serious crimes such as armed robbery, the proceeds usually take the form of cash which needs to enter the financial system by some means. Street purchases of drugs are almost always made with cash.

2. Despite the variety of methods employed, the laundering process is accomplished in three stages. These may include numerous transactions by the launderers that could alert an FSP to criminal activity:

   (1) Placement - the physical placement of proceeds derived from criminal activity into the financial system.

   (2) Layering - separating the illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.

   (3) Integration - the provision of apparent legitimacy to wealth derived from crime. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

3. The three basic steps may or may not occur as separate and distinct phases. They may occur simultaneously or, more commonly, they may overlap. How the basic steps are used depends on the available laundering mechanisms and the requirements of the criminal organisations. Some typical examples of these three stages are listed below.

Table - Stages of Money Laundering

Placement Stage	Layering Stage	Integration Stage
Cash paid into an FSP (Sometimes with staff complicity or mixed with proceeds of legitimate business)	Wiring transfer abroad (often using shell companies or funds disguised as proceeds of legitimate business)	False loan repayments and forged invoices used as cover for laundered money
Cash exported	Cash deposited in overseas banking system	Complex web of transactions (both domestic and/or international) makes tracing source of funds virtually impossible
Cash used to buy high value items	Resale of goods or assets	Income from property or legitimate business assets appears 'clean'

4. Certain points of vulnerability have been identified in the laundering process which the money launderer finds difficult to avoid, and where his/her activities are therefore more susceptible to being recognised, such as:

   (1) entry of cash into the financial system;
   (2) cross-border flows of cash;
   (3) acquisition of financial assets;
   (4) transfers within and from the financial system;
   (5) incorporation of companies; and
   (6) establishment of financial vehicles (e.g. ostensible pooled investment funds, merchant and barter companies).

G. WHAT IS TERRORIST FINANCING?

1. Terrorism is an unlawful action which is intended to compel a government or an international organisation, or intimidate the public to do or abstain from doing any act for the purpose of advancing a political, religious, racial, or ideological cause. These actions include serious violence against a person, endangering a person's life, serious damage to property, creating serious risk to public health and safety, or serious interference with or disruption to the provision of emergency services, or essential infrastructure, or to an electronic or computer system. By contrast, financial gain is the main objective of other types of financial crimes. Nonetheless, terrorist groups, like criminal organisations, must develop sources of funding, a means of laundering those funds, and a way of using those funds to obtain materials and logistical items to commit terrorist acts.

2. For the purpose of these Guidance Notes, FSPs shall refer to the meaning of terms 'terrorism' and 'terrorist financing' in the Terrorism Law (2017 Revision) ("TL").

3. Sources of funding for terrorism could be unlawful sources such as kidnapping, extortion, smuggling, various types of fraud (e.g. through credit cards or charities), theft and robbery, and narcotics trafficking. FSPs must be aware however, that funding for terrorist groups, unlike for criminal organisations, may also include funds derived from legitimate sources or from a combination of lawful and unlawful sources. This funding from legal and legitimate sources is a key difference between terrorist groups and traditional criminal organisations.

4. Terrorist groups find ways of laundering the funds in order to disguise links between them and their funding sources, and to be able to use the funds without drawing the attention of authorities. Some of the particular methods detected with respect to various terrorist groups include cash smuggling (both by couriers or bulk cash shipments), structured deposits to or withdrawals from bank accounts, purchases of various types of monetary instruments (travellers' cheques, bank cheques, and money orders/money transfers), use of credit or debit cards, and wire transfers.

5. Charities or other non-profit organizations ("NPOs") are also vulnerable and could be misused for TF. Terrorist groups use NPOs to raise and launder funds for terrorism.

6. There have also been indications that some forms of underground banking (particularly the hawala system[1]) have had a role in moving terrorist related funds. While underground banking may not play a major role in the domestic economy, FSPs should be aware of their existence and develop procedures for identifying transactions that may be linked to such systems.

7. The TL applies to actions, persons, or property, both inside and outside of the Cayman Islands. Any person who believes or suspects that another person has committed an offence under this law must disclose the information to the Financial Reporting Authority ("FRA") or to the police as soon as is reasonably practical. Failure to do so is an offence and is punishable- (a) on summary conviction, to imprisonment for two years and a fine of four thousand dollars; or (b) on conviction on indictment, by imprisonment for five years, and to a fine. The Court may also make a forfeiture order.

8. FSPs should take note of their obligations under different international targeted financial sanctions/orders, and designations and directions issued in relation to TF/PF as applicable and comply. United Nations and European Union sanctions are implemented in the Cayman Islands by way of Overseas Orders in Council. FSPs must take actions such as filing suspicious activity reports, freezing funds, and informing the Governor as required under the relevant laws/orders if they discover a relationship that contravenes any applicable sanctions orders or directions. For the list of applicable sanctions orders, see section on "Sanctions Compliance" in Part II of these Guidance Notes.

H. WHAT IS PROLIFERATION FINANCING?

1. PF refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical, radiological or biological weapons and their means of delivery and related materials (including both technologies and dual use of goods used for illegitimate purposes), in contravention of national laws or, where applicable, international obligations.

2. For the purpose of these Guidance Notes, FSPs shall refer to the meaning of term "Proliferation" in the Proliferation Financing (Prohibition) (Amendment) Law, 2016, ("PFPL").

3. The TL deals with matters relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. The TL makes it an offence to provide, receive or invite instruction or training in the making or use of-(a) firearms; (b) explosives; or (c) chemical, biological or nuclear weapons.

[1] Hawala is an alternative unregulated remittance system which could be used by criminals to launder money. A hawala banker, who usually is a trader, accepts money from persons for certain fees to remit the amount to another person (recipient) usually in a different jurisdiction through another hawala banker in that jurisdiction. The two hawala dealers will settle the accounts as a trade transaction. The hawala system is useful for immigrants or persons without bank accounts to transfer their money to their families. Due to the lack of supervisory oversight,, hawala became more attractive to money launderers.

4. The PFPL requires persons that have in their possession, custody or control in the Islands, any funds or resources or is otherwise dealing with all funds or economic resources of designated persons to immediately freeze all such funds or economic resources of the designated persons[2] and entities without prior notice. The PFPL further requires persons to disclose details of freezing funds or economic resources or any actions taken to the FRA.

5. Where there is a risk of proliferation activities the FRA may issue directions under the PFPL to person(s) in the financial sector and impose requirements such as conducting enhanced customer due diligence; monitoring designated persons; or restricting FSPs from entering or continuing the business relationship with designated persons. The PFPL imposes both civil and criminal sanctions for failure to comply with the aforementioned obligations.

6. For applicable international targeted financial sanctions in relation to terrorism and, proliferation, FSPs shall refer to the websites of the Supervisory Authorities, FRA and Gazettes published by the Cayman Islands Government.

I. AREAS OF CONCERN

1. No financial sector is immune to abuse, and all FSPs should consider the ML, TF and PF risks posed by the products and services that they offer, and establish appropriate systems to mitigate and manage those risks.

2. The high risk category relates to those products or services where unlimited third party funds can be freely received, or where funds can be regularly paid to, or received from third parties without evidence of identity of the third parties being taken. Examples of products in the high risk category are- (a)products offering money transfer facilities through chequebooks, telegraphic transfers; (b)deposits from third parties; (c)cash withdrawals by means of credit and debit cards or any other means.

3. Some of the low risk products are those in which funds can only be received from a named investor by means of a payment from an account held in the name of the investor, and where the funds can only be returned to the same account of the named investor. No third party funding or payments are possible. However, despite their apparent low risk, they are not immune from ML/TF. For instance, other risk factors such as the geographical location of an FSP's customer base will also affect the ML risk and TF analysis. As such, FSPs shall consider all the relevant risks and take a risk based approach in conducting business with their customers. Further guidance on risks and risk factors is provided in Part II of this document and the Sector Specific Guidance.

4. While conducting the risk assessments, FSPs shall also take into account the ML/TF threats/risks identified in the National Risk Assessment ("NRA"). The Cayman Islands

[2] Designated person" means a person, including any subsidiary or other entity owned or controlled by that person, to whom Security Council of the United Nations anti-proliferation financing measures relates.

Government conducted a NRA in 2014/2015 and published the results which can be found at

http://www.gov.ky/portal/page/portal/cighome/help/features/Summary%20Results%20of%20the%20CINRA%20relating%20to%20MLTFPF.pdf

J. NEED FOR VIGILANCE

1. All FSPs should be constantly vigilant in deterring criminals from engaging in any form of ML or TF. Although the task of detecting crime falls to law enforcement agencies, FSPs will be called upon to assist law enforcement agencies in the avoidance and detection of ML, TF and PF activities and to react in accordance with the law in the reporting of knowledge or suspicion of such.

2. Due to the diversity of FSPs, the nature and scope of their vigilance systems will vary according to the size and nature of the institution. However, irrespective of these factors, all institutions must exercise sufficient vigilance to ensure consistency with the procedures as outlined in the AMLRs and these Guidance Notes.

3. FSPs' senior management must be engaged in the decision making processes and take ownership of the risk based approach. Senior management must be aware of the level of ML/TF risk the FSP is exposed to and take a view on whether the FSP is equipped to mitigate that risk effectively. Staff must be adequately trained to enable them to identify suspicious activities and be trained in the internal reporting systems required for compliance with the AMLRs.

4. All FSPs must maintain and periodically review their procedural manuals relating to entry, verification and recording of customer information and reporting procedures. The frequency of review should be based on the size, nature and complexity of the FSP, however, it should be done at least annually or where there are significant changes to the AML/CFT systems and obligations.

5. In dealing with customers the duty of vigilance starts with the commencement of a business relationship or a significant one-off transaction and continues until that relationship ends. However, retention of records upon the cessation of the relationship must be in conformity with the record keeping procedures outlined in the AMLRs and these Guidance Notes.

6. FSPs shall ask their applicants/ customers additional questions in circumstances of unusual or suspicious activity. Any failure by the applicant/customer to provide credible answers will almost always give grounds for further enquiry about his/her activities, make the FSP reconsider the wisdom of doing business with the applicant/customer, and potentially, lead to a suspicious activity report being made.

K. COMPLIANCE CULTURE

1. It is recognised that FSPs exist to make a profit. Nevertheless, each FSP must give due priority to establishing and maintaining an effective compliance culture.

2. The business objectives of customer care are closely aligned to the regulatory objectives of the Know-Your-Customer ("KYC") principle. Similarly, linked are the philosophies behind the regulatory objectives of protecting the reputation of the Cayman Islands and the commercial desirability of protecting the reputation of individual entities.

3. In these respects all FSPs must encourage an open and welcoming approach to compliance and AML/CFT issues amongst staff and management.

4. Where an FSP in the Cayman Islands operates branches or controlled subsidiaries, agencies or representative offices in another jurisdiction, it must have group-wide compliance programmes and comply with the relevant requirements under the AMLRs. Please see guidance on group-wide programmes under section 2 of Part II of these Guidance Notes.

SECTION 2

CAYMAN ISLANDS LEGISLATIVE AND REGULATORY FRAMEWORK

A. INTRODUCTION

1. The Cayman Islands is committed to fighting ML, TF and PF. The Anti-Money Laundering Steering Group ("AMLSG") appointed by the Cabinet is responsible for the general oversight of the AML policy of the Government and promoting effective collaboration between regulators and law enforcement agencies. Key elements of the AML/CFT legislative framework include:

   (1) Anti-Corruption Law (2014 Revision)

   (2) Penal Code (2017 Revision)

   (3) Proceeds of Crime Law (2017 Revision) (the "Law")

   (4) Terrorism Law (2017 Revision)

   (5) Misuse of Drugs Law (2017 Revision)

   (6) Proliferation Financing (Prohibition) (Amendment) Law (2016 Revision)

   (7) Anti-Money Laundering Regulations (2017 Revision)

   (8) International Targeted Financial Sanctions and Orders

B. OUTLINE OF THE OFFENCES

1. The AML/CFT legislation criminalises ML, TF and PF and carries penalties and criminal sanctions for these offences. FSPs shall note that the commission of ML offences may lead to enforcement actions, and/or prosecution. ML offences under different laws are listed below.

2. The ML offences under the Law, in summary:

   (1) Section 133 of the Law creates the offence of concealing or disguising property, which is the proceeds of criminal conduct, or converting or transferring that property or removing it from the jurisdiction. The section applies to a person's own proceeds of criminal conduct or where he/she knows or has reasonable grounds to suspect that the property he/she is dealing with represents the proceeds of another's criminal conduct.

   (2) Under section 134 of the Law, a person commits an offence if he/she enters into or becomes concerned in an arrangement which he/she knows or suspects facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person. This may be by concealment, removal from the jurisdiction, transfer to nominees or otherwise.

(3) The acquisition, possession or use (even temporary) of property knowing that it represents the proceeds of criminal conduct is an offence under section 135 of the Law.

(4) According to section 136 of the POCL, a person commits an offence if the person fails to make a disclosure to the FRA or a nominated officer as soon as reasonably practicable after knowledge or suspicion of ML/TF, where such knowledge or suspicion is based on the information which comes to that person's attention in the course of his/her trade, profession, business or employment. Section 4(2) of Law further states that, notwithstanding any other law to the contrary, the FRA shall receive all disclosures of information concerning ML and TF.

(5) Tipping-off the target or a third party about an investigation or proposed investigation into ML, any matter, which is likely to prejudice such an investigation or a report to the FRA, is an offence per section 139 of the Law.

3. TF offences under the TL, in summary:

(1) Section 19 of the TL makes it an offence to solicit, receive or provide property intending that it be used, or having reasonable cause to suspect that it may be used, for the purposes of terrorism.

(2) According to section 20 of the TL, it is an offence for a person to use property for the purposes of terrorism or to possess property intending that it be used, or having reasonable cause to suspect that it may be used for the purposes of financing of acts of terrorism, terrorists, or terrorist organisations.

(3) Section 21 of the TL makes it an offence for a person to enter into or become concerned with an arrangement as a result of which property is made available to another knowing or having reasonable cause to suspect that it will or may be used for the purposes of terrorism.

(4) Under section 22 of the TL, a person commits a ML offence if he "enters into or become concerned in an arrangement that facilitates the retention or control by or on behalf of another person of terrorist property by concealment, by removal from the jurisdiction or by transfer to nominees".

4. It is not necessary that the original offence from which the proceeds stem was committed in the Cayman Islands if the conduct contravenes the law of the country in which it occurred and would also constitute an offence had it taken place within the Islands. This is known as the concept of dual criminality.

5. No duty is imposed on an FSP to inquire into the criminal law of another country in which the conduct may have occurred. However, FSP should be aware of and understand the laws of those jurisdictions in which they operate. The question is whether the conduct amounts to an indictable offence in the Cayman Islands or would if it took place in the Cayman Islands. An FSP is not expected to know the

exact nature of criminal activity concerned or that the particular funds in question are definitely those which flow from the crime.

C. OUTLINE OF THE DEFENCES

1. There are general defences enabling a defendant to prove, for example, that he/she did not suspect that an arrangement related to the proceeds of criminal conduct or that it facilitated the retention or control of the proceeds by the criminal. There are also specific defences provided by reporting a suspicious transaction. It will not be an offence to act in accordance with an arrangement which would otherwise be a crime if a report is made of the suspicion about the source of the funds or investment. If a disclosure of the arrangement is made before the action in question or volunteered as soon as it reasonably might be after the action, no offence is committed.

2. An employee who makes a report to his employer in accordance with established internal procedures is specifically protected by the Law in sections 134, 135 and 136 as well as sections 23 and 24 of the TL.

3. There is a risk that efforts to detect ML and follow the assets will be impeded by the use of alternative undetected channels for the flow of illegal funds consequent to an automatic cessation of business (because a service provider suspected that funds stemmed from illegal activity). To avoid that risk, FSPs are permitted to report their suspicions to the FRA but continue the business relationship or transaction. In carrying out transactions where an institution is considering making a suspicious activity report, the institution should consider duties owed to third parties such as in the case of a constructive trustee. In such cases, it is recommended that independent legal advice is sought.

4. A report of a suspicious activity made to the FRA does not give rise to any civil liability to the customer or others and does not constitute, under Cayman Islands law, a breach of a duty of confidentiality. There are statutory safeguards governing the use of information received by the FRA.

5. To avoid tipping-off, caution must be adopted in determining what may be disclosed to a customer in the event that a report of suspicious activity is made or information obtained about ML investigations.

D. REGULATORY LAWS, RULES AND GUIDANCE

1. The regulatory laws require, and the Monetary Authority expects that FSPs-
   (1) should conduct the management and direction of the business in a fit and proper manner; and

   (2) should not carry on any aspect of their business in a manner detrimental to the public interest, the interest of its customers, depositors, beneficiaries of any trust, creditors, policy holders or investors.

2. As such, the Authority expects that FSPs-

   (1) will understand and comply with all applicable laws, rules, and regulations of any government, regulatory authority/body, or licensing agency, governing their business activities; and

   (2) will not knowingly participate or assist in, and must disassociate from any violation of such laws, rules, or regulations.

3. FSPs that knowingly participate or assist in the violation of the laws, rules, or regulations of any jurisdiction-

   (1) would be carrying on business in a manner detrimental to the public interest, the interest of its customers, depositors, beneficiaries of any trust, creditors, policy holders or investors;

   (2) would not be conducting the business of the FSP in a manner that is fit or proper;

   (3) may expose the jurisdiction to reputational risks; and

   (4) may also expose the FSP to legal, compliance and AML/CFT risks.

4. These Guidance Notes are also intended to assist FSPs in applying national AML/CFT/APF measures, and in particular, in detecting and reporting suspicious activities[3]. They embody best practices and set out minimum criteria that the Supervisory Authorities expect FSPs to follow as it relates to the interpretation and application of national AML/CFT measures. Although the Guidance Notes are described as guidance, FSPs are reminded that in deciding whether a person committed an offence under the relevant sections of the Law or complied with the AMLRs, the Courts shall consider whether that person followed any relevant supervisory guidance issued or adopted by the relevant Supervisory Authority at the time. It is expected therefore that FSPs will studiously comply with the Guidance Notes.

5. FSPs should also be aware of the enforcement powers of the Supervisory Authorities under the Anti-Money Laundering Regulations (2017 Revision) ("AMLRs") as they relate to supervisory or regulatory guidance.

[3] FATF R. 34 and Methodology 34.1

GUIDANCE NOTES ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING AND TERRORIST FINANCING IN THE CAYMAN ISLANDS

PART II

GENERAL AML/CFT GUIDANCE

Section 1

GENERAL MATTERS[4]

A. INTRODUCTION

1. This part of the Guidance Notes is applicable to FSPs as specified under Part I of these Guidance Notes[5]. They are to be read and applied in conjunction with the relevant Sector Specific Guidance Notes ("SSGN") that are provided in PART III to PART VIII hereof.

2. Sections in PART II of this document are arranged to correspond with "Parts" in the AMLRs. However, FSPs shall take note of the fact that such arrangement of sections is only for ease of reference and guidance for certain aspects may have been provided in different sections of this document. As such, FSPs shall consider these Guidance Notes in entirety and adopt and comply with all relevant sections as appropriate and not restrict themselves to any particular section of these Guidance Notes.

[4] Regulations 1 and 2 AMLRs (2017 Revision)
[5] Under Part I, see section 1 "Purpose and Scope"

Section 2

COMPLIANCE PROGRAMME, SYSTEMS AND TRAINING OBLIGATIONS[6]

A. INTRODUCTION

1. This section provides guidance on the systems, policies and procedures that an FSP shall establish and maintain to prevent and report ML/TF. The systems should be appropriate to the size of the FSP and the ML/TF risks to which the FSP is exposed.

B. PROGRAMMES AGAINST ML AND TF

1. FSPs should develop and maintain AML/CFT systems and programmes which should include:

   (1) Customer due diligence measures;

   (2) Policies and procedures to undertake a Risk Based Approach ("RBA");

   (3) Internal policies, procedures and controls to combat ML/TF, including appropriate compliance management arrangements;

   (4) Adequate systems to identify ML/TF risks relating to persons, countries and activities which should include checks against all applicable sanctions lists;

   (5) Record keeping procedures;

   (6) Internal reporting procedures;

   (7) Screening procedures to ensure high standards when hiring employees;

   (8) An appropriate employee training programme;

   (9) An audit function to test the AML/CFT system; and

   (10) Group-wide AML/CFT programmes.

2. Senior management of an FSP is responsible for the effective management of its business. Therefore, it is the responsibility of the senior management to ensure that appropriate systems are in place to prevent and report ML/TF/PF and the FSP is in compliance with the applicable legislative and regulatory obligations.

[6] Part II of the AMLRs (2017 Revision)

3. Detailed guidance on the above listed programmes is provided in different sections of this part of the Guidance Notes.

C. COMPLIANCE FUNCTION

1. FSPs should develop a comprehensive AML/CFT compliance programme to comply with the relevant and applicable laws and obligations, and prevent and report ML/TF/PF. FSPs' senior management should set a culture of compliance with a top-down approach.

2. To oversee the compliance function, FSPs shall appoint an AML Compliance Officer ("AMLCO") at the management level, who shall be the point of contact with the supervisory and other competent authorities.

3. Where a Supervisory Authority requires FSPs to provide notification or obtain prior approval for the appointment of an AMLCO, FSPs should comply with such requirements in the manner prescribed, if any, by the relevant Supervisory Authority.

4. AMLCOs must have the authority and ability to oversee the effectiveness of FSPs' AML/CFT systems, compliance with applicable AML/CFT legislation and guidance and the day-to-day operation of the AML/CFT policies and procedures.

5. An AMLCO must be a person who is fit and proper to assume the role and who:

   (1) has sufficient skills and experience;

   (2) reports directly to the Board of Directors ("Board") or equivalent;

   (3) has sufficient seniority and authority so that the Board reacts to and acts upon any recommendations made;

   (4) has regular contact with the Board so that the Board is able to satisfy itself that statutory obligations are being met and that sufficiently robust measures are being taken to protect the FSP against ML/TF risks;

   (5) has sufficient resources, including sufficient time and, where appropriate, support staff; and

   (6) has unfettered access to all business lines, support departments and information necessary to appropriately perform the AML/CFT compliance function.

6. An FSP may demonstrate clearly apportioned roles for countering ML and TF where the AMLCO (or other audit, compliance, review function):

   (1) Develops and maintain systems and controls (including documented policies and procedures) in line with evolving requirements;

(2) Ensures regular audits of the AML/CFT programme;

(3) Maintains various logs, as necessary, which should include logs with respect to declined business, PEPs, and requests from competent authorities particularly in relation to investigations;

(4) Advises the Board of AML/CFT compliance issues that need to be brought to its attention;

(5) Reports periodically to the Board or Board committees (e.g. audit committee), as appropriate, on the FSP's systems and controls; and

(6) Responds promptly to requests for information by the relevant competent authorities.

7. An FSP may designate its AMLCO to act as a Money Laundering Reporting Officer ("an MLRO") or vice versa as far as the person is competent and has sufficient time to perform both roles efficiently. Where an individual is both an MLRO and AMLCO, that person should understand the roles and responsibilities of each function. The role of MLRO is discussed in section 9 of Part II of this document.

8. An FSP may designate a staff member to be an AMLCO or outsource[7] the compliance function. However, FSPs shall not contract or transfer their compliance obligations under the AMLRs. As such, irrespective of whether the AMLCO is an employee or not, the FSP is ultimately responsible for complying with applicable AML/CFT obligations. Guidance on outsourcing is provided under Part II section 10 ("Other Internal Controls") of this document.

D. GROUP-WIDE PROGRAMMES

1. The AMLRs require a financial group or other person carrying out relevant financial business through a similar financial group arrangement to have group-wide AML/CFT programmes.

2. In relation to branches and majority-owned subsidiaries, FSPs shall consider conducting a gap analysis between their group-wide AML/CFT programmes and the Cayman Islands AML/CFT legislative and regulatory requirements to ensure that they, at a minimum, comply with the applicable Cayman Islands requirements.

3. The gap analysis should be conducted initially before relying on the group-wide programmes and as and when there are any changes to applicable AML/CFT obligations or group-wide programmes. Where gaps are identified during the gap analysis, FSPs shall address those by making amendments to their AML/CFT programmes, as appropriate, subject to the legislative

[7] Outsourcing should be subject to any required approvals by the Board or equivalent governing body and the establishment of, and compliance with, appropriate policies and procedures. Where a FSP has outsourced the AMLCO function, the FSP shall refer to the Statement of Guidance on outsourcing issued by the Monetary Authority, if applicable.

limitations, if any, for doing so in the countries in which the other group entities operate.

4. The group-wide policies should be appropriate to all branches and majority-owned subsidiaries of the FSP and include:

   (1) Policies and procedures for sharing information required for conducting Customer Due Diligence ("CDD");

   (2) AML/CFT risk management policies and procedures; and

   (3) Adequate safeguards on the confidentiality and use of information exchanged.

5. Where the AML/CFT requirements of foreign branches and subsidiaries are less strict than those of the Cayman Islands, FSPs shall ensure that the group entities apply AML/CFT measures consistent with the requirements of this jurisdiction.

6. Where the host countries (i.e., countries in which a branch or a subsidiary of an FSP is located) do not permit the proper implementation of AML/CFT measures consistent with those of the Cayman Islands, the FSP shall inform the same to the relevant Supervisory Authority along with the appropriate additional measures that they wish to apply to manage ML/TF risks. Where the proposed additional measures are not sufficient to mitigate the risks, the Supervisory Authority may make recommendations to the FSP on further action.

Section 3

ASSESSING RISK AND APPLYING A RISK BASED APPROACH[8]

A. THE RISK-BASED APPROACH[9]

1. The AMLRs require FSPs to apply a RBA. The adoption of a RBA is an effective way to prevent or mitigate ML/TF as it will enable FSPs to ensure that AML/CFT measures are commensurate to the risks identified and allow resources to be allocated in the most efficient ways. As such, FSPs should develop an appropriate RBA for their particular organisation, structure and business activities. Where appropriate and feasible, the RBA should be articulated on a group-wide basis.

2. As is the case for an FSPs' overall risk management, FSPs' senior management should understand the nature and level of the risks that they are exposed to and ensure that systems and processes are in place to identify, assess, monitor, manage and mitigate ML/TF risks.

3. FSPs shall, before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied, take into account all the relevant risk factors. This would include the risks that are identified at the national level through the NRA or similar assessment, or risk assessment conducted by the relevant Supervisory Authority, whichever is most recently issued.

4. FSPs should at the outset of the relationship understand their business risks and know who their applicants for business ("applicants")/customers are, what they do, in which jurisdictions they operate, and their expected level of activity with the FSP.

5. As a part of the RBA, FSPs shall:

   (1) Identify ML/TF risks relevant to them;

   (2) Assess ML/TF risks in relation to-

      (a) Their applicants/customers (including beneficial owners);

      (b) Country or geographic area in which persons under (a) above reside or operate and where the FSP operates;

      (c) Products, services and transactions that the FSP offers; and

      (d) Their delivery channels[10].

[8] Part III of the AMLRs
[9] FATF R.1 and IN- 1
[10] Delivery channel in this context is the way/means whereby an FSP carries its business relationship with a customer, i.e., directly or through other means such as email, internet, intermediary, or any correspondent institution

(3) Design and implement policies, controls and procedures that are approved by senior management to manage and mitigate the ML/TF risks that they identified under (1), commensurate with assessments under (2) above;

(4) Evaluate mitigating controls and adjust as necessary;

(5) Monitor the implementation of systems in (3) above and improve systems where necessary;

(6) Keep their risk assessments current through ongoing reviews and, when necessary, updates;

(7) Document the RBA including implementation and monitoring procedures and updates to the RBA; and

(8) Have appropriate mechanisms to provide risk assessment information to competent authorities.

6. Under the RBA, where there are higher risks, FSPs are required to take enhanced measures to manage and mitigate those risks; and correspondingly, where the risks are lower, simplified measures may be permitted. However, simplified measures are not permitted whenever there is a suspicion of ML/TF.[11] In the case of some very high-risk situations or situations which are outside the firm's risk tolerance, the FSP may decide not to take on the applicant, or to exit from the relationship.

B. IDENTIFICATION AND ASSESSMENT OF RISKS

1. FSPs should adopt risk assessment policies and procedures appropriate to their size, nature and complexity. ML/TF risks should be measured considering all available relevant information.

2. FSPs should identify and assess inherent risks they face with regard to their products, services, delivery channels, customer types, geographic locations in which they or their customers operate and any other relevant risk category.

3. Additionally, FSPs should also conduct risk assessments of their customers, which includes:

(1) risk posed by the combination and complexity of products, services and delivery channels that the applicant/customer uses;

(2) risk posed by the geographical location of the applicant/customer (e.g., countries in which the applicant (and its beneficial owner) resides or from which it operates); and

(3) risk posed by the customer's characteristics, nature and purpose of the relationship or nature of transaction.

4. ML/TF risks may be measured using a number of risk categories and for each category applying various factors to assess the extent of the risk. For example, one of the risk factors that may be relevant when considering the risk associated with its customers is whether a customer issues bearer shares[12] or has nominee shareholders.

5. FSPs should consider all relevant risk factors for each risk category before determining the overall risk classification (E.g. high, medium or low) and the appropriate level of mitigation to be applied.

6. FSPs should make their own determination as to the risk weights to be given to the individual risk factors or combination of risk factors. When weighing risk factors, FSPs should take into consideration the relevance of different risk factors in the context of a particular customer relationship or occasional transaction. Examples of the application of various factors to the different categories that may result in high and low risk classifications are provided below.

7. FSPs may differentiate the extent of CDD measures, depending on the type and level of risk for the various risk factors. For example, in a particular situation, they could apply normal CDD for customer acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa.[13] Similarly, allowing a high-risk customer to acquire a low risk product or service on the basis of a verification standard that is appropriate to that low risk product or service, can lead to a requirement for further verification requirements, particularly if the customer wishes subsequently to acquire a higher risk product or service.

8. FSPs should document their risk assessment in order to be able to demonstrate their allocation of compliance resources, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to the relevant Supervisory Authority (and competent authorities and self-regulatory bodies ("SRBs"), if required). The nature and extent of any assessment of ML/TF risks should be appropriate to the nature and size of the business.

C. EXAMPLES OF RISK CLASSIFICATION FACTORS

9. As stated in paragraph 8 above, examples of risk factors for different risk categories are provided below. These examples of risk factors/indicators are not intended to be comprehensive, and although they are considered to be helpful indicators, they may not be relevant in all circumstances.

[12] Note that bearer shares are not permitted under the laws of the Cayman Islands
[13] FATF R.1 and IN- 12

High-Risk Classification Factors

10. When assessing the ML/TF risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially high-risk situations (in addition to those set out in Part VI of the AMLRs) include the following:

(1) Customer[14] risk factors:

(a) The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the FSP and the applicant/customer).

(b) Non-resident applicants/customers.

(c) Legal persons or arrangements that are personal asset-holding vehicles.

(d) Companies that have nominee shareholders or shares in bearer form[15].

(e) Business that is cash-intensive.

(f) The ownership structure of the applicant/customer appears unusual or excessively complex given the nature of the applicant/customer's business.

(2) Country or geographic risk factors:

(a) Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports by international bodies such as the FATF and MoneyVal, as not having adequate AML/CFT systems.

(b) Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.

(c) Countries identified by credible sources as having significant levels of corruption or other criminal activity.

(d) Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

[14] FSPs may conduct customer risk assessments for individual customers or group of customers having similar characteristics.

[15] FSPs are reminded that Cayman Islands Companies are not allowed to issue shares in bearer form. Please refer to the Companies Law for further guidance. As a best practice, FSPs should restrict themselves from conducting business with persons whose shares are in bearer form.

(3) Product, service, transaction or delivery channel risk factors:

(a) Anonymous transactions (which may include cash).

(b) Non-face-to-face business relationships or transactions.

(c) Payments received from unknown or un-associated third parties.

(d) The surrender of single premium life products or other investment-linked insurance products with a surrender value.

(e) Other activities, products or services including private banking, trade finance, payable through accounts, trust and asset management services, prepaid cards, remittance, lending activities (loans secured by cash collateral) and special use or concentration accounts.

Low Risk Classification Factors

11. When assessing the ML/TF risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially low risk situations include the following:

(1) Customer/Client risk factors:

(a) An applicant/customer that satisfies the requirements under regulation 22 (d) of the AMLRs.

(2) Product, service, transaction or delivery channel risk factors:

(a) Insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral.

(b) A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme.

(c) Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion[16] purposes.

[16] In general terms, financial inclusion involves providing access to an adequate range of safe, convenient and affordable financial services to disadvantaged and other vulnerable groups, including low income, rural and undocumented persons, who have been underserved or excluded from the formal financial sector. Financial inclusion also involves making a broader range of financial products and services available to individuals who currently only have access to basic financial products. Financial inclusion can also be defined as ensuring access to appropriate financial products and services at an affordable cost in a fair and transparent manner. For AML/CFT purposes, it is essential that these financial products and services are provided through financial institutions

(3) Country risk factors:

(a) Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems.

(b) Countries identified by credible sources as having a low level of corruption or other criminal activity.

(c) Countries or geographic areas that are listed by the AMLSG as having equivalent AML/CFT legislation.

12. In making a risk assessment, FSPs could, when appropriate, also take into account possible variations in ML/TF risk between different regions or areas within a country.

D. RISK MANAGEMENT AND MITIGATION

Risk Tolerance

1. Risk tolerance is the amount of risk that the FSP is willing and able to accept. An FSP's risk tolerance is an important component for achieving effective risk management and impacts its decisions about risk mitigation measures and controls. For example, if an FSP determines that the risks associated with a particular type of customer exceed its risk tolerance, it may decide not to accept or maintain that particular type of customer(s). Conversely, if the risks associated with a particular type of customer are within the bounds of an FSP's risk tolerance, the FSP must ensure that the risk mitigation measures it applies are commensurate with the risks associated with that type of customer(s).

2. FSPs should establish their risk tolerance. Such establishment should be done by senior management and the Board. In establishing the risk tolerance, the FSP shall identify the risks that it is willing to accept and the risks that it is not willing to accept. It should consider whether it has sufficient capacity and expertise to effectively manage the risks that it decides to accept.

3. When establishing the risk tolerance, an FSP should consider consequences such as legal, regulatory, financial and reputational consequences of an AML/CFT compliance failure.

4. If an FSP decides to establish a high-risk tolerance and accept high risks then the FSP should have mitigation measures and controls in place commensurate with those high risks.

subject to adequate regulation in line with the FATF Recommendations. Examples of such products/services can include basic/low amount savings accounts, school children savings accounts. For additional information see the FATF's Guidance "Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion".

Risk Management and Mitigation

5. FSPs should have appropriate policies, procedures and controls that enable them to manage and mitigate effectively the risks that they have identified, including the risks identified by the country. They should monitor the implementation of those controls and enhance them, if necessary. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with legal and regulatory requirements.[17]

6. The policies and procedures designed to mitigate assessed ML/TF risks should be appropriate and proportionate to these risks and should be designed to provide an effective level of mitigation.

7. The nature and extent of AML/CFT controls will depend on a number of aspects, which include:

   (1) The nature, scale and complexity of the FSP's business

   (2) Diversity, including geographical diversity of the FSP's operations

   (3) FSP's customer, product and activity profile

   (4) Volume and size of transactions

   (5) Extent of reliance or dealing through third parties or intermediaries.

8. Some of the risk mitigation measures that FSPs may consider include:

   (1) determining the scope of the identification and verification requirements or ongoing monitoring based on the risks posed by particular customers, productsor a combination of both;

   (2) setting transaction limits for higher-risk customers or products;

   (3) requiring senior management approval for higher-risk transactions, including those involving PEPs;

   (4) determining the circumstances under which they may refuse to take on or terminate/cease high risk customers/products or services;

   (5) determining the circumstances requiring senior management approval (e.g. high risk or large transactions, when establishing relationship with high risk customers such as PEPs).

Evaluating Residual Risk and Comparing with the Risk Tolerance

9. Subsequent to establishing the risk mitigation measures, FSPs should evaluate their residual risk.

[17] FATF R.1 and IN- 9

10. Residual risk is the risk remaining after taking into consideration the risk mitigation measures and controls. Residual risks should be in line with the FSP's overall risk tolerance.

11. Where the FSP finds that the level of residual risk exceeds its risk tolerance, or that its risk mitigation measures do not adequately mitigate high-risks , the FSP should enhance the risk mitigation measures that are in place.

E. MONITORING AML/CFT SYSTEMS AND CONTROLS

12. FSPs will need to have systems in place to monitor the risks identified and assessed as they may change or evolve over time due to certain changes in risk factors, which may include changes in customer conduct, development of new technologies, new embargoes and new sanctions. FSPs shall update their systems as appropriate to suit the change in risks.

13. Additionally, FSPs shall assess the effectiveness of their risk mitigation procedures and controls, and identify areas for improvement, where needed. For that purpose, the FSP will need to consider monitoring certain aspects which include:

(1) the ability to identify changes in a customer profile or transaction activity/behaviour, which come to light in the normal course of business;

(2) the potential for abuse of products and services by reviewing ways in which different products and services may be used for ML/TF purposes, and how these ways may change, supported by typologies/law enforcement feedback, etc.;

(3) the adequacy of staff training and awareness;

(4) the adequacy of internal coordination mechanisms i.e., between AML/CFT compliance and other functions/areas;

(5) the compliance arrangements (such as internal audit or external review);

(6) the performance of third parties who were relied on for CDD purposes;

(7) changes in relevant laws or regulatory requirements; and

(8) changes in the risk profile of countries to which the FSPs or its customers are exposed to.

F. DOCUMENTATION

1. FSPs must document their RBA. Documentation of relevant policies, procedures, review results and responses should enable the FSP to demonstrate to the relevant Supervisory Authority and/or to a court:

(1) risk assessment systems including how the FSP assesses ML/TF/PF risks;

(2) details of the implementation of appropriate systems and procedures, including due diligence requirements, in light of its risk assessment;

(3) how it monitors and, as necessary, improves the effectiveness of its systems and procedures; and

(4) the arrangements for reporting to senior management on the results of ML/TF risk assessments and the implementation of its ML/TF risk management systems and control processes.

2. FSPs shall note that the ML/TF risk assessment is not a one-time exercise and therefore, they must ensure that their ML/TF risk management processes are kept under regular review which is at least annually.

G. NEW PRODUCTS AND TECHNOLOGIES

1. FSPs should have systems in place to identify and assess ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products such as:

(1) digital information storage including cloud computing ;

(2) digital or electronic documentation storage;

(3) electronic verification of documentation;

(4) data and transaction screening systems; or

(5) the use of virtual or digital currencies.

2. Electronic money systems for example, may be attractive to money launderers or those financing terrorism if the systems offer liberal balance and transaction limits, but provide for limited monitoring or review of transactions. FSPs may also face increased difficulty in applying traditional AML/CFT measures because of the remote access by customers of the systems.

3. Systems utilizing new technologies that are involved with the collection, monitoring or maintenance of customer information for example, may not be as reliable or work as expected or may not be fully understood by staff. Such systems could therefore be vulnerable and result in FSPs not complying with the AMLRs.

4. FSPs should also:
   (1) Undertake a risk assessment prior to the launch or use of such products, practices and technologies; and

   (2) Take appropriate measures to manage and mitigate the risks[18].

[18] FATF- R. 15 and Methodology 15.1 and 15.2

3. FSPs should have policies and procedures in place or such measures as may be needed to prevent the misuse of technological development in ML/TF schemes, particularly those technologies that favour anonymity. Banking and investment business on the Internet, for example, add a new dimension to FSPs' activities. The unregulated nature of the Internet is attractive to criminals, opening up alternative possibilities for ML/TF, and fraud.

4. It is recognized that on-line transactions and services are convenient. However, it is not appropriate that FSP should offer on-line live account opening allowing full immediate operation of the account in a way which would dispense with or bypass normal identification procedures.

5. However, initial application forms could be completed on-line and then followed up with appropriate identification checks. The account, in common with accounts opened through more traditional methods, should not be put into full operation until the relevant account opening provisions have been satisfied in accordance with these Guidance Notes.

6. The development of technologies such as encryption, digital signatures, etc., and the development of new financial services and products, makes the Internet a dynamic environment offering significant business opportunities. The fast pace of technological and product development has significant regulatory and legal implications, and FSPs must ensure that appropriate staff members keep abreast of relevant technological developments and identified methodologies in ML/TF schemes. This may involve reviewing papers from international bodies such as the FATF on AML/CFT typologies, warnings and information issued by regulators and law enforcement, as well as information issued by industry bodies or trade associations.

7. To maintain adequate systems, FSPs should ensure that its systems and procedures can be and are kept up to date with such developments and the potential new risks and impact they may have on the products and services offered by the FSPs. Risks identified must be fed into the FSPs' business risk assessment.

Section 4

CUSTOMER DUE DILIGENCE[19]

A. CUSTOMER DUE DILIGENCE [20]

1. FSPs shall take steps to know who their customers are. FSPs shall not keep anonymous accounts[21] or accounts in fictitious names. FSPs are not allowed to open or maintain numbered accounts. A numbered account is an account that is not in the name of a customer and is managed with a number assigned to the underlying customer.

2. FSPs shall take steps to ensure that their customers are who they purport themselves to be. FSPs shall conduct CDD which comprises of identification and verification of customers including beneficial owners, understanding the intended nature and purpose of the relationship, and ownership and control structure of the customer.

3. CDD measures involve:

   (1) Identifying the applicant or customer and verifying that identity using reliable, independent source documents, data or information.

   (2) Identifying the beneficial owner(s) (of the applicant/customer and beneficiaries, where appropriate), and taking reasonable measures to verify the identity of the beneficial owner, such that it is satisfied that it knows who is the beneficial owner. Where the applicant/customer is a legal person or arrangement, FSPs should take steps to understand the ownership and control structure of the applicant/customer.

   (3) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

   (4) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the FSP's knowledge of the customer, its business and risk profile, including, where necessary, the source of funds.

4. FSPs shall conduct CDD when:

   (1) Establishing a business relationship;

   (2) Carrying out a one-off transaction valued in excess of fifteen thousand dollars (KYD 15,000), which comprises a single transaction or several transactions of smaller values that are linked;

[19] Part IV of the AMLRs (2017 Revision)
[20] FATF- R.10 and IN 1 to 3
[21] Example - Bearer shares

(3) Carrying out one-off transactions that are wire transfers;

(4) There is a suspicion of ML/TF; or

(5) There are doubts as to the veracity or adequacy of the previously obtained customer identification information.

5. In case of suspicion of ML/TF, an FSP should:

(1) Seek to identify and verify the identity of the applicant/customer and the beneficial owner(s), whether permanent or occasional, and irrespective of any exemption or any designated threshold (e.g. KYD 15,000 threshold for one-off transactions) that might otherwise apply; and

(2) File a SAR with the FRA, in accordance with the requirements under the Law and the AMLRs.

6. FSPs shall monitor transactions to determine whether they are linked. One-off transactions could be deliberately restructured into two or more transactions of smaller values to circumvent the applicable threshold (KYD 15,000). As such, FSPs should be vigilant and pay special attention to one-off transactions to ascertain if they are linked and exceed the set threshold. Guidance on one-off transactions is provided under section 5 of these Guidance Notes.

7. FSPs shall verify the identification of an applicant/customer using reliable independent source documents, data or information. For verification purposes, FSPs may use independent sources such as company registries, World Check (or similar internationally accepted screening databases), Regulatory Data Corp (RDC), and Google.

8. Similarly, FSPs shall identify and verify the applicant's beneficial owner(s) to ensure that the FSP understands who the ultimate beneficial owner is.

9. FSPs shall ensure that they understand the purpose and intended nature of the proposed business relationship or transaction. FSPs shall assess and ensure that the nature and purpose are in line with its expectation and use the information as a basis for ongoing monitoring.

10. The AMLRs require FSPs to identify and verify the identity of any person that is purporting to act on behalf of the applicant/customer ("authorised person"). The FSP should also verify whether that authorised person is properly authorised to act on behalf of the applicant/customer.

11. FSPs shall conduct CDD on the authorised person(s) using the same standards that are applicable to an applicant/customer.

12. Additionally, FSPs shall ascertain the reason for such authorisation and obtain a copy of the authorisation document.

13. FSPs shall conduct ongoing monitoring of their business relationship with their customers. Ongoing monitoring helps FSPs to keep the due diligence information up-to-date, and review and adjust the risk profiles of the customers, where necessary.

CDD- For Legal Persons & Arrangements[22]

14. When performing CDD measures in relation to applicants that are legal persons[23] or legal arrangements, FSPs should identify and verify the identity of the applicant, and understand the nature of its business, and its ownership and control structure (further guidance on the identification and verification procedures are provided in the later part of this section).

15. The purpose of the requirements set out regarding the identification and verification of the applicant and the beneficial owner is twofold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the applicant to be able to properly assess the potential ML/TF risks associated with the business relationship; and second, to take appropriate steps to mitigate the risks.

16. As two aspects of one process, these requirements are likely to interact and complement each other naturally. In this context, FSPs should:

(1) Identify the applicant and verify its identity. The type of information that would normally be needed to perform this function would be:

(a) Name, legal form and proof of existence – verification could be obtained, for example, through a certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust, or other documentation from a reliable independent source proving the name, form and current existence of the customer.

(b) The constitutional documents that regulate and bind the legal person or arrangement (e.g. the memorandum and articles of association of a company), as well as the names of the relevant persons holding a senior management position in the legal person or arrangement (e.g. directors, senior managing directors in a company, trustee(s) of a trust).

(c) The address of the registered office, and, if different, a principal place of business.

[22] FATF- R.10 and IN 5

[23] According to the FATF guidance issued on beneficial ownership, legal persons in the context of CDD include any entities, other than natural persons, that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, anstalt, partnerships or associations and other relevantly similar entities that have legal personality. This can include non-profit organizations, that can take a variety of forms which vary between jurisdiction, such as foundations, associations, or cooperative societies.

17. Further guidance on the identification and verification procedures for legal persons is provided below in "Identification information and verification procedures for corporate customers and partnerships/unincorporated businesses". Similarly, additional guidance for legal arrangements is provided below in "Identification information and verification procedures for Trust and fiduciary customers".

CDD For Beneficiaries Of
Long-term Insurance Policies[24]

18. FSPs conducting long-term insurance business shall, in addition to the CDD measures required for the applicant and the beneficial owner, conduct the following CDD measures on the beneficiary(ies) of insurance policies, as soon as the beneficiary(ies) are identified or designated:
    (1) for beneficiary(ies) that are identified as specifically named natural or legal persons or legal arrangements – taking the name of the person;

    (2) for beneficiary(ies) that are designated by characteristics or by class (e.g. spouse or children at the time that the insured event occurs) or by other means (e.g. under a will) – obtaining sufficient information concerning the beneficiary to satisfy the FSP that it will be able to establish the identity of the beneficiary at the time of the pay-out.

19. The information collected should be recorded and maintained in accordance with the requirements for record-keeping under Part VIII of the AMLRs.

20. For both cases referred to above, the verification of the identity of the beneficiary(ies) should occur at least at the time of the payout.

21. The beneficiary of a long-term insurance policy should be included as a relevant risk factor by the FSP in determining whether enhanced CDD measures are applicable. If the FSP determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, then the enhanced CDD measures should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

B. IDENTIFICATION INFORMATION AND VERIFICATION PROCEDURES

8. When considering entering into a business relationship, certain principles should be followed when ascertaining the level of identification and verification checks to be completed.

9. It is also recognised that the guidance relating to corporate customers (other than those regulated or listed) is principally directed at relatively small, closely controlled private companies without substantial physical activities.

[24] FATF- R.10 and IN 6

There is a distinguishable category of large private enterprise where it may be possible to obtain satisfactory evidence of identity from public sources, in which case the process by which the identity of the customer is verified should be approved in writing by senior management of the FSP. Copies of the identification evidence should be retained and maintained and made available to the relevant Supervisory Authority upon request or during the course of on-site inspections.

10. Reasonable measures should be taken to obtain sufficient information to distinguish those cases in which a business relationship is commenced or relevant financial business is conducted with a person acting on behalf of another. This also includes where the FSP is providing to his own customer, fiduciary or nominee services or holds funds on "customer accounts" which are omnibus accounts.

11. There may be cases where the intermediary applicant[25] meets both the following criteria:

    (1) acts in the course of business in relation to which an overseas regulatory authority exercises regulatory functions; and

    (2) is based or incorporated in or formed under the law of a country specified in the AMLSG Country List.

12. In such cases the FSP should require the applicant to complete and sign the Eligible Introducers ("EIs") form in Appendix A or its functional equivalent. If the intermediary applicant does not meet the above criteria, then full CDD as outlined in these guidance notes should be followed.

13. There are situations in which a customer is dealing in his own name on behalf of his own customers; for example, an attorney may himself enter into an arrangement on behalf of his customer or a fund manager may operate an account with a bank for the benefit of a number of customers not identified to the FSP. In this sort of case the intermediary is the applicant of the FSP rather than the underlying customers for which the intermediary acts.

14. The position of the intermediary applicant must be distinguished from that of a person (an 'introducer') who introduces a customer (which may also be his customer). The Introducer may then withdraw from the business relationship established with the person he has just introduced or may provide other collateral services for him, for example by passing on instructions. The person who is being introduced is the applicant of the FSP. It is the identity of the introduced applicant which must then be established.

15. Whenever appropriate and practical the applicant should be interviewed personally. If the applicant fails or is unable to provide adequate evidence of

[25] In this context an 'intermediary applicant' includes a person or applicant for business who is or appears to be acting as an agent or nominee for a principal.

identity or in circumstances in which the FSP is not satisfied that the transaction for which it is or may be involved is bona fide, an explanation should be sought and a judgment made as to whether it is appropriate to continue the relationship, what other steps can be taken to verify the applicant's/customer's identity and whether or not a report to the FRA ought to be made.

16. In circumstances in which the relationship is discontinued, funds held to the order of the applicant should be returned only to the source from which they came and not to a third party save for some exceptional instances such as to comply with a court order in case of controllership.

17. FSPs should have policies and procedures in place to address any specific risks associated with non-face to face business relationships and transactions.

18. Verification of identity is a cumulative process. Except for small one-off transactions that are not linked and do not pose suspicion of ML/TF, it is not sufficient to rely on a sole piece of evidence of identity. The below lists the identification information, verification documentation and associated requirements for identifying and verifying applicants/customers that are:

(1) Direct personal applicants/customers
(2) Corporate applicants/customers
(3) Partnerships/Unincorporated Businesses
(4) Trust and Fiduciary applicants/customers
(5) NPOs
(6) Other applicants/customers

IDENTIFICATION INFORMATION AND VERIFICATION PROCEDURES FOR DIRECT PERSONAL CUSTOMERS

Identification

19. It will normally be necessary to obtain the following documented information concerning direct personal customers:

(1) full name/names used;

(2) correct permanent address including postcode, (if appropriate);

(3) date and place of birth;

(4) nationality;

(5) occupation;

(6) the purpose of the account;

(7) estimated level of turnover expected for the account; and

(8) the source of funds (i.e. generated from what transaction or business.)

20. In the case of non-resident applicants, original, certified or electronic identification documents of the same sort set out in 19 above which bear a photograph and are pre-signed by the applicant should normally be obtained. On a risk based approach, this evidence should, where necessary, be supplemented by additional information such as a reference from a respected professional (e.g. attorney) with which the customer maintains a current relationship or other appropriate reference. FSPs should be aware that other identifying information when practicable, for example, a government issued identification number, could be of material assistance in an audit trail. In any event, the true name, current address or place of business/employment, date of birth and nationality of a prospective customer should be recorded.

21. Nationality(ies) should be established to ensure that the applicant is not from a high-risk country or a nation that is subject to sanctions by the United Nations or similar prohibition from any other official body or government that would prohibit such business being transacted. Information on applicable sanction orders are provided in the last section ("Sanctions Compliance") of this document.

22. Obtaining a date of birth provides an extra safeguard if, for example, a forged or stolen passport or driving licence is used to confirm identity which bears a date of birth that is clearly inconsistent with the age of the person presenting the document.

Documentation for Evidence of Identity

23. Information and documentation should be obtained and retained to support, or conform, the details provided by the applicant.

24. Identification documents, either originals or certified copies, or, subject to paragraph B 27 below, legitimate electronic documentation should be pre-signed and bear a photograph of the applicant, e.g.:

(1) Current valid passport(s);

(2) A Cayman Islands employer ID card bearing the photograph and signature of the applicant;

(3) Government issued photo bearing ID card;

(4) Provisional or full drivers licence bearing the photograph and signature of the applicant; or

(5) Armed Forces ID card

25. Identification documents which do not bear photographs or signatures, or are easy to obtain, are normally not appropriate as **sole** evidence of identity, e.g. birth certificate, credit cards, non-Cayman Islands provisional driving licence, student union cards.

26. Any photocopies of documents showing photographs and signatures should be plainly legible. Where applicants put forward documents with which an FSP is unfamiliar, either because of origin, format or language, the FSP must take reasonable steps to verify that the document is indeed genuine, which may include contacting the relevant authorities or obtaining a notarised translation. FSP should also be aware of the authenticity of passports.

27. CDD documents in electronic form are acceptable provided that the FSP takes a RBA and has suitable documented policies and procedures in place to ensure the authenticity of the electronic document(s). The FSP should, for example, check the type of electronic file and ensure that it is tamper resistant. For further guidance, FSPs may refer to the SOG on the 'Nature, accessibility and retention of records' issued by the Monetary Authority, where applicable.

Persons Without
Standard Identification Documentation

28. Irrespective of the type of business, it is recognised that certain classes of applicants/customers, such as the elderly, the disabled, students and minors, may not be able to produce the usual types of evidence of identity, such as a driving licence or passport. In these circumstances, a common sense approach and some flexibility without compromising sufficiently rigorous AML/CFT procedures is recommended. The important point is that a person's identity can be verified from an original or certified copy of another document, preferably one with a photograph.

29. If information and documentation set above cannot be obtained to enable verification to be completed and the account to be opened, a request may be made to another institution or institutions (for example, entities that qualify under regulation 22(d) of the AMLRs) for confirmation of identity (as opposed to a banker's reference). Failure of that institution to respond positively and within a reasonable time should put the requesting institution on its guard.

Verification of Name & Address

30. FSPs should also take appropriate steps to verify the name and address of applicants by one or more methods, for example:

(1) obtaining a reference from a "respected professional" who knows the applicant;

(2) checking the register of electors;

(3) making a credit reference agency search;

(4) checking a current local telephone directory;

(5) requesting sight of a recent rates or utility bill. Care must be taken that the document is an original and not a copy. If a document is presented in an electronic form, it may be regarded as an original if it is evident that it was issued or created in such an electronic form; or

(6) personal visit to the home of the applicant where possible.

31. The term 'respected professional' could be applied to for instance, lawyers, accountants, directors or managers of a regulated institution, priests, ministers or teachers.

32. Where an applicant's address is temporary accommodation, for example an expatriate on a short term overseas contract, FSPs should adopt flexible procedures to obtain verification under other categories, such as a copy of contract of employment; a copy of that person's lease agreement; or his banker's or employer's written confirmation.

33. In circumstances where an applicant/customer appoints another person as an account signatory e.g. appointing a member of his/her family, full identification procedures should also be carried out on the additional account signatory.

34. The form in Appendix B may be used for verification of identity to supplement the identification documentation already held.

35. For the avoidance of doubt, the form in Appendix B is not intended to be used as the sole means of obtaining evidence of identity of an applicant, but is designed to be a standardised means by which verification can be obtained concerning identification evidence already obtained.

Certification of Identification Documents

Suitable Certifiers

36. A certifier must be a suitable person, such as for instance a lawyer, accountant, director or manager of a regulated entity/ FSP, a notary public, a member of the judiciary or a senior civil servant. Such persons are expected to adhere to ethical and/ or professional standards and exercise his or her profession or vocation in a jurisdiction that has an effective AML/CFT regime. The certifier should sign the copy document (printing his/her name clearly underneath) and clearly indicate his/her position or capacity on it together with a contact address and phone number.

37. The list above of suitable certifiers is not intended to be exhaustive, and FSPs should exercise due caution when considering certified copy documents,

especially where such documents are easily forged or can be easily obtained using false identities or originate from a country perceived to represent a high risk, or from unregulated entities in any jurisdiction.

38. Where certified copies of documents are accepted, it is the FSP's responsibility to satisfy itself that the certifier is appropriate. An FSP may for instance, include in its policies and procedures a list of suitable certifiers approved by senior management. In all cases, the FSP should also ensure that the customer's signature on the identification document matches the signature on the application form, mandate, or other document.

Face-to-Face

39. Where possible, face-to-face customers must show FSP's staff original documents. Copies should be taken immediately, retained and certified by a senior staff member at the managerial level or a member of staff that is suitably trained**.**

Non Face-to-Face

40. Any interaction between an FSP and an applicant/customer in a non-direct manner increases the exposure to risk. Not only does this allow for third parties to have access to assets or property through impersonation but may also disguise the true owner of that property by, for example, provision of false identification documentation. FSPs should put into place policies and procedures that appropriately address the risks posed by non-face-to-face contact for customers either at the opening of the business relationship or through the operation of that relationship.

41. Examples of financial business conducted on a non-face-to-face basis include internet and telephone banking, and online share dealing.

42. Where identity is verified electronically or copy documents are used, an FSP should apply additional verification checks. For example, where it is impractical or impossible to obtain sight of original documents, a copy should only be accepted where it has been certified by a suitable certifier as being a true copy of the original document and that the photo is a true likeness of the applicant.

Intra-group

43. In intra-group business, the FSP should ensure- a) that the certification of documents is in accordance with group policies and the local regulatory requirements of the jurisdiction where the business is being done; b) and those requirements are at least to the standard of the Cayman Islands.

IDENTIFICATION INFORMATION AND VERIFICATION PROCEDURES FOR CORPORATE CUSTOMERS

44. With respect to legal persons, FSPs should identify the beneficial owners of the applicant and take reasonable measures to verify the identity of such persons, through the following information:

(1) The identity of the natural person (if any – as ownership interests can be so diversified that there are no natural persons (whether acting alone or together) who is the beneficial owner;

(2) To the extent that there is doubt under (1) as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural persons (if any) exercising control of the legal person through other means; and

(3) Where no natural person is identified under (1) or (2) above, FSPs should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of the general partner, president, chief executive officer, director(s), manager(s), or such other person who is in an equal senior management position exercising control over the management of the legal person.

45. The following paragraphs provide detailed guidance as to the various acceptable documents concerning corporate (legal persons) customers. FSPs shall take a risk based approach in determining the scope of the identification and verification documentation that is required to be collected. FSPs may need to collect several or all types of documentation and information as listed below depending on the specifics/type of the corporate applicant and risks posed:

(1) Certificate of Incorporation or equivalent, details of the registered office, and, if different, a principal place of business; -

(2) Explanation of the nature of the applicant's business, the reason for the relationship being established, an indication of the expected turnover, the source of funds, and a copy of the last available financial statements where appropriate;

(3) Satisfactory evidence of the identity of each of the legal owners, beneficial owners and a Register of Members;

(4) In the case of a bank account, satisfactory evidence of the identity of the account signatories, details of their relationship with the company and if they are not employees an explanation of the relationship. Subsequent changes to signatories must be verified;

(5) Evidence of the authority to enter into the business relationship (for example, a copy of the Board Resolution authorising the account signatories in the case of a bank account);

(6) Copies of Powers of Attorney, or any other authority, affecting the operation of the account given by the directors in relation to the company;

(7) Obtain and verify the names and addresses of any natural persons having Powers of Attorney or the authority in (6)

(8) Copies of the list/register of directors or their equivalent;

(9) Satisfactory evidence of identity must be established for directors, one of whom should, if applicable, be an executive director, if where different from account signatories. FSPs shall take a risk based approach in determining the number of directors on whom due diligence should be conducted and document the rationale for such determination;

(10) Certificate of good standing or a similar document confirming that the applicant/customer is listed in the company registry of its place of formation and has not been dissolved, struck-off, wound up or terminated;

(11) A copy of the constitutional documents i.e., memorandum and articles of association, by-laws of the applicant/ customer.

46. It is sometimes a feature of corporate entities being used to launder money that account signatories are not directors, managers or employees of the corporate entity. In such circumstances, the FSP should exercise caution, making sure to verify the identity of the signatories, and where appropriate, monitoring the ongoing business relationship more closely.

47. Where it is impractical or impossible to obtain sight of the original Certificate of Incorporation or equivalent, an FSP may accept a suitably certified copy in accordance with the procedures stated in paragraphs under "Certification of Identification Documents" of this document.

48. It is recognised that on some occasions companies may be used as a disguise for their beneficial owner. FSPs shall take reasonable measures to ensure that they are not engaged in business relationship with such entities.

49. In addition to the documents and information to be obtained in respect of corporate customers, FSPs providing a registered office for a private trust company ("PTC") (as defined in the Private Trust Company Regulations, 2013), whether on their own account or for another FSP, should obtain the

identification evidence detailed for trust and fiduciary customers save to the extent not already obtained in respect of the private trust company itself.

IDENTIFICATION INFORMATION AND VERIFICATION PROCEDURES FOR PARTNERSHIPS / UNINCORPORATED BUSINESSES

50. In the case of Cayman Islands limited partnerships and other unincorporated businesses or partnerships FSPs should obtain, where relevant:

(1) Identification evidence for at least two partners/controllers, the general partner and/or authorised signatories, in line with the requirements for direct personal customers. When authorised signatories change, care should be taken to ensure that the identity of the current signatories has been verified.

(2) Evidence of the trading address of the business or partnership and a copy of the latest financial report and accounts (audited where applicable).

(3) An explanation of the nature of the business or partnership should be ascertained (but not necessarily verified from a partnership deed) to ensure that it has a legitimate purpose. In cases where a formal partnership arrangement exists, a mandate from the partnership authorising the opening of an account or undertaking the transaction and conferring authority on those who will undertake transactions should be obtained.

IDENTIFICATION INFORMATION AND VERIFICATION PROCEDURES FOR TRUST AND FIDUCIARY CUSTOMERS

51. Trusts and other fiduciary relationships can be useful to criminals wishing to disguise the origin of funds.

52. In the case of legal arrangements, FSPs shall identify the beneficial owners of the applicant and take reasonable measures to verify the identity of such persons, through the following information[26]:

(4) Trusts – the identity of the settlor, the trustee(s), the protector (if any), the enforcer (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership).

(5) Other types of legal arrangements – the identity of persons in equivalent or similar positions.

[26] FATF- R.10 and IN 5

53. In the event where an applicant settlor is a trustee, in its capacity as trustee, the FSP should take the necessary steps to verify the identity of that trustee and the identity and source of funds of the settlor of the trust from which the assets originated.

54. FSPs should normally, in addition to obtaining identification evidence for the trustee(s) and any other person who has signatory powers on the account:

(1) make appropriate enquiry as to the general nature of the trust (e.g. family trust, pension trust, charitable trust etc.) and the source of funds;

(2) obtain identification evidence for the settlor(s), i.e. the person(s) whose property was settled on the trust; and

(3) in the case of a nominee relationship, obtain identification evidence for the beneficial owner(s) if different to the settlor(s).

(4) in the case of a PTC, consider whether some or all of the documented information recommended to be obtained in respect of a corporate customer, should be obtained in respect of the private trust company save to the extent not already obtained in respect of the settlor(s).

55. In some cases it may be impractical for the FSP to obtain all of the above (e.g. if the settlor has died) or the FSP may need some additional information depending on the risks identified. As such, FSPs shall take a risk based approach in determining what identification and verification documentation should be obtained.

56. FSPs providing trustee services should refer to Part IV of these Guidance Notes for sector specific guidance.

IDENTIFICATION INFORMATION AND VERIFICATION PROCEDURES FOR NPOS (INCLUDING CHARITIES)

57. NPOs may pose a potential risk of ML/TF for FSPs. At the placement stage there may be difficulties in identifying the source of funds, the identity of the donor, and verifying the information where it is provided. In some circumstances, such as in the case of anonymous donations, the identity of the donor is not known and as a result neither is the source of the funds.

58. Where the entity is a corporate entity or a trust, the account opening procedures should be in accordance with the relevant procedures set out above.

59. Where an applicant is an NPO, it will normally be necessary to obtain the following documented information:

(1) An explanation of the nature of the proposed entity's purposes and operations; and
(2) The identity of at least two signatories and / or anyone who gives instructions on behalf of the entity.

60. Where an NPO is registered as such in an overseas jurisdiction, it may be useful for the FSP to contact the appropriate charity commission or equivalent body to confirm the registered number of the charity and to obtain the name and address of the commission's correspondent for the charity concerned. For example, www.guidestar.org provides a list of all IRS recognized non-profit organizations including charities; and www.charity-commission.gov.uk provides a list of registered charities. For various reasons, exhaustive lists of all legitimate NPOs in those jurisdictions are not available from these bodies.

61. Whilst it is not practical to obtain documentary evidence of identity of all donors, FSPs should undertake a basic "vetting" of foreign NPOs and NPOs established overseas, in relation to known ML and terrorist activities. This includes a reasonable search of public information; verifying that the NPO does not appear on any terrorist lists nor has any association with ML or a high risk country and that identification information on representatives / signatories is obtained. FSPs are advised to consult the databases related to applicable sanctions. Particular care should be taken where the purposes to which the associations' funds are applied are located in a high-risk country.

Provision of Safe Custody & Safety Deposit Boxes

62. Where facilities to hold boxes, parcels and sealed envelopes in safe custody are made available, it is expected that an FSP will follow the identification procedures set out in these Guidance Notes. In addition, such facilities should only be made available to account holders.

Managed Financial Services Providers

63. For the avoidance of doubt, an FSP which is managed by another FSP retains the ultimate responsibility for ensuring that the AMLRs are complied with.

64. It is recognised, however, that a managed FSP may have to delegate AML compliance functions in accordance with the principles set out in these Guidance Notes. There is no objection to such delegation provided that:

(1) Details thereof and written evidence of the suitability of any such person or institution to perform the relevant functions on behalf of the FSP are made available to the Monetary Authority on request;

(2) There is a clear understanding between the FSP and the delegate as to the functions to be performed;

(3) The relevant applicant/customer information is readily available to the Monetary Authority on request and to the FRA and law enforcement authorities in accordance with the relevant procedures; and

(4) The FSP satisfies itself on a regular basis as to the reliability of the delegate's systems and procedures.

65. Where the delegate is located in a AMLSG List country and is subject to the AML/CFT regime of that country, the Monetary Authority will regard compliance with the regulations of such jurisdictions as compliance with the AMLRs and Guidance Notes.

66. Where the function is sub-delegated to a person in a country that is not a AMLSG List country, then it is the responsibility of the FSP to ensure that the sub-delegate complies with the obligations required by the Cayman Islands.

67. Where the Compliance function is outsourced or where the managed FSP is relying on an Eligible Introducer ("EI") from another r jurisdiction, a gap analysis should be conducted before relying on the EI or outsourcing arrangement. The analysis should be conducted to identify the difference between compliance requirements of the Cayman Islands and those of the jurisdiction in which the person to whom the compliance function is outsourced operates or in which the EI operates. Where gaps are identified during the gap analysis, FSPs shall ensure that the EI or the outsourced entity follows the standards established by the Cayman Islands.

C. TIMING OF VERIFICATION[27]

1. The best time to undertake verification is prior to entry into the business relationship or conducting a transaction. However, it could be necessary for sound business reasons to open an account or carry out a significant one-off transaction before verification can be completed. FSPs may complete verification after the establishment of the business relationship, provided that:

   (1) This occurs as soon as reasonably practicable;
   (2) This is essential not to interrupt the normal conduct of business; and
   (3) The ML/TF risks are effectively managed

2. Examples of the types of circumstances (in addition to those referred to above for beneficiaries of long-term insurance policies) where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business, include:

[27] FATF- R.10 and IN 11 and 12

(1) Non face-to-face business.

(2) Securities transactions. In the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.

(3) In cases of telephone or electronic business where payment is or is expected to be made from a bank or other account, the person verifying identity should:

(a) satisfy himself/herself that such account is held in the name of the applicant at or before the time of payment; and

(b) not remit the proceeds of any transaction to the applicant or his/her order until verification of identity has been completed.

3. The above are only examples and FSPs should adopt risk management procedures with respect to the conditions under which an applicant may utilise the business relationship prior to verification. For the avoidance of doubt, FSPs should not postpone the verification where the ML/TF risks are high and enhanced due diligence measures are required to be performed.

4. Such conditions may include restricting the funds received from being passed to third parties, imposing a limitation on the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

5. Alternatively, a senior member of staff at the managerial level may be given authority to allow (sign-off) for a transaction to be conducted prior to the verification. Save in exceptional circumstances, this authority should not be delegated. Any such decision should be recorded in writing.

6. Verification, once begun, should normally be pursued either to a satisfactory conclusion or to the point of refusal. If an applicant does not pursue an application, the FSP's staff could consider that this in itself is suspicious, and they should evaluate whether a report is required.

D. EXISTING CUSTOMERS[28]

1. FSPs are required to apply CDD measures to existing customers on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when

[28] FATF- R.10 and IN 11 and 13

CDD measures have previously been undertaken and the adequacy of data obtained.

2. The CDD requirements under Part IV of the AMLRs do not imply that FSPs have to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. However, if an FSP has a suspicion of ML/TF or becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

3. An FSP is entitled to rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile.

E. OBLIGATIONS WHERE UNABLE TO COMPLETE CDD

1. Where an FSP is unable to complete and comply with CDD requirements as specified in the AMLRs, it shall not open the account, commence a business relationship, or perform the transaction. If the business relationship has already been established, the FSP shall terminate the relationship. Additionally, the FSP shall consider making a SAR to the FRA.

F. TIPPING-OFF & REPORTING

1. As mentioned in Part I of these Guidance Notes, the Law prohibits tipping-off. However, a risk exists that applicants/customers could be unintentionally tipped off when the FSP is seeking to complete its CDD obligations or obtain additional information in case of suspicion of ML/TF. The applicant/customer's awareness of a possible SAR or investigation could compromise future efforts to investigate the suspected ML/TF operation.

2. Therefore, if FSPs form a suspicion of ML/TF while conducting CDD or ongoing CDD, they should take into account the risk of tipping-off when performing the CDD process. If the FSP reasonably believes that performing the CDD or on-going process will tip-off the applicant/customer, it may choose not to pursue that process, and should file a SAR. FSPs should ensure that their employees are aware of, and sensitive to, these issues when conducting CDD or ongoing CDD.

G. NO SIMPLIFIED DUE DILIGENCE FOR HIGHER-RISK SCENARIOS

1. FSPs should not adopt simplified due diligence measures where the ML/TF risks are high. FSPs shall identify risks and have regard to the risk analysis in determining the level of due diligence. High-risk scenarios may include, but are not limited to the following:

   (1) the relevant person proposes to have a business relationship or carry out a one-off transaction with a PEP; or

   (2) the prospective customer holds a deposit-taking licence and proposes to establish a correspondent banking relationship with the FSP; or

   (3) the nature of the situation is such, or a risk assessment reveals, that a higher risk of ML/TF is likely.

H. ON-GOING MONITORING OF BUSINESS RELATIONSHIPS

1. Once the identification procedures have been completed and the business relationship is established, the FSP is required to monitor the conduct of the relationship/account to ensure that it is consistent with the nature of business stated when the relationship/account was opened.
2. FSP should develop and apply written policies and procedures for taking reasonable measures to ensure that documents, data or information collected during the "Identification" process are kept up-to-date and relevant by undertaking routine reviews of existing records.
3. This does not mean that there needs to be automatic renewal of expired identification documents (e.g. passports) where there is sufficient information to indicate that the identification of the customer can readily be verified by other means.
4. The relevance of the documentation underlying the FSP's records will be determined according to circumstances of the customer, and the nature and risk of the transaction or relationship. Particular attention should be paid to higher risk categories of customers and business relationships.
5. FSPs shall consider updating customer CDD records as a part its periodic reviews (within the timeframes set by the FSP based on the level of risk posed by the customer) or on the occurrence of a triggering event, whichever is earlier. Examples of triggering events include:

   (1) Material changes to the customer risk profile or changes to the way that the account usually operates;

   (2) Where it comes to the attention of the FSP that it lacks sufficient or significant information on that particular customer;

   (3) Where a significant transaction takes place;

   (4) Where there is a significant change in customer documentation standards; and

(5) Significant changes in the business relationship.

6. Examples of the above circumstances include:

(1) New products or services being entered into,

(2) A significant increase in a customer's salary being deposited,

(3) The stated turnover or activity of a corporate customer increases,

(4) A person has just been designated as a PEP,

(5) The nature, volume or size of transactions changes.

7. FSPs shall conduct on-going due diligence which includes scrutinising the transactions undertaken throughout the course of the business relationship with a customer.

8. FSPs should be vigilant for any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts. Possible areas to monitor could be:

(1) transaction type

(2) frequency

(3) amount

(4) geographical origin/destination

(5) account signatories

9. However, if an FSP has a suspicion of ML/TF or becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible

10. It is recognised that the most effective method of monitoring of accounts is achieved through a combination of computerised and human manual solutions. A corporate compliance culture, and properly trained, vigilant staff through their day-to-day dealing with customers, will form an effective monitoring method as a matter of course. Computerised approaches may include the setting of "floor levels" for monitoring by amount.

11. Whilst some FSPs may wish to invest in expert computer systems specifically designed to assist the detection of fraud and ML/TF, it is recognized that this may not be a practical option for many FSPs for the reasons of cost, the nature of their business, or difficulties of systems integration. In such circumstances FSPs will need to ensure they have alternative systems in place for conducting on-going monitoring.

Section 5

SIMPLIFIED DUE DILIGENCE MEASURES[29]

A. SIMPLIFIED DUE DILIGENCE MEASURES ("SDD")

1. FSPs may conduct SDD in case of lower risks identified by the FSP. However, the FSP shall ensure that the low risks it identifies are commensurate with the low risks identified by the country[30] or the relevant supervisory authority.

2. While determining whether to apply SDD, FSPs should pay particular attention to the level of risk assigned to the relevant sector, type of customer or activity by the NRA or relevant Supervisory Authority.

3. The simplified measures should be commensurate with the low risk factors. Examples of possible SDD measures are:

   (1) Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship.

   (2) Reducing the frequency of customer identification updates.

   (3) Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold, which in any event should be based on the customer profile.

   (4) Relying on a third party to conduct verification of identity of applicant/customer/beneficial owner(s).

4. SDD is not acceptable in higher-risk scenarios where there is an increased risk, or suspicion that the applicant is engaged in ML/TF, or the applicant is acting on behalf of a person that is engaged in ML/TF.

5. Where the risks are low and where there is no suspicion of ML/TF, the AMLRs allow the FSPs to rely on third parties for verifying the identity of the applicants and beneficial owners. Instances where an FSP can take SDD measures and rely on third parties are discussed below.

6. Where an FSP decides to take SDD measures on an applicant/customer, it should document the full rationale behind such decision and make available that documentation to the relevant Supervisory Authority on request.

B. SCHEDULE 3 OF THE MONEY LAUNDERING REGULATIONS ("MLRs")

1. Schedule 3 of the MLRs (2015 Revision[31]) no longer exists in the AMLRs. However, countries previously listed in the Schedule 3 that are considered to

[29] Part V of the AMLRs
[30] In the NRA or any similar assessments conducted by the Cayman Islands

have equivalent AML/CFT frameworks are now reflected in a list maintained and published by the Anti-Money Laundering Steering Group ("AMLSG"). That list is called the **"List of Countries and Territories Deemed to have Equivalent Legislation"** (the "AMLSG List").

2. The AMLSG List will be reviewed and revised from time to time by the AMLSG.

3. Operating or residing in these countries will not automatically qualify the person as low risk. Therefore, FSPs should take a RBA and consider other risk factors in assigning the appropriate overall risk rating.

4. FSPs may rely on particular third parties from these countries when conducting SDD as provided in the below paragraphs.

C. ACCEPTABLE APPLICANTS (Applicants for whom it may be appropriate to apply SDD)

1. FSPs are required to conduct verification of identity of applicants at the time of establishing the business relationship. However, regulation 22 of the AMLRs allows FSPs not to conduct verification where:

(1) The FSP knows the identity of the applicant/customer;
(2) The FSP knows the nature and intended purpose of the business relationship or one-off transaction;
(3) There is no suspicious activity; and
(4) the applicant/customer is a person who:

(a) is required to comply with the regulation 5 or is a majority-owned subsidiary of the relevant financial business;

(b) is a central or local government organisation, statutory body or agency of government in a country specified in the AMLSG List;

(c) is acting in the course of a business or is a majority-owned subsidiary of the business in relation to which an overseas regulatory authority exercises regulatory functions and is based or incorporated in, or formed under the law of, a country specified in the AMLSG List;

(d) is a company that is listed on a recognised stock exchange and subject to disclosure requirements which impose requirements to ensure adequate transparency of beneficial ownership, or majority owned subsidiary of a such company; or

(e) is a pension fund for a professional association, trade union or is acting on behalf of employees of an entity referred to in subparagraphs (a), to (d) above.

[31] The MLRs are repealed and replaced by the AMLRs

D. PAYMENTS DELIVERED IN PERSON OR ELECTRONICALLY

1. As provided for in regulation 23 of the AMLRs, when a financial transaction involves payment by the applicant and he does so by remitting funds from an account held in his name at a bank in the Cayman Islands or a bank regulated in a country specified in the AMLSG List, the FSP may defer to verify applicant/customer identity at that time. The FSP should however, have evidence identifying the branch or office of the Bank and verifying that the account is in the name of the customer.

2. It may be reasonable to take no further steps to verify identity when payment is made by post, in person or electronic means, or details of the payment to be delivered by post or in person, to be confirmed via telephone or other electronic means if the payment is made from an account (or joint account) in the applicant's name at a bank in a country specified in the AMLSG List.

3. However, such exemption is not allowed :

   (1) If the circumstances of the payment are such that a person handling the transaction knows or suspects, or has reasonable grounds of knowing or suspecting that the applicant /customer is engaged in ML/TF, or that the transaction is carried out on behalf of another person engaged in ML/TF;

   (2) If the payment is made for the purpose of opening a relevant account with a bank licensed under the BTCL in the Cayman Islands; and

   (3) If onward payment is to be made in such way that it results in a payment to the applicant/customer or any other person.

4. When payment does not meet the criteria set out above, and is made with no additional verification undertaken, in addition to the details of the relevant branch or office of the bank and the account name, a record should be retained indicating how the transaction arose.

5. If the payment meets the above criteria then the verification of identity of the applicant/customer must be conducted in accordance with the full identification procedures as outlined in the previous section of this part of the Guidance Notes before payment of any proceeds unless the payment is being made by operation of law. For instance, if the payment of the proceeds requires to be made to a person for whom a court is required to adjudicate payment; e.g. trustee in bankruptcy, a liquidator, a trustee for an insane person or a trustee of the estate of a deceased person.

E. RELIANCE ON THIRD PARTIES FOR VERIFICATION OF IDENTIFICATION

1. FSPs are required under the AMLRs to maintain identification procedures that result in the production of satisfactory evidence of identity of applicants. According to the AMLRs, evidence of identity is satisfactory if it is reasonably

capable of establishing that the applicant is the person he claims to be and the person who obtains the evidence is satisfied, in accordance with the procedures maintained under these regulations in relation to the FSP concerned, that it does establish that fact.

2. There are, however, circumstances in which obtaining and verifying such evidence may be unnecessary duplication, commercially onerous and of no real assistance in the identification of or subsequent investigation into ML/TF.

3. Where the risks are low and where there is no suspicion of ML/TF, subject to certain conditions FSPs may rely on third parties for verification of identification of applicants and beneficial owners.

APPLICANTS WHO ARE NOMINEES OR AGENTS FOR A PRINCIPAL[32]

4. FSPs may rely on applicants who are or appear to be acting as nominees or agents for their principals for the verification of identity of the principals (or beneficial owners). However, the applicant should be a person who falls within the categories listed under an acceptable applicant listed in paragraph C.1.(4) above[33].

5. Furthermore, an FSP shall not rely on the applicant unless the applicant provides a written assurance confirming that:

   (1) The applicant has identified and verified the identity of the principal and, where applicable, the beneficial owner on whose behalf the applicant may act;

   (2) The nature and intended purpose of the business relationship;

   (3) The applicant has identified the source of funds of the principal; and

   (4) The applicant will upon request by the FSP provide the copies of the identification and verification data or information and relevant documentation without any delay after satisfying the CDD requirements in respect of the principal and the beneficial owner.

6. Furthermore, an FSP who is bound by regulation 5 and who relies on the written assurance provided as specified above by the applicant is liable for any failure of the applicant to obtain and record the evidence of identity of the principal or beneficial owner, or to make the same available to the FSP on request without delay.

PROCEDURE FOR INTRODUCED BUSINESS[34]

7. FSPs may place reliance on the due diligence procedures of third party "Eligible Introducers" ("EI") with respect to applicants for business who are

[32] Regulation 24 of the AMLRs
[33] Regulation 22 of the AMLRs specifies who could be acceptable applicants for whom FSPs may apply SDD and not conduct verification.
[34] Regulation 25 of the AMLRs

introduced by the EI and for whom the EI provides a written assurance meeting the criteria in Section 5.E.5 above confirming that it has conducted customer verification procedures substantially in accordance with the AMLRs and the Guidance Notes. The AMLRs further specify and limit EIs to a person that is listed under acceptable applicants above in C. 1. (4).

8. The FSP is ultimately responsible for ensuring that adequate due diligence procedures are followed and that the documentary evidence of the EI that is being relied upon is satisfactory for these purposes. Satisfactory evidence is such evidence as will satisfy the AML/CFT regime in the AMLSG List country (which is at least the standard of the Cayman Islands) from which the introduction is made.

9. Only senior management should take the decision that reliance may be placed on the EI. The basis for deciding that normal due diligence procedures need not be followed should be part of the FSP's risk-based assessment and should be recorded and the record retained in accordance with the AMLRs. (See Appendix C for Introduced Business Flow Chart).

10. The FSP should not enter into a relationship with or rely on an EI if the FSP:

    (1) knows or suspects that the EI, the applicant or any third party on whose behalf the applicant is acting is engaged in ML/TF;

    (2) has any reason to doubt the identity of the applicant, the EI or beneficial owner; and

    (3) is not satisfied that CDD information or documentation will be made available upon request without any delay.

11. Where a relationship presents higher ML/TF risk, FSPs must consider whether it is appropriate to rely solely upon the EI or the terms of business provided by the EI containing the necessary information.

12. The decision of senior management that reliance may be placed on the EI is not static and should be assessed regularly to determine whether there is a reason that the relationship should be discontinued.

13. FSPs that depend on EIs must take steps to satisfy themselves that:

    (1) each person that they have so identified meets the criteria of an EI set out above;

    (2) the information provided clearly establishes that the identity of the applicant (or any beneficial owner) has been verified;

    (3) the level of CDD carried out is made known and that the CDD procedures of the EI are satisfactory;

(4) the EI will make available, on request without delay, copies of any identification and verification data and relevant documents on the identity of the applicants (and any beneficial owners) obtained when applying CDD measures.

14. In the case of 13 (1) above for instance, when the proposed EI is an overseas financial institution captured under C. 1. 4 (c) above, the FSP should obtain, evidence that it is regulated which may comprise corroboration from the EI's regulatory authority, or evidence from the EI itself.

15. When considering whether it is reasonable to rely on an EI additional consideration that senior management may consider include the following:

(1) whether there is a pre-existing customer relationship between the Cayman FSP and the EI and/or between the EI and the applicant and the length of that relationship;

(2) whether the nature of the business of the EI and applicant are appropriate to the business being introduced; and

16. The information provided by the EI should be in written form. The EI's Form in Appendix A or its functional equivalent that satisfies the criteria in E. 5 above should be completed in these circumstances.

17. If an EI fails or is unable to provide a written confirmation or undertaking of the sort required in 17 above, the relationship must be reassessed and a judgment made as to what other steps to verify identity are appropriate or, where there is a pattern of non-compliance, whether the relationship should be discontinued.

18. FSPs should also test procedures on a random and periodic basis to ensure that CDD documentation and information is produced by the EI upon demand and without undue delay. FSPs should maintain a record of the periodic testing, which should clearly highlight any difficulties/delays in the EI's producing the CDD documentation and the remedial action(s) taken by the FSP.

19. It would also be prudent for an FSP placing reliance on an EI to agree with that EI that the CDD information and verification documentation will be maintained for the period specified under the AMLRs. It should also be established that the EI will notify the FSP if it is no longer able to comply with any aspect of the agreement (e.g. if the EI ceases to trade or there is a change in the law) and provide the FSP with the records or copies of records.

20. If FSPs are aware of any cases where EIs have incorrectly been treated as eligible, they must take steps to obtain suitable CDD information and verification documents in accordance with the AMLRs.

21. Following introduction by an EI, it will not usually be necessary to re-verify identity or duplicate records in respect of each transaction or piece of business.

22. FSP and other persons that meet the criteria of EIs who are themselves subject to the AMLRs have no obligation to act as EIs. Should they choose to do so, however, they must be satisfied that the information provided has in fact been obtained appropriately and verified and will be made available to the person relying on it as soon as reasonably practicable. A Cayman Islands licensed bank branch for example should not provide confirmation to another party on any non-compliant account or in circumstances where it would be in breach of the law to provide customer information.

F. VERIFICATION OBLIGATIONS FOR ONE-OFF TRANSACTIONS

1. Unless a transaction is a suspicious one, an FSP is not required to obtain documentary evidence of identity for one-off transactions valued less than KYD 15,000. One-off transaction valued less than KYD 15,000 means is a one-off transaction where the amount of the (single) transaction or the aggregate of a series of linked transactions is less than KYD15,000. In the event of any knowledge or suspicion that ML/TF has occurred or is occurring, the case should be treated the same as one requiring verification and reporting.

2. As a matter of best practice, a time period of 12 months for the identification of linked transactions is normally acceptable. However, there is some difficulty in defining an absolute time scale that linked transactions may fall within. Therefore, the relevant procedures for linking will ultimately depend on the characteristics of the product rather than relating to any arbitrary time limit. For example, FSPs should be aware of any obvious connections between the sender of funds and the recipient.

3. Verification of identity will not normally be needed in the case of a one-off transaction referred to above. If, however, the circumstances surrounding the one-off transaction appear to the FSP to be unusual or questionable, it is likely to be necessary to make further enquiries. Depending on the result of such enquiries, it may then be necessary to take steps to verify the proposed customer's identity. If ML/TF is known or suspected, the FSP should not refrain from making a report to the FRA simply because of the size of the transaction.

Section 6

ENHANCED CDD MEASURES ("EDD")[35]

A. EDD MEASURES

1. FSPs should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, that have no apparent economic or lawful purpose.

2. Where the risks of ML/TF are higher, or in cases of unusual or suspicious activity, FSPs should conduct enhanced CDD measures, consistent with the risks identified. In particular, FSPs should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

3. Examples of enhanced CDD measures that could be applied for high-risk business relationships include:

   (1) Obtaining additional information on the applicant/customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.).

   (2) Updating more regularly the identification data of applicant/customer and beneficial owner.

   (3) Obtaining additional information on the intended nature of the business relationship.

   (4) Obtaining additional information on the source of funds or source of wealth of the applicant/customer.

   (5) Obtaining additional information on the reasons for intended or performed transactions.

   (6) Obtaining the approval of senior management to commence or continue the business relationship.

   (7) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

   (8) Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

[35] Part VI of the AMLRs

4. Where the FSP is unable to conduct enhanced CDD, it shall follow the procedures as specified in the section on CDD under "Obligations where unable to complete CDD" of this document.

B. HOLD MAIL ACCOUNTS

1. "Hold Mail" accounts are accounts where the accountholder has instructed the FSP not to issue any correspondence to the accountholder's address. Although this is not necessarily a suspicious act in itself, such accounts do carry additional risk to FSPs, and they should exercise due caution as a result.

2. Regardless of the source of "Hold Mail" business, it is recommended on a best practice basis that evidence of identity of the accountholder should be obtained by the FSP, even where the customer was introduced by an EI. "Hold Mail" accounts should be regularly monitored and reviewed.

3. It is recommended that FSP have controls in place for when existing accounts change status to "Hold Mail", and that the necessary steps to obtain the identity of the account holder are taken where such evidence is not already in the FSP file.

4. Accounts with a "c/o" address should not be treated as "Hold Mail" accounts, as mail is being issued, albeit not necessarily to the accountholder's address. There are of course many genuine innocent circumstances where a "c/o" address is used, but an FSP should monitor such accounts more closely as they represent a higher risk.

5. FSPs should incorporate procedures to check the current permanent address of hold mail customers when the opportunity arises.

C. High-Risk Countries[36]

1. Certain countries are associated with crimes such as drug trafficking, fraud and corruption, and consequently pose a higher potential risk to an FSP. Conducting a business relationship with an applicant/customer from such a country exposes the FSP to reputational risk and legal risk.

2. FSPs should exercise additional caution and conduct enhanced due diligence on individuals and/or entities based in high-risk countries.

3. Caution should also be exercised in respect of the acceptance of certified documentation from individuals/entities based in high-risk countries/territories and appropriate verification checks undertaken on such individuals/entities to ensure their legitimacy and reliability.

[36] FATF R.19 and IN- 19.1

4. FSPs are advised to consult publicly available information to ensure that they are aware of the high-risk countries/territories. While assessing risk of a country, FSPs are encouraged to consider among the other sources, sanctions issued by the UN and UK, the FATF high risk and non-cooperative jurisdictions, the FATF and its regional style bodies (FSRBs) such as MoneyVal mutual evaluation reports, and Transparency international corruption perception index.

5. Useful websites include: FATF website at www.fatf-gafi.org, the Financial Crimes Enforcement Network (FinCEN) at www.ustreas.gov/fincen/ for country advisories; the Office of Foreign Assets Control (OFAC) www.treas.gov/ofac for information pertaining to US foreign policy and national security; and Transparency International, www.transparency.org for information on countries vulnerable to corruption.

6. FSPs should be aware that with respect to high-risk countries, the relevant Supervisory Authority may apply countermeasures proportionate to the risks, which may include:

   (1) Requiring FSPs to apply specific elements of EDD measures.

   (2) Introducing relevant enhanced reporting mechanisms or systematic reporting of financial transactions.

   (3) Refusing the establishment of subsidiaries or branches or representative offices of FSPs from the country concerned, or otherwise taking into account the fact that the FSP is from a country that does not have adequate AML/CFT systems.

   (4) Prohibiting FSPs from establishing branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant branch or representative office would be in a country that does not have adequate AML/CFT systems.

   (5) Limiting business relationships or financial transactions with the identified country or persons in that country.

   (6) Prohibiting FSPs from relying on third parties located in the country concerned to conduct elements of the CDD process.

   (7) Requiring FSPs to review and amend, or if necessary terminate, correspondent relationships with FSPs in the country concerned.

   (8) Increasing examinations/inspections and/or external audit requirements for branches and subsidiaries of FSPs based in the country concerned.

   (9) Requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned.

Section 7

POLITICALLY EXPOSED PERSONS[37]

A. GENERAL

1. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose FSP to significant reputational and/or legal risk. The risk occurs when such persons abuse their public powers for either their own personal benefit and/or the benefit of others through illegal activities such as the receipt of bribes or fraud. Such persons, commonly referred to as 'politically exposed persons' (PEPs) or 'potentates', include heads of state, ministers, influential public officials, judges and military commanders[38].

2. Reference to PEPs in these Guidance Notes includes their family members and close associates.

3. Family members of a PEP are individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership.

4. Close associates to PEPs are individuals who are closely connected to PEP, either socially or professionally.[39]

5. Provision of financial services to corrupt PEPs exposes an FSP to reputational risk and costly information requests and seizure orders from law enforcement or judicial authorities. In addition, public confidence in the ethical standards of the whole financial system can be undermined.

6. FSPs are encouraged to be vigilant in relation to PEPs from all jurisdictions, who are seeking to establish business relationships. FSPs should, in relation to PEPs, in addition to performing normal due diligence measures:

    (1) have appropriate risk management systems to determine whether the customer is a politically exposed person;

    (2) obtain senior management approval for establishing business relationships with such customers;

    (3) take reasonable measures to establish the source of wealth and source of funds; and

    (4) conduct enhanced ongoing monitoring of the business relationship.

[37] Part VII of the AMLRs
[38] Please refer to the definitions of PEP, family member and close associate provided in the AMLRs
[39] Definitions of "family members" and "close associates" from Part II of the FATF June 2013 Guidance on Politically Exposed Persons (Recommendations 12 and 22)

7. FSPs should obtain senior management approval to continue a business relationship once a customer or beneficial owner is found to be, or subsequently becomes, a PEP.[40]

8. FSPs shall take a risk based approach to determine the nature and extent of EDD where the ML/TF risks are high. In assessing the ML/TF risks of a PEP, the FSP shall consider factors such as whether the customer who is a PEP:

(1) Is from a high risk country (see guidance on high risk countries);

(2) Has prominent public functions in sectors known to be exposed to corruption; and

(3) Has business interests that can cause conflict of interests (with the position held).

9. The other red flags that the FSPs shall consider include (in addition to the above and the red flags that they consider for other applicants):

(1) The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries;

(2) Funds are repeatedly moved to and from countries to which the PEP does not seem to have ties;

(3) A PEP uses multiple bank accounts for no apparent commercial or other reason;

(4) The PEP is from a country that prohibits or restricts certain citizens from holding accounts or owning certain property in a foreign country.

B. PEP STATUS

1. FSPs shall take a risk based approach in determining whether to continue to consider a customer as a PEP who is no longer a PEP. The factors that they should consider include:

(1) the level of (informal) influence that the individual could still exercise; and

(2) whether the individual's previous and current function are linked in any way (e.g., formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

[40] FATF R.12 and IN- 12

C. LONG-TERM INSURANCE POLICIES

1. In the case of long-term insurance policies, FSPs shall take steps to determine whether the beneficiary or beneficial owner of a beneficiary is a PEP. This determination should be done at least at the time of pay-out.

2. Where high risks are identified in the above cases, FSPs shall inform the senior management before the pay-out of the policy and conduct EDD on the whole business relationship. Additionally, where appropriate, FSPs shall consider filing a SAR.

Section 8

RECORD-KEEPING PROCEDURES[41]

A. GENERAL

1. FSPs should maintain, for at least 5 years after termination, all necessary records on transactions to be able to comply swiftly with information requests from the competent authorities. Such records should be sufficient to permit the reconstruction of individual transactions, so as to provide, if necessary, evidence for prosecution of criminal activity.

2. FSPs should also keep records of identification data obtained through the customer due diligence process, account files and business correspondence that would be useful to an investigation for a period of 5 years after the business relationship has ended. This includes records pertaining to enquiries about complex, unusual large transactions, and unusual patterns of transactions. Identification data and transaction records should be made available to domestic competent authorities upon request.

3. Beneficial ownership information must be maintained for at least 5 years after the date on which the customer (a legal entity) is dissolved or otherwise ceases to exist, or five years after the date on which the customer ceases to be a customer of the (professional intermediary or) the FSP.

4. Where there has been a report of a suspicious activity or the FSP is aware of a continuing investigation into ML/TF relating to a customer or a transaction, records relating to the transaction or the customer should be retained until confirmation is received that the matter has been concluded.

5. Records relating to verification of identity will generally comprise:

   (2) a description of the nature of all the evidence received relating to the identity of the verification subject; and

   (3) the evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy.

6. Records relating to transactions will generally comprise:

   (1) details of personal identity, including the names and addresses, of:
   - (a) the customer;
   - (b) the beneficial owner of the account or product; and
   - (c) any counter-party.

   (2) details of securities and investments transacted including:

[41] Part VIII of the AMLRs

(a) the nature of such securities/investments;
(b) valuation(s) and price(s);
(c) memoranda of purchase and sale;
(d) source(s) and volume of funds and bearer securities;
(e) destination(s) of funds and bearer securities;
(f) memoranda of instruction(s) and authority(ies);
(g) book entries;
(h) custody of title documentation;
(i) the nature of the transaction;
(j) the date of the transaction;
(k) the form (e.g. cash, cheque) in which funds are offered and paid out.

B. GROUP RECORDS

1. There may be circumstances in which group records are stored centrally outside the Cayman Islands. In the case of records that are maintained outside the Cayman Islands, the records shall be maintained in accordance with the AMLRs and should be able to be retrieved and provided to the competent authorities promptly on request without delay. For further guidance, FSPs may refer to the Statement of Guidance on Nature, Accessibility and Retention of Records issued by the Monetary Authority.

C. TRAINING RECORDS

1. FSPs should demonstrate that they have complied with the provisions of Section 5 of the AMLRs concerning staff training.

2. They may do so by maintaining records which include:

(1) details of the content of the training programmes provided;
(2) the names and designations/titles of staff who have received the training;
(3) the date on which the training was delivered;
(4) the results of any testing carried out to measure staff understanding of the money laundering requirements; and
(5) an on-going training plan.

D. ESTABLISHMENT OF REGISTERS

1. An FSP should maintain a register of all enquiries made to it by the FRA and all disclosures to the FRA.

2. The register should be kept separate from other records and contain as a minimum the following details:

(1) the date and nature of the enquiry;

(2) details of the account(s) involved; and

(3) be maintained for a period of at least 5 years after termination of the relationship.

E. EQUIVALENCY

1. Where, in order to satisfy the requirements of the AMLRs, the FSP- (a) has delegated the performance of any function to a person or institution in an AMLSG List country; or (b) relies on a person or institution in an AMLSG List country to perform any function required to be performed, then the FSP must be satisfied that the relevant records will be maintained in accordance with the relevant requirements of the AMLRs. FSPs may refer to section 10 of this part of the Guidance Notes and to the Statement of Guidance on Nature, Accessibility and Retention of Records issued by the Monetary Authority.

2. The FSP shall ensure that those records will be available to the relevant Supervisory Authority on request and to the FRA or law enforcement authorities in accordance with the relevant provisions.

Section 9

MONEY LAUNDERING REPORTING OFFICER[42]

A. INTERNAL REPORTING PROCEDURES FOR SUSPICIOUS ACTIVITIES

1. FSPs must establish written internal procedures so that, in the event of a suspicious activity being discovered, all staff is aware of the reporting chain and the procedures to be followed.

2. Such procedures should be periodically updated to reflect any legislative changes.

B. APPOINTING AN MLRO TO WHOM ALL REPORTS OF KNOWLEDGE OR SUSPICION OF ML/TF ARE MADE.

1. Each FSP should designate a suitably qualified and experienced person as Money Laundering Reporting Officer (MLRO) at management level, to whom suspicious activity reports must be made by staff.

2. The FSP should ensure that the person acting as MLRO can dedicate sufficient time for the efficient discharge of the MLRO function, particularly where the MLRO has other professional responsibilities.

3. As mentioned above (in the section on "Compliance Function"), the person designated as MLRO may carry out a Compliance, Audit or Legal role within the FSP's business.

4. FSPs should also designate a Deputy Money Laundering Reporting Officer ("DMLRO"), who should be a staff member of similar status and experience to the MLRO. In the absence of MLRO, the DMLRO shall discharge the MLRO functions.

5. The MLRO should be well versed in the different types of transactions which the FSP handles and which may give rise to opportunities for ML/TF. Appendix D and Sector Specific Guidance Notes in Parts III to VIII of the Guidance Notes gives examples of such transactions, which are not intended to be exhaustive.

6. It is recognised that it is possible that an FSP has no employees in the Cayman Islands and where it may not be possible for a senior member of staff (or a sole trader him/herself) cannot be the MLRO. In these circumstances the FSP may:

[42] Part IX of the AMLRs

(1) Identify a person with suitable qualifications and experience, who is fit and proper, as the appropriate person to assume the role of MLRO to whom an internal report is to be made, provided that that person has the following characteristics:

(a) is a natural person;

(b) is autonomous (meaning the MLRO is the final decision maker as to whether to file a SAR);

(c) is independent (meaning no vested interest in the underlying activity); and

(d) has and shall have access to all relevant material in order to make an assessment as to whether the activity is or is not suspicious.

(2) Delegate/outsource the MLRO function in accordance with the principles set out in these Guidance Notes. See section 10 for guidance on outsourcing.

7. Where the FSP is a mutual fund regulated in the Cayman Islands, the FSP should utilise the further options set out in the relevant Sector Specific Guidance Notes.

8. Where it is not possible to nominate a staff member (or a sole trader, him/herself) as a DMLRO, the FSP may delegate/outsource the DMLRO function in a similar manner to the MLRO as specified above.

9. Where the relevant Supervisory Authority requires FSPs to provide notification or obtain prior approval for the appointment of an AMLRO/DMLRO, FSPs should comply with such requirements in the manner prescribed, if any, by the relevant Supervisory Authority.

10. Where an FSP has no staff, the provisions under the AMLRs regarding awareness and training will not apply. However, the FSP shall ensure that the person assuming the role of the MLRO is receiving adequate AML/CFT related training (that is appropriate and useful to perform the MLRO function diligently) on a regular basis.

11. The FSP is responsible for ensuring that any staff member involved in the relevant activities of the FSP is aware of the identity of the MLRO (and DMLRO) and that all internal SARs are submitted to the MLRO or in his/her absence to the DMLRO.

12. Where the MLRO that is located outside of the Islands files a suspicious activity report with the appropriate authority under the laws and regulations of his home country, it would be appropriate, where permitted by such laws

and regulations, for the MLRO to simultaneously file a SAR with the FRA in the Cayman Islands.

C. IDENTIFYING THE MLRO AND REPORTING CHAINS

1. All staff engaged in the business of the FSP at all levels must be made aware of the identity of the MLRO and DMLRO, and the procedure to follow when making a suspicious activity report. All relevant staff must be aware of the chain through which suspicious activity reports should be passed to the MLRO. A suggested format of an internal report form is set out in Appendix E.

2. FSPs should ensure that staff report all unusual/suspicious activities to the MLRO, and that "any such report be considered in the light of all other relevant information by the MLRO, or by another designated person, for the purpose of determining whether or not the information or other matter contained in the report does give rise to a knowledge or suspicion."

3. Where staff continue to encounter suspicious activities on an account which they have previously reported to the MLRO, they should continue to make reports to the MLRO whenever a further suspicious transaction occurs, and the MLRO should determine whether a disclosure in accordance with the legislation is appropriate.

4. All reports of suspicious activities must reach the MLRO (or DMLRO in the absence of the MLRO) and the MLRO/DMLRO should have the authority to determine whether a disclosure in accordance with the legislation is appropriate. However, the line/relationship manager can be permitted to add his comments to the suspicious activity report indicating any evidence as to why he/she believes the suspicion is not justified.

D. IDENTIFYING SUSPICIONS

1. A suspicious activity will often be one that is inconsistent with a customer's known, legitimate activities or with the normal business for that type of account. Therefore, the first key to recognition is knowing enough about the customer and the customer's normal expected activities to recognize when a transaction, series of transactions, or an attempted transaction is unusual.

2. Although these Guidance Notes tend to focus on new business relationships and transactions, institutions should be alert to the implications of the financial flows and transaction patterns of existing customers, particularly where there is a significant, unexpected and unexplained change in the behaviour/activity of an account.

3. As the types of transactions which may be used by money launderers are almost unlimited, it is difficult to define a suspicious transaction. However, it

is important to properly differentiate between the terms "unusual" and "suspicious".

Unusual Vs Suspicious

4. Where a transaction is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, the transaction must be considered unusual, and the staff member put "on enquiry". Complex transactions or structures may have entirely legitimate purposes. However, FSPs should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

5. The background and purpose of such transactions should as far as possible be examined and documented by the FSP. Findings regarding enquiries about complex, unusual large transactions, and unusual patterns of transactions should be kept by the FSP, and be available to help competent authorities and auditors for at least five years.

6. Where the staff member conducts enquiries and obtains what that person considers to be a satisfactory explanation of the complex or unusual large transaction, or unusual pattern of transactions, the person may conclude that there are no grounds for suspicion, and therefore take no further action as he is satisfied with matters. However, where the enquiries conducted by the staff member do not provide a satisfactory explanation of the transaction, he may conclude that there are grounds for suspicion requiring disclosure and escalate matters to the MLRO/DMLRO/Line manager.

7. Enquiries regarding complex, unusual large transactions, and unusual patterns of transactions, their background, and their result should be properly documented and made available to the relevant authorities upon request. Enquiries to check whether complex or unusual transactions or structures have legitimate economic or lawful purpose, where conducted properly and in good faith, are not regarded as tipping off.

8. Activities which should put staff on enquiry may be recognizable as falling into one or more of the following categories. This list is not meant to be exhaustive, but includes:
   (1) any unusual financial activity of the customer in the context of the customer's own usual activities;

   (2) any unusual transaction in the course of some usual financial activity;

   (3) any unusually-linked transactions;

   (4) any unusual engagement of an intermediary in the course of some usual transaction or financial activity;

(5) any unusual method of settlement;

(6) any unusual or disadvantageous early redemption of an investment product; and

(7) any unwillingness to provide the information requested.

9. The guidance in D 1 to D 8 above should also be extended to attempted transactions or instructions.

E. QUESTIONS TO ASK YOURSELF

1. The following factors should be considered when seeking to identify a suspicious transaction. This list is not meant to be exhaustive.

(1) Is the applicant/customer known personally?

(2) Is the transaction in keeping with the customer's normal activity known to the FSP, the markets in which the customer is active and the customer's own business? (i.e. does it make sense?)

(3) Is the transaction in keeping with normal practice in the market to which it relates i.e. with reference to market, size and frequency?

(4) Is the role of the agent involved in the transaction unusual?

(5) Is the transaction to be settled in the normal manner?

(6) Are there any other transactions linked to the transaction in question which could be designed to disguise money and divert it into other forms or to other destinations or beneficiaries?

(7) Are the reasons for the transaction(s) comprehensible (i.e. might there be an easier, cheaper or more convenient method available?)

F. CASH TRANSACTIONS

1. Given the international nature of the business conducted by many FSPs, cash transactions may be relatively uncommon, whereas for banks, building societies or money services businesses offering services to local customers, cash transactions may be a normal every-day service to many customers.

2. Where cash transactions are being proposed by customers, and such requests are not in accordance with the customer's known reasonable practice, many FSPs will need to approach such situations with caution and make further relevant enquiries.

3. Depending on the type of business each FSP conducts and the nature of its customer portfolio, each FSP may wish to set its own parameters for the

identification and further investigation of cash transactions. Where the staff member of the FSP has been unable to satisfy him/herself that any cash transaction is reasonable, and therefore she/he considers it suspicious, he/she should make a disclosure as appropriate.

4. Whilst certain cash transactions may lead the FSP to make further enquiries to establish or dispel suspicion, it goes without saying that equal vigilance must be applied to transactions which do not involve cash.

G. ROLE OF STAFF MEMBERS

1. Staff should be required to report any suspicion of ML/TF either directly to their MLRO or, if the FSP so decides, to their line manager for preliminary investigation in case there are any known facts which may negate the suspicion subject to C(2) of this section.

2. Employees should comply at all times with the vigilance systems of their institution and will be treated as having met appropriate standards of vigilance if they disclose their suspicions to their MLRO or other appropriate senior colleague according to the vigilance systems in operation in their institution.

H. THE ROLE OF THE MLRO

1. On receipt of a report concerning a suspicious applicant/customer or suspicious activity, the MLRO/DMLRO should determine whether the information contained in such report supports the suspicion. The MLRO/DMLRO should investigate the details in order to determine whether in all the circumstances he/she in turn should submit a report to the FRA.

2. If the MLRO decides that the information does substantiate a suspicion of ML/TF, he/she must disclose this information promptly to the FRA. If the MLRO decides that the information does not substantiate a suspicion, he/she would nevertheless be well advised to record fully the reasons for his decision not to report to the FRA.

3. It is for each FSP (or group) to consider whether its vigilance systems should require the MLRO to report suspicions within the FSP (or group) to the inspection or compliance department at head office.

4. Failure by the MLRO to diligently consider all relevant material may lead to vital information being overlooked and the suspicious activity not being disclosed to the FRA in accordance with the requirements of the legislation. Alternatively, it may also lead to vital information being overlooked which may have made it clear that a disclosure would have been unnecessary.

5. MLROs should establish and maintain a register of ML/TF referrals made to him/her by staff.

6. Staff members should note that in the event of suspicion of ML/TF, a disclosure should be made even where there has been no transaction by or through the FSP. Staff members should ensure that they do not commit the offence of tipping off the customer who is the subject of the disclosure.

I. REPORTING SUSPICIONS TO THE FRA

1. If the MLRO decides that a disclosure should be made, a report, in standard form as prescribed by the FRA, should be sent to the FRA without delay. The FRA's prescribed reporting form can be found on its website through the link below.
http://www.fra.gov.ky/contents/page/4

2. The Form should be completed in its entirety and any fields that are not applicable should be so indicated. It is important that the MLRO fill in the form to the fullest extent possible providing as much relevant information and detail as they have available. This will provide more assurance that the information provided is of benefit to the FRA.

3. The reason for suspicion section of the Form is a key part of the report. It is important for the MLRO to explain why there are suspicions about a specific transaction or transactions. Information about the subject and why there is a suspicion in the context of the business relationship should be included. Other useful information that should be provided includes how the transaction and/or business relationship was initiated, relevant dates, the amount of funds involved, the current status of the account if applicable and what action if any the FSP intends to take or may have taken.

4. If the MLRO considers that a report should be made urgently (e.g. where the account is already part of a current investigation), initial notification to the FRA should be delivered by hand or any means prescribed by the FRA and must be followed up in writing as soon as is reasonably practicable.

5. Vigilance systems should require the maintenance of a register of all reports made to the FRA pursuant to this paragraph. Such registers should contain details of:
   (1) the date of the report;

   (2) the person who made the report;

   (3) the person(s) to whom the report was forwarded; and

   (4) a reference by which supporting evidence is identifiable.

J. DECLINED BUSINESS

1. It is normal practice for an FSP to turn away business that they suspect might be criminal in intent or origin. Where an applicant or a customer is hesitant/fails to provide adequate documentation (including the identity of any beneficial owners or controllers), consideration should be given to filing a SAR.

2. Also, where an attempted transaction gives rise to knowledge or suspicion of ML/TF, that attempted transaction should be reported to the FRA.

3. Reporting of such events will allow the FRA to build a clearer picture of the ML/TF threat to the Island, and to use such intelligence on a proactive basis.

4. Furthermore, the FSP should refrain from referring such business to other FSPs.

Section 10

OTHER INTERNAL CONTROLS
(RELATING TO AUDIT FUNCTION, OUTSOURCING, EMPLOYEE SCREENING AND TRAINING)

A. INTRODUCTION

1. FSPs are expected to have systems and controls that are comprehensive and proportionate to the nature, scale and complexity of their activities and the ML/TF risks they identified. FSPs obligation to establish and maintain AML/CFT policies and procedures are discussed in different sections of this document. This section specifically discusses the internal controls in relation to:

   (1) an audit function to test the AML/CFT systems, policies and procedures;

   (2) outsourcing arrangements;

   (3) employee screening procedures to ensure high standards when hiring employees; and

   (4) an appropriate employee training programme.

2. The type and extent of measures to be taken should be appropriate to the ML/TF risks, and to the size of the FSP.

B. AUDIT FUNCTION

1. An FSP should, on a regular basis, conduct an AML/CFT audit. The frequency of the audit should be commensurate with the FSP's nature, size, complexity, and risks identified during the risk assessments. The AML/CFT audits should be conducted to assess the AML/CFT systems which include:

   (1) test the overall integrity and effectiveness of the AML/CFT systems and controls;

   (2) assess the adequacy of internal policies and procedures including;

      (a) CDD measures;
      (b) Record keeping and retention;
      (c) Third party relationships (e.g. EIs) and supporting documentation; and
      (d) Transaction monitoring;

   (3) assess compliance with the relevant laws and regulations;

   (4) test transactions in all areas of the FSP, with emphasis on high–risk areas, products and services;

(5) assess employees' knowledge of the laws, regulations, guidance, and policies & procedures;

(6) assess the adequacy, accuracy and completeness of training programmes; and

(7) assess the adequacy of the FSP's process of identifying suspicious activity including screening lists.

C. OUTSOURCING

1. FSPs should maintain policies and procedures in relation to outsourcing where they intend to outsource some of their functions. The guidance provided here particularly addresses the required controls for outsourcing AMLCO and MLRO functions.

2. Where an FSP decides to outsource its compliance function or MLRO/DMLRO position, it should, prior to entering into the proposed outsourcing arrangement, assess associated risks including the country risk. Where the associated risks cannot be effectively managed and mitigated, the FSP shall not enter into that outsourcing arrangement.

3. The FSP shall conduct the due diligence on the proposed service provider to whom it intends to outsource as appropriate and also ensure that the service provider ("OSP") is fit and proper to perform the activity that is being outsourced.

4. Where the FSP decides to enter into an outsourcing arrangement, the FSP shall ensure that the outsourcing agreement clearly sets out the obligations of both parties.

5. FSPs entering into an outsourcing arrangement should develop a contingency plan and a strategy to exit the arrangement in the event that the OSP fails to perform the outsourced activity as agreed.

6. The OSP should report regularly to the FSP within the timeframes as agreed upon with the FSP. The FSP should have access to all the information or documents relevant to the outsourced activity maintained by the OSP.

7. FSPs must not enter into outsourcing arrangements where access to data without delay is likely to be impeded by confidentiality, secrecy, privacy, or data protection restrictions.

8. FSPs shall ensure that the outsourcing agreement requires OSPs to file a SAR with the FRA in case of suspicions arising in the course of performing the outsourced activity.
9. Where the outsourcing arrangement allows for sub-contracting, the OSP may sub-contract any of the outsourced activities that are allowed for sub-

contracting. The FSP shall ensure that while sub-contracting, the OSP follows the outsourcing standards equivalent to that of the FSP.

10. Where the OSP operates from a country outside the Cayman Islands in which the standards are lower when compared to the Cayman Islands, then the OSP should adopt the Cayman Islands standards. The same approach should be adopted in case of sub-contracting. Where the sub-contractor is from a country whose standards are lower when compared to the Cayman Islands, the sub-contractor should adopt the standards of the Cayman Islands.

11. For further guidance on outsourcing, FSPs may refer to the Statement of Guidance on Outsourcing issued by the Monetary Authority, where applicable.

D. EMPLOYEE SCREENING

1. The AMLRs (5 (a) (iii)) require FSPs to maintain procedures to screen employees to ensure high standards when hiring.

2. The extent of employee screening should be proportionate to the potential risk associated with ML/TF in relation to the business in general, and to the particular risks associated with the individual positions. Employee screening should be conducted at the time of recruitment, periodically thereafter, i.e., at least annually and where a suspicion has arisen as to the conduct of the employee.

3. FSPs shall ensure that their employees are competent and proper for the discharge of the responsibilities allocated to them. While determining whether an employee is fit and proper, the FSP may:

   (1) Verify the references provided by the prospective employee at the time of recruitment

   (2) Verify the employee's employment history, professional membership and qualifications

   (3) Verify details of any regulatory actions or actions taken by a professional body

   (4) Verify details of any criminal convictions; and

   (5) Verify whether the employee has any connections with the sanctioned countries or parties which may include doing checks against screening databases (e.g. world check).

E. EMPLOYEE TRAINING

1. Where FSPs have staff, they should ensure that all appropriate staff, in accordance with Section 5 of the AMLRs, receive training on ML/TF prevention on a regular basis, ensure all staff fully understand the procedures and their importance, and ensure that they fully understand that they will be committing criminal offences if they contravene the provisions of the legislation.

The Timing & Content of Training Programmes

1. Training to staff should be provided at least annually, or more frequently where there are changes to the applicable legal or regulatory requirements or where there are significant changes to the FSP's business operations or customer base.

2. FSPs should provide their staff training in the recognition and treatment of suspicious activities. Training should also be provided on the results of the FSP's risk assessments. Each FSP can tailor its training programmes to suit its own needs, depending on size, resources and the type of business they undertake.

3. Smaller organisations with no in-house training function may wish to approach third parties such as specialist training agencies, firms of attorneys or legal practitioners, or the major firms of accountants or management consultants. Training should be structured to ensure compliance with all of the requirements of the applicable legislation.

4. Where the FSP has delegated the performance of relevant functions to a person or an institution in an AMLSG List country, it must be satisfied that equivalent training and education procedures are in place in relation to the applicable laws and regulations of such country. In cases where the delegated party is an affiliate or subsidiary of the FSP, the FSP is typically responsible for ensuring that the respective staff is appropriately trained on a regular and ongoing basis.

Staff Awareness

5. Staff should appreciate the serious nature of the background against which the AMLRs have been issued. They should be aware of their own personal obligations and of their personal liability under the legislation should they fail to report information in accordance with internal procedures and legislation. All staff should be encouraged to co-operate fully and provide a prompt and adequate report of any suspicious activities.

6. All staff needs to be fully educated on the AML/CFT systems, policies and programmes (as specified in regulation 5 which includes systems in relation to

RBA, CDD, record keeping and reporting). FSPs should take steps to make the staff aware of the relevant AML/CFT legislation and regulatory requirements.

New Employees

7. Irrespective of seniority, all new employees should be given a general introduction to the background of ML/TF and the procedures for reporting suspicious activities to the MLRO, prior to them becoming actively involved in day to day operations. New employees should also receive a clear indication of the importance placed on ML/TF issues by the organisation, of the legal requirement to report, and of their personal legal obligations in this regard.

8. FSPs shall consider obtaining an undertaking from their staff members (both new and existing) confirming that they have attended the training on AML/CFT matters, read the FSP's AML/CFT manuals, policies and procedures, and understand the AML/CFT obligations under the relevant legislation.

Operations Staff

9. Staff members who deal with the public such as cashiers, sales persons etc., are the first point of contact with potential money launderers, and their efforts are vital to an organisation's effectiveness in combating ML/TF. Staff responsible for opening new accounts or dealing with new customers should be aware of the need to verify the customer's identity, for new and existing customers and be aware of the procedures for treatment of declined business as outlined in these Guidance Notes. Training should be given on the factors which may give rise to suspicions about a customer's activities, and actions to be taken when a transaction is considered to be suspicious.

10. Staff involved in the processing of deals or transactions should receive relevant training in the processing and verification procedures, and in the recognition of abnormal settlement, payment or delivery instructions. Staff should be aware of the types of suspicious activities which may need reporting to the relevant authorities regardless of whether the transaction was completed. Staff should also be aware of the correct procedure(s) to follow in such circumstances.

11. All staff should be vigilant in circumstances where a known, existing customer opens a new and different type of account, or makes a new investment e.g. a banking customer with a personal account opening a business account. Whilst the FSP may have previously obtained satisfactory identification evidence for the customer, the FSP should take steps to learn as much as possible about the customer's new activities.

Training for Supervisors, Managers & Senior Management

12. Although Directors and Senior Managers may not be involved in the day-to-day procedures for handling transactions that may relate to ML/TF, it is important that they understand the statutory duties placed upon them, their staff and the firm itself given that these individuals are involved in approving AML/CFT policies and procedures.

13. Supervisors, managers and senior management (including Board of Directors) should receive a higher level of training covering all aspects of AML/CFT procedures, including the offences and penalties arising from the relevant primary legislation for non-reporting or for assisting money launderers, the procedures relating to dealing with production and restraint orders and the requirements for verification of identity and retention of records.

Training for Money Laundering Reporting Personnel (MLRO)

14. MLROs and DMLROs should receive in-depth training on all aspects of the primary legislation, the AMLRs, supervisory or regulatory guidance and relevant internal policies. They should also receive appropriate initial and ongoing training on the investigation, determination and reporting of suspicious activities, on the feedback arrangements and on new trends of criminal activity.

Continuing Vigilance & Refresher Training

15. Over time, due to the multiple demands placed on their time, there is a danger that staff may become less vigilant concerning ML/TF, and there could be new/evolving threats and changes to the legislative or regulatory requirements. As such, it is vital that all staff receive appropriate refresher training to maintain the prominence that ML/TF prevention requires, and that they fully appreciate the importance that their employer places on AML/CFT and their compliance obligations.

Section 11

IDENTIFICATION AND RECORD-KEEPING REQUIREMENTS RELATING TO WIRE TRANSFERS[43]

A. GENERAL[44]

1. These Guidance Notes in respect of identification and record-keeping procedures relating to wire transfers are issued with the objective of preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds, and for detecting such misuse when it occurs. Specifically, they aim to ensure that basic information on the payer (originator) and payee (beneficiary) of wire transfers is immediately available:

   (1) to appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, and prosecuting terrorists or other criminals, and tracing their assets;

   (2) to the FRA for analysing suspicious or unusual activity, and disseminating it as necessary; and

   (3) to the payment service provider ("PSP") of the payer, intermediary service provider and PSP of the payee to facilitate the identification and reporting of suspicious transactions, and to implement the requirements to take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001) relating to the prevention and suppression of terrorism and terrorist financing.

2. These Guidance Notes are not intended to impose rigid standards or to mandate a single operating process that would negatively affect the payment system.

B. SCOPE[45]

1. These Guidance Notes apply to transfer of funds i.e., cross-border wire transfers and domestic wire transfers, including serial payments, and cover payments in any currency.

2. Recognising, and in keeping with international standards that certain transfers of funds represent a low risk of ML/TF, the AMLRs do not require FSPs to

[43] Part X of the AMLRs
[44] FATF R. 16 and IN. 16.1
[45] FATF R. 16 and IN. 16.3 to 16.5

comply with the identification and record keeping obligations provided in this section in case of the following types of funds transfers [46]:

(1) where the payer withdraws cash from his own account;

(2) where truncated checks (electronically imaged copies of original checks) are used;

(3) for fines, duties and levies within the Cayman Islands;

(4) where there is a debit transfer authorisation (standing order) between two parties permitting payments between them through accounts, if a unique identifier accompanies the transfer of funds, allowing the person to be traced back;

(5) where both the payer and the payee are PSPs acting on their own behalf; and

(6) by credit or debit card or similar payment instrument, providing that the payee has an agreement with the PSP permitting payment for goods or services and that the transfer is accompanied by a unique identifier permitting the transaction to be traced back to the payer.

C. WIRE TRANSFERS - INDENTIFICATION INFORMATION AND RECORD KEEPING REQUIREMENTS[47]

1. Information accompanying all qualifying wire transfers to which Part X of the AMLRs applies should always contain:

   (1) the name of the payer;

   (2) the payer's account number or unique identifier where such an account is used to process the transaction and allows the transaction to be traced back to the payer;

   (3) the payer's address, or date and place of birth;

   (4) the payer's customer identification number or the number of a government issued document, evidencing identity (e.g. passport or drivers licence);

   (5) the name of the payee; and

   (6) the payee account number or unique transaction reference in order to facilitate the traceability of the transaction identifier where such an account is used to process the transaction (and trace back).

2. The PSP of the payer shall verify the complete information on the payer before transferring the funds unless the payer's account is held with a BTCL licensee or where the payer is bound by regulation 5 of the AMLRs.

[46] Regulation 25 of the AMLRs
[47] FATF R. 16 and IN. 16.6 to 16.8

3. The PSP of the payer should keep complete information on the payer and payee, which accompanies wire transfers for a period of five years. The PSP of the payee and the intermediary service provider should also keep records of any information received on the payer for a period of five years.

4. The PSP of the payee shall verify the identity of the payee and keep records for five years. Similarly, an intermediary service provider shall also keep the records of the payee for five years.

D. BATCH TRANSFERS

1. For batch file transfers from a single payer where the PSP of the payee is located outside of the Cayman Islands, there is no need for complete payer information for each transfer bundled together if (a) that batch contains the complete payer information, (b) the individual transfers carry the account number of the payer or a unique identifier and (c) full payee information (that is fully traceable within the payee country).

E. DOMESTIC WIRE TRANSFERS

1. Where both the PSP of the payee and the PSP of the payer are situated within the Cayman Islands, transfer of funds need only be accompanied by the account information or a unique identifier which will allow the information to be traced back to the payer.

2. If the PSP of the payee requests complete information on the payer, then such information should be provided by the PSP of the payer within three working days of such request.

F. INCOMPLETE & MISSING INFORMATION ON INCOMING WIRE TRANSFERS

1. The PSP of the payer shall not execute the transfer where it is unable to collect and maintain information on the payer or payee.

2. The PSP of the payee should have effective risk based procedures in place to detect missing or incomplete information on both the payer and payee from the messaging or payment and settlement system used to effect the transfer of funds. In order not to disrupt straight-through processing, it is not expected that monitoring should be undertaken at the time of processing the transfer.

3. The PSP of the payee shall consider missing or incomplete information on the payer as a risk factor in assessing whether the transfer funds or any related transaction is suspicious and whether it must be reported to the FRA.

G. DETECTION UPON RECEIPT

1. Where the PSP of the payee detects, when receiving transfer of funds, that the required payer information is missing or incomplete, then it shall either reject the transfer, or ask for or otherwise obtain, complete information on the payer. This may include the acquisition of the information from a source other than the service provider of the payer.

H. POST-EVENT MONITORING

1. The PSP should subject incoming wire transfers to an appropriate level of post event random sampling that is risk-based. The sampling may be weighted toward transfers from :

   (1) countries deemed to be high-risk for ML/TF; and

   (2) PSPs of payers who are identified from such sampling as having previously failed to comply with the relevant information requirements.

2. This does not obviate the obligation to report suspicious actions in accordance with normal suspicious transaction reporting procedures.

3. Where the PSP regularly fails to supply the required payer information and the PSP of the payee has taken reasonable measures to have the PSP of the payer correct the failures, then the payment service provider of the payee should either-

   (1) reject any future transfers of funds from the PSP;

   (2) restrict its business relationship with the PSP; or

   (3) terminate its business relationship with the PSP and report to the FRA and the Monetary Authority any such decision to restrict or terminate the relationship.

I. PAYMENTS VIA INTERMEDIARIES & TECHNICAL LIMITATIONS

1. Where the PSP of the payer is situated outside the Cayman Islands and the intermediary payment service provider is situated within the Cayman Islands, then the intermediary payment service providers should ensure that all information received on the payer that accompanies a transfer of funds is kept with the transfer.

2. The intermediary payment service provider may use a payment system with technical limitations that prevent information on the payer from

accompanying the transfer, to send transfer of funds to the payment service provider of the payee, provided that it is able to provide the PSP of the payee with the complete information using a mutually acceptable means of communication.

3. Where the intermediary payment service provider receives a transfer of funds without complete information on the payer, then it may use a payment system with technical limitations if it is able to provide the PSP of the payee with the complete information using a mutually acceptable means of communication.

4. Where the intermediary payment service provider uses a payment system with technical limitations, it is obligated to make available within three working days to the PSP of the payee upon request, all information on the payer which it has received. This is irrespective of whether the information is complete or not.

5. The intermediary service provider shall keep the all the information received for five years.

J. CO-OPERATION WITH THE FRA

1. PSPs are obligated to respond fully and without delay to enquiries made by the FRA concerning information on the payer accompanying transfer of funds and corresponding records.

K. MONEY SERVICES BUSINESS (MSB)/ MONEY VALUE TRANSFER SERVICES OPERATORS (MVTS)[48]

1. More detailed Sector Specific Guidance Notes are provided in Part VI of these Guidance Notes in respect of MSBs. However, these Guidance Notes which pertain to them in the execution of their wire transfer functions should also be observed by MVTS or MSB.

2. An MSB should comply with all of the relevant requirements of these Guidance Notes relating to wire transfers in the countries in which they operate, directly or through their agents.

3. In the case of an MSB that controls both the ordering and the beneficiary side of a wire transfer, the MSB:

   (1) Should take into account all the information from both the ordering and beneficiary sides in order to determine whether a SAR has to be filed; and

[48] FATF R. 16 and IN. 16.22

(2) Should file a SAR in any country affected by the suspicious wire transfer, and without delay make relevant transaction information available to the FRA and the relevant authorities in the Cayman Islands.

Section 12

CORRESPONDENT BANKS[49]

A. CORRESPONDENT BANKING

1. Correspondent Banking is the provision of banking services by one institution to another institution (the respondent institution). Correspondent banking does not include one-off transactions.

2. Correspondent institutions that process or execute transactions for their customer's (i.e. respondent institution's) customers may present high ML/TF risk and as such may require EDD.

3. In order for FSPs to manage their risks effectively, they shall consider entering into a written agreement with the respondent institution before entering into the correspondent relationship.

4. In addition to setting out the responsibilities of each institution, the agreement could include details on how the FSP will monitor the relationship to ascertain how effectively the respondent institution is applying CDD measures to its customers, and implementing AML/CFT controls. Furthermore, the agreement may include details in relations to the usage of the correspondent account, products and services permitted, and conditions in relation to payable through accounts.

5. Correspondent Institutions are encouraged to maintain an ongoing and open dialogue with the respondent institutions to discuss the emerging risks, strengthening AML/CFT controls, and help the respondent institutions in understanding the correspondent institutions' AML/CFT policies and expectations of the correspondent relationship.

6. FSPs should, in relation to cross-border correspondent banking and other similar relationships, in addition to performing CDD measures:

   (1) Gather sufficient information about a respondent institution to understand fully the nature of the respondent institution's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a ML/TF investigation or regulatory action.

   (2) Assess the respondent institution's AML/CFT controls.

   (3) Obtain approval from senior management before establishing new correspondent relationships.

   (4) Document the respective responsibilities of each institution.

[49] Part XI of the AMLRs

7. With respect to "payable-through accounts[50]", FSP shall be satisfied that the respondent institution has verified the identity of and performs on-going due diligence on the customers having direct access to accounts of the correspondent institution and that the respondent institution is able to provide relevant customer identification data upon request to the correspondent bank.

8. FSPs should not enter into, or continue, a correspondent relationship with a "shell bank"[51]; and should take appropriate measures to ensure that they do not enter into, or continue a corresponding banking relationship with a bank which is known to permit its accounts to be used by a shell bank. Neither should FSPs set up anonymous accounts or anonymous passbooks for new or existing customers.

9. FSPs should satisfy themselves that the respondents in foreign countries do not permit their accounts to be used by shell banks.

10. The similar relationships to which FSPs should apply criteria under 6 above include, for example, those established for securities transactions or funds transfers, whether for the cross-border financial institution as principal or for its customers.[52]

[50] FATF R.13 and IN- 13: Payable-through accounts are correspondent accounts that are used directly by third parties to transact business on their own behalf.

[51] A" Shell Bank" is a bank that is incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial institution

.

[52] FATF R.13 and IN- 13

Section 13

SANCTIONS COMPLIANCE

A. SANCTIONS OVERVIEW

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

2. For the purpose of these Guidance Notes, sanctions include international targeted financial sanctions and designations/directions issued under the TL and the PFPL.

3. The types of sanctions that may be imposed include:
   (1) targeted sanctions focused on named persons or entities, generally freezing assets and prohibiting making any assets available to them, directly or indirectly (these may be referred to as "specific directions");

   (2) economic sanctions that prohibit doing business with, or making funds or economic resources available to, designated persons, businesses or other entities, directly or indirectly (these may be referred to as "general directions");

   (3) currency or exchange control (such as the requirement for prior notification or authorisation for funds sent to or from Iran);

   (4) arms embargoes, which would normally encompass all types of military and paramilitary equipment (note that certain goods, such as landmines, are subject to a total prohibition and others, such as certain policing and riot control equipment, are subject to strict controls under export and trade control law);

   (5) prohibiting investment, financial or technical assistance in general or for particular industry sectors or territories, including those related to military or paramilitary equipment or activity;

   (6) controls on the supply of dual-use items (i.e. items with both a legitimate civilian use as well as a potential military or WMD use), including supplies of technology etc. and intangible supplies;

(7) import and export embargoes involving specific types of goods (e.g. oil products), or their movement using aircraft or vessels, including facilitating such trade by means of financial or technical assistance, brokering, providing insurance etc.;
(8) measures designed to prevent WMD proliferation; and
(9) visa and travel bans (e.g. banning members of a ruling regime from visiting the EU).

B. SANCTIONS COMPLIANCE

1. FSPs shall make their sanctions compliance programme an integral part of their overall AML/CFT compliance programme and accordingly should have policies, procedures, systems and controls in relation to sanctions compliance. FSPs shall provide adequate sanctions related training to their staff.

2. Official sanctions orders applicable in the Cayman Islands are published by the Cayman Islands Government in the Gazettes. Sanctions related information and applicable orders are posted on the Monetary Authority's website at http://www.cimoney.com.ky/AML_CFT/aml_cft.aspx?id=150. However, it is the responsibility of the FSPs to check from time-to-time for updates.

3. When conducting risk assessments, FSPs shall, as noted in Section 3.C, take into account any sanctions that may apply (to applicants/customers or countries).

4. FSPs shall screen applicants, customers, beneficial owners, transactions, service providers and other relevant parties to determine whether they are conducting or may conduct business involving any sanctioned person or person associated with a sanctioned person/country. In the event of updates to the relevant sanctions lists, FSPs may discover that certain sanctions are applicable to one or more of their customers, existing or new.

5. Where there is a true match or suspicion, FSPs shall take steps that are required to comply with the sanctions obligations including reporting Pursuant to the Law, AMLRs and TL, FSPs must file a SAR with the FRA, if they discover a relationship that contravenes a sanctions order or a direction under the PFPL FSPs shall document and record all the actions that were taken to comply with the sanctions regime, and the rationale for each such action.

6. FSPs are expected to keep track of all the applicable sanctions, and where the sanction lists are updated, shall ensure that existing customers are not listed.

7. Generally, the sanctions lists in force in the UK (HM Treasury) are extended to the Cayman Islands. These sanctions apply to all individuals and entities in the Cayman Islands. The lists issued in the United Kingdom (HM Treasury) might be different from lists issued by other countries, such as the United States (OFAC). While the OFAC sanctions may have no legal effect in the

Cayman Islands, because of the extra-territorial effect of the US measures, and their implications for international banking transactions in US dollars, FSPs should take note of them. It is important that FSPs carefully select the sanctions lists as lists that do not include at least all the sanctions applicable in the Cayman Islands may cause an FSP's sanctions compliance programme and monitoring to be deficient.

GUIDANCE NOTES ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING AND TERRORIST FINANCING IN THE CAYMAN ISLANDS

PART III

SECTOR SPECIFIC GUIDANCE: BANKS AND OTHER DEPOSIT TAKING FINANCIAL INSTITUTIONS

The purpose of this part of the Guidance Notes is to provide some guidance specifically for the Banks and Other Deposit Taking Financial Institutions sector. The types of FSPs covered in Part III are: (1) Retail and Non-Retail Banks; (2) Credit Unions; and (3) Building Societies. This sector specific guidance addresses specialised areas of relevant financial business that require more and / or different guidance or explanation than dealt with in the general body of these Guidance Notes. PART III should be read in conjunction with Part I and Part II of the Guidance Notes and the Appendices.

SECTION 1

RETAIL BANKS AND NON-RETAIL BANKS

A. OVERVIEW

1. Section 2 of the Banks and Trust Companies Law defines "banking business" as:

> "the business of receiving (other than from a bank or trust company) and holding on current, savings, deposit or other similar account money which is repayable by cheque or order and may be invested by way of advances to customers or otherwise".

2. Banking encompasses a wide range of financial products and services, which include, but are not limited to:

   (1) Retail banking, where banks offer products and services directly to personal and business customers (including legal arrangements), such as current accounts, loans (including mortgages) and savings products;
   (2) Corporate and investment banking, where banks provide corporate finance and corporate banking products and investment services to corporations, governments and institutions;
   (3) Investment services (or wealth management), where banks provide products and services to manage their customers' wealth (sometimes referred to as private banking); and
   (4) Correspondent services, where banking services are provided by one bank (the "correspondent bank") to another bank (the "respondent bank").[53] Guidance on correspondent banking is provided in Part II of these Guidance Notes.

B. SCOPE

1. This sector specific guidance seeks to provide practical assistance to Retail Banks and Non-Retail Banks (collectively, "Banks") in complying with the AMLRs, interpreting and applying the general provisions of these Guidance Notes, and for Banks to adopt sound risk management and internal controls for their operations.

2. The AMLRs apply to Banks as indicated in the list of activities falling within the definition of "Relevant Financial Business" in the Sixth Schedule of the Law.

[53] FATF Guidance for a Risk-Based Approach – The Banking Sector (October 2014)

3. It is the responsibility of each Bank to have systems and training in place to prevent ML/TF. This means that each Bank must maintain AML/CFT policies and procedures appropriate for the purposes of forestalling and preventing ML/TF.

C. ML/TF RISKS

1. Certain products and services offered by Banks may pose a higher risk of ML or TF depending on the nature of the specific product or service offered.

2. Such products and services may facilitate a higher degree of anonymity, or involve the handling of high volumes of currency or currency equivalents. Some of these products and services are listed below, but the list is not all inclusive:

Retail Banking

(1) The provision of services to cash-intensive businesses is a particular area of risk associated with retail banking. Some businesses are legitimately cash based and so there will often be a high level of cash deposits associated with some accounts. The risk is in failing to identify such businesses where the level of cash activity is higher than the underlying business would justify. [54]

Wealth Management

(2) Wealthy and powerful customers may be reluctant or unwilling to provide adequate documents, details and explanations. The situation with regards to these types of customers can be exacerbated where the customer occupies a high public profile, and may fall into the category of a PEP indicating that they wield or have recently wielded political or economic power or influence. Additionally, wealthy customers often have many accounts in more than one jurisdiction, either within the same firm or group, or within different firms, which may be more difficult for wealth managers to accurately assess the true purpose and business rationale for individual transactions. [55]

Correspondent Banking

(3) The correspondent bank often has no direct relationship with the underlying customers of the respondent bank and therefore may have limited information on a transaction and may not be in a position to verify their identities. Correspondent banks often have limited information regarding the nature or purpose of the underlying transactions, particularly when processing electronic payments.

[54] - [4] The Joint Money Laundering Steering Group – Prevention of money laundering/combating terrorist financing – Guidance for the UK Financial Sector Part II Sectoral Guidance (Amended November 2014)

Correspondent banking relationships, if poorly controlled, can allow other financial services firms with inadequate AML/CFT systems and controls, and customers of those firms[56], direct access to international banking systems.

Lending

(4) The main ML/TF risk arises through the acceleration of an agreed repayment schedule, either by means of lump sum payments, or early termination. Additionally, the involvement of multiple parties may increase the risk of ML/TF when the source and use of the funds are not transparent. This lack of transparency can create opportunities in any of the three stages of ML/TF financing schemes.

Payable Through Accounts ("PTA")

(5) PTA may be prone to higher risk because banks may not implement the same due diligence requirements for PTAs that they require of other customers who want to open checking and other accounts. These banks then process thousands of sub-accountholder cheques and other transactions, including currency deposits, through the foreign financial institution's PTA. In most cases, little or no independent effort is expended to obtain or confirm information about the individual and business sub-accountholders that use the PTAs. The potential for facilitating ML or TF and other serious crimes increases when a bank is unable to identify and adequately understand the transactions of the ultimate users of its account with a foreign correspondent.[57]

Trade Financing

(6) The international trade system is subject to a wide range of risks and vulnerabilities that provide criminal organizations with the opportunity to launder the proceeds of crime and move funds to terrorist organizations with a relatively low risk of detection. The involvement of multiple parties on both sides of any international trade transaction can make the process of due diligence more difficult. Also, due to the fact that trade finance can be more document-based than other banking activities, it can be susceptible to documentary fraud, which can be linked to ML/TF. While banks should be alert to transactions involving high-risk goods (e.g., trade in weapons or nuclear equipment), they need to be aware that any good may be over or under-valued in an effort to evade AML/CFT or customs regulations, or to move funds or value across national borders. [58]

---

[56] Financial institutions with poor AML/CFT systems are vulnerable to ML/TF risks and could be misused by the money launderers.
[57] Bank Secrecy Act Anti-Money Laundering Examination Manual – Payable Through Accounts - Overview
[58] Bank Secrecy Act Anti-Money Laundering Examination Manual – Trade Finance Activities - Overview

D. RISK BASED APPROACH

1. Banks must adopt a risk-based approach to managing ML/TF risks. The risk based approach to AML/CFT aims to support the development of prevention and mitigation measures that are commensurate to the ML/TF risks identified. This applies to the way banks allocate their compliance resources, organize their internal controls and internal structures, and implement policies and procedures to deter and detect ML/TF.

2. The bank's risk assessment forms the basis of a bank's RBA. In identifying and assessing the ML/TF risk to which they are exposed, Banks should consider a range of factors which may include[59]:

   (1) The nature, scale, diversity and complexity of their business;
   (2) Target markets;
   (3) The number of customers already identified as high risk;
   (4) The jurisdictions the bank is exposed to, either through its own activities or the activities of customers, especially jurisdictions with relatively higher levels of corruption or organised crime;
   (5) The distribution channels, including the extent to which the bank deals directly with the customer or the extent to which it relies (or is allowed to rely on) third parties to conduct CDD and the use of technology;
   The internal audit and regulatory findings; and
   (6) The volume and size of its transactions, considering the usual activity of the bank and the profile of its customers.

E. CUSTOMER DUE DILIGENCE

Who is the Customer/Applicant for Business?

1. The applicant may be any one of the following:
   (1) Natural persons;
   (2) Corporate persons (including MSBs, other deposit taking financial institutions, trust and fiduciary customers, companies); and
   (3) Partnerships / Unincorporated Businesses.

2. The following are the applicants whose identity must be verified by Banks and the evidence of identity required in each case:

Applicant for Business	**CDD Requirements (Highlights and supplementary only– please refer to section 4 of Part II of the Guidance Notes for the full (normal) CDD requirements).**
Natural Persons	(1) CDD documentation to identify and verify that identity should be obtained for the customer and, where appropriate, beneficial owner(s) of accounts.

[59] FATF - Risk-based approach guidance for the banking sector

	(2) Satisfactory evidence of identity, name and address confirmed by using one or more of the verification methods outlined in section 4 of Part II of the Guidance Notes. (3) Information, including necessary documentation required to understand the purpose and intended nature of the business relationship as outlined in section 4 of Part II of the Guidance Notes. Note: As stated in paragraph 16, Section 4, Part II of these Guidance Notes, it is usually not sufficient to rely on one document or data source and the extent of documentation and data that an FSP needs to collect depends on the risk assessment of the customer. FSPs must also be aware that some documents are more easily forged than others. Additionally, under the RBA, where there are higher risks, FSPs are required to take enhanced measures to manage and mitigate those risks. In such cases, Banks should supplement their verification documentation with references from other FSPs that are banks as in (4) below or with references from a respected professional (e.g. Attorney) or other appropriate reference with whom the customer maintains a current relationship. (4) Current, satisfactory bank reference from at least one bank with whom the prospective customer has had a relationship for not less than 3 years. If one is not forthcoming, satisfactory reference from a person or entity who has personal knowledge of the prospective customer and which establish his bona fides and integrity. References confirmed for genuineness. Genuineness may be confirmed by directly contacting the referee either via email or telephone. (5) For non-face-to-face verification, suitably certified or authenticated documents. Note: Given the international nature of banking business in and from the Cayman Islands, Bank FSPs should also be particularly vigilant in ensuring that CDD documentation collected that are in a foreign language are appropriately translated and verified and the copy of the translation kept with the original document. (6) Evidence of identity required for assets bought, sold or managed through the relationship

Corporate customers (including MSBs, other deposit taking financial institutions, trust and fiduciary customers, companies)	(1) (2) (3)	CDD as set out in Part II Section 4. N.B. Paragraphs 14 to 17 and 42 to 49 (of Part II Section 4).. Consistent with that required for natural persons, documentary evidence of identity for all directors that are natural persons; all those with signing powers, including third parties; and beneficial owners. (See section 4 of Part II in the Guidance Notes). Documentary evidence of identity of the new owner/controller where there is a change in ownership or control, in accordance with that required of natural persons.
Partnerships / Unincorporated Businesses	(1) (2) (3)	Identification information and satisfactory evidence of its existence, confirmed by at least one of the following independent checks, of existence of partnership / unincorporated business: (a) Partnership agreement or excerpt if relevant (b) Certificate of Registration (if applicable); Consistent with that required for direct personal customers, documentary evidence of identity required for partners/managers; all those with signing powers; all relevant parties, including third parties; and controlling partners / shareholders/beneficial owners as defined in the Guidance Notes, Section 4 (e.g., excerpt from partnership document. Documentary evidence of identity of the new owner/controller where there is a change in ownership or control, in accordance with that required of direct personal relationships.

When must identify be verified?

3. Customer verification information must be obtained and verification should be conducted prior to opening the account or establishing the business relationship.

4. Where the verification information is not forthcoming at the outset or within a reasonable time after initial contact, the relationship must be re-evaluated and transactions must not proceed.

When might it be possible to rely on third-parties to verify identity?

5. Banks should use their judgment in determining whether or not in the context of banking they should place reliance on third parties for conducting the due diligence procedures (verification). However, such reliance should only be considered in situations where the ML/TF risks have been assessed as low and where there is no suspicion of ML/TF.

6. Refer to section 5 of the Part II of the Guidance Notes, for guidance on SDD and "Procedure for Introduced Business".

F. ENHANCED DUE DILIGENCE ("EDD")

7. In case of high-risk situations/customers, the bank has to conduct EDD. Customers that pose high ML or TF risks present increased exposure to banks; in such cases, banks should apply EDD. EDD for high-risk customers is especially critical in understanding their anticipated transactions and implementing a suspicious activity monitoring system that reduces the bank's reputation, compliance, and transaction risks. High-risk customers and their transactions should be reviewed more closely and more frequently throughout the term of their relationship with the bank.

8. NPOs (including Charities), PEPs, Correspondent Banking, Trade Financing and customers in High-Risk Countries are some factors to consider which may result in EDD. Additional examples would include cases whereby a customer is confidentiality-driven, or presents a multi-layered structure of beneficial ownership.

9. In applying EDD, banks may for example collect sufficient information regarding intra-group relationships, if any; types of customers; service providers; and trading partners to establish a trading profile which can be monitored against transactions. More examples of enhanced CDD measures are provided in section 6, Part II of the Guidance Notes.

G. ON-GOING MONITORING

1. Banks should conduct on-going monitoring of the business relationship. On-going monitoring includes the scrutiny of transactions to determine whether those transactions are consistent with the Bank's knowledge of the customer and the nature and purpose of the business relationship. Monitoring also involves identifying changes to the customer profile and keeping it up to date, which may require the application of new, or additional CDD measures. Monitoring transactions is an essential component in identifying transactions/activities that are potentially suspicious.

2. Monitoring should be carried out on a continuous basis or triggered by specific transactions. It could also be used to compare a customer's activity with that of a peer group. For some types of banking activity where large volumes of transactions occur on a regular basis, automated systems may be the only realistic method of monitoring transactions. However, where automated systems are used, banks should understand their operating rules, verify their integrity on a regular basis and check that they address the identified ML/TF risks.

3. Banks should adjust the level of monitoring in line with their institutional risk assessment and individual customer risk profiles. Enhanced monitoring should be required for high risk situations. The adequacy of monitoring systems and the factors leading banks to adjust the level of monitoring should be reviewed regularly for continued relevance to the bank's AML/CFT risk programme.[60]

4. Refer to section 4 of the Part II of the Guidance Notes, "On-Going Monitoring of Business Relationships", for additional guidance.

H. ML/TF WARNING SIGNS OR "RED FLAGS"

1. The following are examples of potentially suspicious activities or "red flags" for ML/TF. Although these lists are not all-inclusive, they may help banks recognize possible ML/TF schemes. The below red flags, when encountered, may warrant additional scrutiny. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny will assist in determining whether the activity is unusual or suspicious or one for which there does not appear to be a reasonable business or legal purpose.

Transactions Involving Large Amounts of Cash

2. The following are some of the warning signs and red flags that Banks should be alert to in respect of transactions. The list is not exhaustive, but includes:

   (1) Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity.
   (2) Frequent withdrawal of large amounts by means of cheques, including traveller's cheques.
   (3) Customers making large and frequent cash deposits but cheques drawn on the accounts are mostly to individuals and firms not normally associated with their business.

[60] FATF Guidance for a Risk-Based Approach – The Banking Sector (October 2014)

(4) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.

(5) A large amount of cash is withdrawn and immediately deposited into another account.

(6) Exchanging an unusually large amount of small-denominated notes for those of higher denomination.

(7) Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank.

(8) Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash, rather than by way of debits and credits normally associated with the normal commercial operations of the company (e.g. cheques, letters of credit, bills of exchange).

(9) Depositing cash by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the cumulative total of which is substantial.

(10) The deposit of unusually large amounts of cash by a customer to cover requests for bankers' drafts, money transfers or other negotiable and readily marketable money instruments.

(11) Aberrant customer transactions of large cash deposits using cash deposit machines or similar facilities, thereby avoiding direct contact with the bank.

(12) Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.

(13) Customers whose deposits contain counterfeit notes or forged instruments.

(14) Customers who use cash advances from a credit card or charge card account to purchase money orders or bank drafts to transfer funds to foreign destinations.

(15) Customers who take cash advances from a credit card or charge card account to deposit into another account.

(16) Large cash payments for outstanding credit card or charge card balances.

(17) Customers who maintain positive balances on their credit card or charge card and then request cash advances or other type of refunds.

<u>Transactions Involving Transfers Abroad</u>

3. The following are some of the warning signs and red flags that Banks should be alert to in respect of transactions involving cross-border transfers. The list is not exhaustive, but includes:

(1) Large and regular payments that cannot be clearly identified as bona fide transactions, from and to countries or jurisdictions that are high-risk, which include jurisdictions that are associated with (a) the production, processing or marketing of narcotics or other illegal drugs or (b) terrorism or related criminal conduct.

(2) Substantial increase in cash deposits by a customer without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account or to a destination not normally associated with the customer.

(3) Repeated transfers of large amounts of money abroad accompanied by the instruction to pay the beneficiary in cash.

(4) Building up large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas.

(5) Cash payments remitted to a single account by a large number of different persons without an adequate explanation.

(6) "U-turn" transactions, i.e. where funds received from a person or company in a foreign country or jurisdiction are immediately remitted to another person or company in the same country or foreign jurisdiction, or to the sender's account in another country or jurisdiction.

Electronic Payments

1. The following are some of the warning signs and red flags that Banks should be alert to in respect of electronic payments. The list is not exhaustive, but includes:

(1) Multiple electronic payments ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.

(2) Electronic payments to or for an individual where information on the originator, or the person on whose behalf the transaction is conducted, is not provided with the wire transfer, when the inclusion of such information would be expected.

(3) Use of multiple personal and business accounts or the accounts of NPOs to collect and then funnel funds immediately or after a short time to a small number of foreign beneficiaries.

(4) Foreign exchange transactions that are performed on behalf of a customer by a third party followed by electronic payments of the funds to locations having no apparent business connection with the customer or to countries of ML/TF concern.

Lending

5. The following are some of the warning signs and red flags that Banks should be alert to in respect of lending. The list is not exhaustive, but includes:

(1) Loans secured by pledged assets held by third parties unrelated to the borrower.
(2) Loans secured by deposits or other readily marketable assets, such as securities, particularly when owned by apparently unrelated third parties.
(3) Borrower defaults on cash-secured loan or any loan that is secured by assets that are readily convertible into currency.
(4) Loans are made for, or are paid on behalf of, a third party with no reasonable explanation.
(5) To secure a loan, the customer purchases a certificate of deposit using an unknown source of funds, particularly when funds are provided via a currency or multiple monetary instruments.
(6) Loans that lack a legitimate business purpose, provide the bank with significant fees or assuming little or no risk, or tend to obscure the movement of funds (e.g., loans made to a borrower and immediately sold to an entity related to the borrower or back to back loans without any identifiable and legally admissible purpose).

Trade Finance

6. The following are some of the warning signs and red flags that Banks should be alert to in respect of trade finance. The list is not exhaustive, but includes:
(1) Items shipped that are inconsistent with the nature of the customer's business (e.g., a steel company that starts dealing in paper products, or an information technology company that starts dealing in paper products).
(2) Customers conducting business in high-risk jurisdictions.
(3) Customers shipping items through high-risk jurisdictions.
(4) Customers involved in potentially high-risk activities, including activities that may be subject to export/import restrictions.
(5) Obvious over or under pricing of goods and services.
(6) Obvious misrepresentation of quantity or type of goods imported or exported.
(7) Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.
(8) Customer requests payment of proceeds to an unrelated third party.
(9) Shipment locations or description of goods not consistent with letter of credit.
(10) Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment.

Employee Activity

7. The following are some of the warning signs and red flags that Banks should be alert to activities of their own employees. The list is not exhaustive, but includes:
   (1) Employee lives a lavish lifestyle that cannot be supported by his salary.
   (2) Employee fails to adhere to bank's internal policies, procedures, and processes and frequently overrides internal controls.
   (3) Employee is reluctant to take a vacation.

SECTION 2

CREDIT UNIONS

A. CREDIT UNIONS

1. Section 2 of the Cooperative Societies Law defines "credit union business", in relation to a registered society (i.e., a society that, among other criteria, has as its object the promotion of the economic interest of its members in accordance with cooperative principles), as:

   "The business of –
   (1) promoting thrift among the members of the society by the accumulation of their savings;
   (2) creating sources of credit for the benefit of the members of the society at a fair and reasonable rate of interest;
   (3) using and controlling the members' savings for their mutual benefit; and
   (4) training and educating the members in the wise use of money and in the management of their financial affairs.

B. SCOPE

1. This sector specific guidance seeks to provide practical assistance to credit unions in complying with the AMLRs, interpreting and applying the general provisions of these Guidance Notes, and for credit unions to adopt sound risk management and internal controls for their operations.

2. The AMLRs apply to credit unions as indicated in the list of activities falling within the definition of "Relevant Financial Business" in the Sixth Schedule of the Law.

3. It is the responsibility of each credit union to have systems and training in place to prevent ML/TF. This means that each credit union must maintain identification procedures, record-keeping procedures, and such other procedures and controls appropriate for the purposes of forestalling and preventing ML/TF.

C. ML/TF RISKS

1. Credit unions should consider all relevant risk factors at the sectorial and business relationship levels in conducting risk assessments and determining the appropriate level of mitigating measures to be applied.

2. Risk factors related to credit union business activities include, but are not limited to:

   (1) Money transfers to third parties;
   (2) Third parties paying in cash on behalf of the member;
   (3) Unusual loan or savings patterns (including regular significant payments);
   (4) Reluctance to provide documentary evidence of identity when joining;
   (5) Large One-Off transactions – e.g. sudden loan repayment; and
   (6) Regular requests for loans that are soon repaid.

D. RISK BASED APPROACH

1. Credit unions must adopt a risk-based approach to managing ML/TF risks. The risk based approach to AML/CFT aims to support the development of prevention and mitigation measures that are commensurate to the ML/TF risks identified.

2. The credit union needs to take a number of steps, documented in a formal policy which assesses the most effectual and proportionate way to manage ML and TF risks. These steps are:

   (1) Identify the ML and TF risks that are relevant to the credit union;
   (2) Assess the risks presented by the credit unions':
      (a) Members
      (b) Products
      (c) Delivery channels
   (3) Design and implement controls to manage and mitigate these assessed risks; and
   (4) Monitor and improve the effective operation of these controls.

E. CUSTOMER DUE DILIGENCE ("CDD")

Who is the Applicant for Business?

1. The applicant for business is a natural person.

2. The following are the applicants whose identity must be verified by credit unions and the evidence of identity required in each case:

	Applicant for Business	**Requirements**
1.	**Natural Persons**	(1) Identification documentation should be obtained for the customer and beneficial owners of accounts. (2) Evidence of identity required for assets bought, sold

		or managed through the relationship. (3) Satisfactory evidence, confirmed by using one or more of the verification methods outlined in section 4 Part II of the Guidance Notes. (4) Current, satisfactory bank reference from at least one bank with whom the prospective customer has had a relationship for not less than 3 years. If one is not forthcoming, satisfactory reference from a person or entity who has personal knowledge of the prospective customer and which establish his bona fides and integrity. (5) References confirmed for genuineness. This can be achieved by email or telephone confirmations. (6) For non face to face verification, suitably certified or authenticated documents.

When must identity be verified?

3. A credit union must obtain identity information prior to accepting a person's application to become a member.

F. ENHANCED DUE DILIGENCE ("EDD")

4. EDD is required in cases where a credit union is exposed to high ML/TF risks i.e., where the customer and product/service combination is considered to be a greater risk. (Refer to Part II, Section 6 of these Guidance Notes and Part VI of the AMLRs for additional information). EDD is required to mitigate the high ML/TF risks.

5. Example of high risk scenarios include[61]:

   (1) where the member is a PEP
   (2) when the member is involved in a business that is considered to present a high ML/TF risk

6. The nature and extent of EDD to be applied will depend on the nature and severity of the ML/TF risks identified. Examples of EDD measures are provided in Part II Section 6 of these Guidance Notes. The credit union should satisfy itself the EDD measures undertaken have sufficiently mitigated the risks identified.

[61] A high-risk customer does not mean that they will be involved in ML/TF or other criminal activity but that there is an increased possibility of such activity.

G. ON-GOING MONITORING

1. Credit unions must establish a process for monitoring member transactions and activities, which will highlight unusual transactions and those which need further investigation. It is important to take into account the frequency, volume and size of transactions. The key elements to monitoring are having up-to-date member information on the basis of which it will be possible to recognize the unusual transaction, and to ask pertinent questions to elicit the reasons for unusual transactions.

2. Refer to section 4 of Part II of the Guidance Notes, "On-Going Monitoring of Business Relationships".

H. ML/TF WARNING SIGNS OR "RED FLAGS"

1. The following are examples of potentially suspicious activities or "red flags" for ML/TF. Although these lists are not all-inclusive, they may help credit unions recognize possible ML/TF schemes. The below red flags, when encountered, may warrant additional scrutiny. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny will assist in determining whether the activity is unusual or suspicious or one for which these does not appear to be a reasonable business or legal purpose.

Customer Behaviour

2. The following are some of the warning signs and red flags that Credit Unions should be alert to in respect of customer behaviour. The list is not exhaustive, but includes:
   (1) Member uses unusual or suspicious identification documents, or refuses to produce originals for verification.
   (2) Member refuses to provide personal background information when opening an account.
   (3) Member's permanent address is outside of the credit union's service area.
   (4) Member indicates that he/she does not want a statement of account or any mail sent to his/her address.
   (5) A member is reluctant to provide information about the nature and purpose of the member's business or expected account activity.
   (6) Member asks about record-keeping or reporting requirements.
   (7) Member discourages employee from filing required reports or complying with recordkeeping requirements.
   (8) Member reluctant to proceed with cash transaction after being told it must be reported.

Cash Transactions

3. The following are some of the warning signs and red flags that Credit Unions should be alert to in respect of cash transactions. The list is not exhaustive, but includes:
   (1) Member regularly uses ATMs to make several deposits below the reporting threshold.
   (2) Member comes in with another member and they go to different tellers to conduct currency transactions under the reporting threshold.
   (3) Member opens different accounts under different names, and then makes several cash deposits under the reporting threshold.
   (4) Member deposits cash into several accounts in amounts below the reporting threshold and subsequently transfers the funds into one account and wire transfers them overseas.
   (5) Member attempts to take back a portion of the proposed cash deposit after learning that the proposed cash deposit exceeds the reporting threshold.
   (6) Member makes numerous purchases of monetary instruments with cash in amounts less than the reporting threshold.
   (7) Member purchases a number of prepaid cards for large amounts, inconsistent with normal account activity.

Credit Transactions

4. The following are some of the warning signs and red flags that Credit Unions should be alert to in respect of credit transactions. The list is not exhaustive, but includes:
   (1) Member suddenly pays down or pays off a large loan with no credible explanation as to where the funds came from.
   (2) Member purchases certificates of deposit and uses them as loan collateral.
   (3) Loans are made for, or paid on behalf of, a third party with no plausible explanation.
   (4) Member's loan proceeds are unexpectedly transferred offshore or member requests that loan proceeds be wire transferred.

Employee Activity

5. The following are some of the warning signs and red flags that Credit Unions should be alert to in respect of employee activity. The list is not exhaustive, but includes:

   (1) Employee lives a lavish lifestyle that cannot be supported by his salary.

(2) Employee fails to adhere to credit union's internal policies, procedures, and processes and frequently overrides internal controls.

(3) Employee is reluctant to take a vacation.

SECTION 3

BUILDING SOCIETIES

A. BUILDING SOCIETIES

1. A Building Society is a financial institution that provides banking and other financial services to its members (i.e. the people who invest in savings schemes and those who hold mortgages and other accounts with them). Building societies offer banking and related financial services, especially savings and mortgage lending.

B. SCOPE

1. This sector specific guidance seeks to provide practical assistance to Building Societies in complying with the AMLRs, interpreting and applying the general provisions of these Guidance Notes, and for Building Societies to adopt sound risk management and internal controls for their operations.

2. The AMLRs apply to Societies as indicated in the list of activities falling within the definition of "Relevant Financial Business" in the Sixth Schedule of the Law.

3. It is the responsibility of each building society to have systems and training in place to prevent ML/TF. This means that each building society must maintain identification procedures, record-keeping procedures, and such other procedures and controls appropriate for the purposes of forestalling and preventing ML/TF.

C. ML/TF RISKS

1. Building societies should consider all relevant risk factors at the sectorial and business relationship levels in order to assess the ML/TF risks and determine the appropriate level of mitigating measures to be applied.

2. Risk factors related to building society business activities include, but are not limited to:
   (1) Third parties paying in cash on behalf of the member;
   (2) Unusual loan or savings patterns (including regular significant payments);
   (3) Reluctance to provide documentary evidence of identity when joining;
   (4) Large One-Off transactions – e.g. sudden loan repayment; and
   (5) Regular requests for loans that are soon repaid.

D. RISK BASED APPROACH

1. Building societies must adopt a risk-based approach to managing ML/TF risks. The risk based approach to AML/CFT aims to support the development of prevention and mitigation measures that are commensurate to the ML/TF risks identified.

2. The building society needs to take a number of steps, documented in a formal policy which assesses the most effectual and proportionate way to manage ML and TF risks. These steps are:
   (1) Identify the ML and TF risks that are relevant to the building society;
   (2) Assess the risks presented by the building societies':
      (a) Members
      (b) Products
      (c) Delivery channels
      (d) Geographical areas of operation
   (3) Design and implement controls to manage and mitigate these assessed risks; and
   (4) Monitor and improve the effective operation of these controls.

E. CUSTOMER DUE DILIGENCE

Who is the applicant for business?

1. The applicant may be any one of the following:
   (1) Natural persons;
   (2) Corporate persons (including MSBs, companies); and
   (3) Partnerships / Unincorporated Businesses.

2. The following are the applicants for business whose identity must be verified by building societies and the evidence of identity required in each case:

	Applicant for Business	**Requirements**
	Natural Persons	(1) Identification documentation should be obtained for the customer and beneficial owners of accounts. (2) Evidence of identity required for assets bought, sold or managed through the relationship. (3) Satisfactory evidence, confirmed by using one or more of the verification methods outlined in section 4 of the Guidance Notes. (4) Current, satisfactory bank reference from at least one bank with whom the prospective customer has had a relationship for not less than 3 years. If one is not forthcoming, satisfactory reference from a person or entity who has personal knowledge of the prospective

		customer and which establish his bona fides and integrity. (5) References confirmed for genuineness. Genuineness may be confirmed by directly contacting the referee either via email or telephone. (6) For non face to face verification, suitably certified or authenticated documents.
	Corporate customers (including MSBs, companies)	(a) CDD as set out in Part II Section 4. N.B. Paragraphs 14 to 17 and 42 to 49 (of Part II Section 4).. (b) Consistent with that required for natural persons, documentary evidence of identity for all directors that are natural persons; all those with signing powers, including third parties; and beneficial owners. (See section 4 of Part II in the Guidance Notes). (c) Documentary evidence of identity of the new owner/controller where there is a change in ownership or control, in accordance with that required of natural persons.
	Partnerships / Unincorporated Businesses	(1) Identification information and satisfactory evidence of its existence, confirmed by at least one of the following independent checks, of existence of partnership / unincorporated business: (a) Partnership agreement or excerpt if relevant (b) Certificate of Registration (if applicable); (2) Consistent with that required for direct personal customers, documentary evidence of identity required for partners/managers; all those with signing powers; all relevant parties, including third parties; and controlling partners / shareholders/beneficial owners as defined in the Guidance Notes, Section 4 (e.g., excerpt from partnership document. (3) Documentary evidence of identity of the new owner/controller where there is a change in ownership or control, in accordance with that required of direct personal relationships.

When must identity be verified?

3. A building society must obtain identity information prior to accepting a person's application to become a member.

4. Where the verification information is not forthcoming at the outset or within a reasonable time after initial contact, the relationship must be re-evaluated and transactions must not proceed.

When might it be possible for identity to be verified by a party not based in the Cayman Islands?

5. Where the building society is relying on another entity within its group to verify the identity of a member who may not be physically present in the jurisdiction, all documentation must be certified by a senior manager within the group entity and copies provided prior to any outward transaction.

F. ENHANCED DUE DILIGENCE ("EDD")

6. EDD is required in cases where the credit union is exposed to high ML/TF risks i.e., where the customer and product/service combination is considered to be a greater risk. (Refer to Part II, Section 6 of these Guidance Notes and Part VI of the AMLRs for additional information). EDD is required to mitigate the high ML/TF risks.

7. Example of high risk scenarios include[62]:

   (1) where the member is a PEP
   (2) when the member is involved in or is a business that is considered to present a high risk for ML/TF

8. In applying EDD the building society may for example, collect sufficient information regarding intra-group relationships, if any; types of customers; service providers; and trading partners to establish a trading profile which can be monitored against transactions. The nature and extent of EDD to be applied will depend on the nature and severity of the ML/TF risks identified. More examples of enhanced CDD measures are provided in section 6, Part II of the Guidance Notes. The FSP should satisfy itself the EDD measures undertaken have sufficiently mitigated the risks identified

G. ON-GOING MONITORING

[62] A high-risk customer does not mean that they will be involved in ML/TF or other criminal activity but that there is an increased possibility of such activity.

1. Building societies must conduct on-going monitoring of the business relationship with its members. On-going monitoring of a business relationship includes:
   (1) Scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions are consistent with the building society's knowledge of the member, his/her business and risk profile;
   (2) Ensuring that the documents, data or information held by the building society are kept up to date and relevant.

2. Monitoring member activity is useful in identifying unusual/suspicious transactions/activities. On-going monitoring helps to adjust the mitigating measures proportionate to the risks and apply appropriate CDD measures.

3. Refer to section 4 of Part II of the Guidance Notes, "On-Going Monitoring of Business Relationships", for additional guidance.

H. ML/TF WARNING SIGNS OR "RED FLAGS"

1. The following are examples of potentially suspicious activities or "red flags" for ML/TF. Although these lists are not all-inclusive, they may help building societies recognize possible ML/TF schemes. The below red flags, when encountered, may warrant additional scrutiny. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny will assist in determining whether the activity is suspicious or one for which these does not appear to be a reasonable business or legal purpose.

   (1) A member provides minimal, vague or fictitious information that cannot be easily verified.
   (2) Frequent deposits or withdrawals of large amounts of cash with no apparent business source, or the business is of a type not known to generate substantial amounts of cash.
   (3) Accounts with a high volume of activity, which carry low balances or are frequently overdrawn.
   (4) A member makes large deposits and maintains large balances with little or no apparent justification.
   (5) A sudden, unexplained increase in account activity, both from cash and non-cash items. An account may be opened with a nominal balance that subsequently increases rapidly and significantly.
   (6) Reluctance to provide the purpose of the loan, or the stated purpose is ambiguous.

(7) Inappropriate disbursement of loan proceeds, or disbursements for purposes other than the stated loan purpose.
(8) A member suddenly pays down or pays off a large loan, with no evidence of refinancing or other explanation.
(9) Loans are made for, or are paid on behalf of, a third party with no reasonable explanation.
(10) Loans secured by pledged assets held by third parties unrelated to the borrower.
(11) Loans that lack a legitimate business purpose.

Employee Activity

2. The following are some of the warning signs and red flags that Building Societies should be alert to in respect of employee activity. The list is not exhaustive, but includes:

(1) Employee lives a lavish lifestyle that cannot be supported by his salary.
(2) Employee fails to adhere to the FSP's internal policies, procedures and processes and frequently overrides internal controls.
(3) Employee is reluctant to take a vacation.

GUIDANCE NOTES ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING AND TERRORIST FINANCING IN THE CAYMAN ISLANDS

PART IV

SECTOR SPECIFIC GUIDANCE: FIDUCIARY (COMPANY FORMATION AND TRUSTS)

The purpose of this part of the Guidance Notes is to provide some guidance specifically for the Fiduciary sector (Company Formation and Management and Trusts) on more complex AML / CFT matters or issues which require more explanation than provided for in the general body of these Guidance Notes This sector specific guidance should be read in conjunction with Part I and Part II of the Guidance Notes.

SECTION 1

COMPANY FORMATION AND MANAGEMENT

A. OVERVIEW

1. Company formation and management business carried out in and from the Cayman Islands is defined and regulated pursuant to the Companies Management Law (2003 Revision) and the Directors Registration and Licensing Law, 2014.

2. There are a number of FSPs under other regulatory laws that are allowed to engage in company formation and management activity without being required to hold a licence under the Companies Management Law. Those FSPs that operate within such circumstances are required to comply with the AML/CFT framework outlined in this Section and under the General Guidance Notes which are designed for company management and formation services professionals (CSPs).

B. SCOPE

1. This guidance is specific to CSPs, and is intended to provide support in complying with the AMLRs.

2. The AMLRs apply to CSPs as indicated in the list of activities falling within the definition of "Relevant Financial Business" in the Sixth Schedule of the POCL.

3. CSPs must have systems and training in place to prevent ML/TF. This means that each CSP must maintain ML and TF policies and procedures appropriate for the purposes of preventing ML and TF.

C. ML/TF RISKS

1. The company is an extremely versatile vehicle that is often used in various structures and for a broad range of activities; including financial structures, financial transactions, and the management and custody of wealth.

2. In spite of the many varied legitimate uses of companies, companies are vulnerable to being improperly utilised to perpetrate fraud, illegally hide the ownership of assets, hide the proceeds of corruption, perpetrate ML schemes, or to facilitate TF.

3. There is potential for companies to be misused to facilitate ML/TF activity at various stages by allowing the conversion of proceeds of crime or disguising financing for illicit and terrorist activity.

D. CUSTOMER DUE DILIGENCE

Who is the Applicant for Business?

Company Formation

1. In the case of forming a company, the applicant for business is the ultimate customer upon whose instructions the company is formed. This may or may not be a proposed shareholder. In addition to obtaining identification evidence for the customer, as outlined in Part II, Section 4 of these Guidance Notes, the FSP will normally be required to obtain:

   (1) an explanation of the nature of the proposed company's business,
   (2) the source of funds;
   (3) satisfactory evidence of the identity of each of the proposed beneficial owners; and
   (4) satisfactory evidence of the identity of each of the proposed directors (and in the event of corporate directors, evidence of the identity of the natural persons that will be acting on the corporate directors' behalf). CSPs should understand the ownership and control structure.

2. In some circumstances reliance may be placed on the due diligence of other persons. (Refer to the section on Introduced Business in Part II Section 5 D of the Guidance Notes).

Company Management

3. Where a CSP provides corporate services to a company, the CSP must look behind the company for due diligence purposes and, depending upon the circumstances, investigate and obtain proof of identity of any or all of the following:

   (1) the shareholders (or beneficial owners if different from the registered shareholders);
   (2) the directors and officers;
   (3) anyone who is giving instructions to the CSP on behalf of the company; and
   (4) anyone who introduces any of the above persons to the CSP.

4. Where a CSP provides corporate services to a company, the CSP must understand the ownership and control structure. At the start of the arrangement, the CSP should establish the legal status of any legal persons or arrangements in the structure and monitor the same on an ongoing basis.

Business Introduction

5. However, it is recognized that obtaining due diligence on all of the above in every case could be onerous and could lead to a duplication of procedures, unnecessary complication and eventual loss of legitimate business. The AMLRs and the Guidance Notes therefore, allow for reliance, in certain circumstances, on third party intermediaries. For guidance in this area see

section on Introduced Business in Part II of the Guidance Notes. Where the CSP is approached by a shareholder or beneficial owner, or directors or officers as the applicant for business, the CSP should carry out appropriate due diligence on:

(1) the shareholders and beneficial owners;
(2) the directors and officers; and
(3) anyone who gives instructions to the company manager on behalf of:
    (a) the company;
    (b) the directors and officers of the company; or
    (c) the shareholders and beneficial owners of the company.

6. This must be done in accordance with the requirements pertaining to Corporate Customers outlined in Part II of the Guidance Notes.

7. Where the CSP is approached by a person who gives instructions to the CSP on behalf of the company, the CSP should carry out appropriate due diligence on that person (the applicant for business), the shareholders, and the directors and officers of the company in accordance with the requirements pertaining to Corporate Customers outlined in Part II of the Guidance Notes.

8. However it may, in certain circumstances, be acceptable to rely solely on the due diligence of the person giving those instructions. (Refer to the section on Introduced Business in Part II Section 5 B of the Guidance Notes).

9. Where the CSP relies upon the due diligence of an introducer, such a decision must be made by senior management and the reasons for the decision must be documented. In addition, the CSP must carry out appropriate due diligence on the introducer or intermediary to ensure their eligibility and ensure that written undertakings are received from the introducer or intermediary in accordance with the Guidance Notes.

Structured Finance Companies

10. Where a company is established to undertake one or more structured finance transactions, it may be established by a trustee (the applicant for business) or an Arranger for that transaction or generally. In such cases, the FSP must identify the parties and the commercial purpose and conduct enquiries on any or all of the following persons and entities as appropriate in the circumstances, with a view to ensuring that appropriate due diligence and anti-money laundering compliance is applied to the identity of the investors / note holders and persons that control the flow of the funds, in accordance with the AMLRs and Guidance Notes.

11. Such enquiry may extend to any or all of the following:
(1) the arranger; or
(2) the originator; or
(3) where relevant, the promoter;

(4) investors in the securities of the company; and
(5) other relevant parties.

Private Trust Companies

12. In the case of a private trust company (as defined in the Private Trust Companies Regulations (2013 Revision)), the applicant for business will usually be the settlor(s) of the trusts of which the private trust company will be trustee.

13. In addition to the due diligence required to be obtained in the company formation and company management sections above, it will be necessary to obtain the due diligence recommended in the Trusts Section of these Guidance Notes, save to the extent not already obtained in respect of the private trust company itself.

Discontinued Relationships

14. Funds held to the order of a customer or prospective customer should only be returned to the source from which they came and not to a third party, save for some exceptional instances such as where there is need to comply with a court order in case of controllership.

Ongoing Monitoring

15. In order to be alert for instances of ML/TF, CSPs must continue monitoring the activities of their client companies for signs of unusual or suspicious activities.

16. Activities that warrant special attention include:
(1) changes in transaction type, frequency, unusually large amounts, geographical origins and destinations attributes;

(2) changes in account signatories;

(3) changes in use of the company from the originally stated purpose; and

(4) changes which involve money flows into dormant companies.

17. It is important that monitoring systems be implemented to detect and deter ML/TF activity and such systems should be tested for effectiveness on an ongoing basis.

18. This is an ongoing process which will require periodic refinement to the approach. However, the focus should be to understand changing risks, while maintaining additional implementation of effective ML/TF controls. Additional

effective ML/TF controls should be implemented as appropriate.

Hold Mail and c/o Addresses

19. Sometimes the directors or beneficial owners of client companies request that mail not be forwarded but held at the registered office for storage or later collection. In such cases FSPS should follow the guidance set out in Part II Section 6 B (EDD – Hold Mail Accounts) and extend its application to beneficial owners where necessary.

20. Customers who request "c/o" addresses should also receive additional attention.

21. CSPs should understand and document the customers' rationale for requesting "c/o" and Hold Mail services.

Bearer Shares

22. The Cayman Islands Companies Law does not allow the issue of bearer shares.

23. In circumstances where a CSP provides corporate services to a foreign company that has issued bearer shares, the CSP is directed to:
    (1) maintain proof of identity of all of the following:
        1. the beneficial owners;
        2. the directors and officers;
        3. any person who gives instructions to the CSP on behalf of the company; and

    (2) maintain proof of identity of any custodian of the bearer shares, or person in like capacity, who can at all times verify the identity of the ultimate beneficial owner of the bearer shares.

24. In circumstances where a CSP provides corporate services to a company that is owned by a structure that has vehicles owned through bearer instruments, the CSP must ensure that it can at all times verify the ultimate beneficial owners and natural persons that control the company.

Changes in Service Provider

25. Customers have the right to choose which CSP should manage their affairs and to change to others if they so desire.

26. However, CSPs who are asked by a prospective customer to take over the management of a company which is being managed by another service

provider should communicate with that service provider and make appropriate enquiries as to the reason for the transfer of business.

E. RISK BASED APPROACH

1. CSPs must adopt a risk-based approach to managing ML and TF risks as set out in Part II Section 3 of these Guidance Notes.

2. In identifying and assessing the ML/TF risk to which they are exposed, CSPs should consider a range of factors which may include:
   (1) the nature, scale, diversity and complexity of their business;
   (2) target markets;
   (3) the number of customers already identified as high risk;
   (4) the jurisdictions the CSP is exposed to, either through its own activities or the activities of customers, especially in jurisdictions with relatively higher levels of corruption or organised crime, and those jurisdictions that are not listed on the AMLSG country list;
   (5) the internal audit function and regulatory findings.

F. ML/TF WARNING SIGNS

1. In taking on new business or in monitoring existing business relationships, CSPs should consider that particular structures, customers and activities may pose a higher ML/TF risk. However, just because a factor is listed below, does not automatically make the relationship high-risk provided that suitable controls are in place.

2. Some potentially higher risk services include:
   (1) ownership and management structures that consist of nominee arrangements, where the actual beneficial owner is unclear or undisclosed;
   (2) complex networks of legal persons and/or arrangements (e.g. multiple layers or tiers of intermediate persons or arrangements) where there is no clear rationale for the structure proposed and/ or result in a lack of transparency without an acceptable explanation;
   (3) complex structures that span a number of different jurisdictions, with no clear legitimate rationale;
   (4) Commercial, private, or real property transactions or services with no apparent legitimate business, economic, tax, family governance, or legal reasons;
   (5) trading entities for which CSPs provide management services, particularly where the customer retains some control, or where there is difficulty in monitoring movement of goods, services and financial flows;
   (6) customers who request third-party signatories on bank accounts (including themselves);
   (7) structures and customers that are involved with or connected to higher risk businesses or activities including cash and cash equivalent

businesses such as casinos or money services businesses and businesses or industries that are more prone to higher levels of corruption such as oil, mining, pharmaceuticals or defence (arms);

(8) structures and customers that are involved with or connected to high risk jurisdictions; and

(9) Involvement of PEPs in the structures, including where the PEP may not be the CSP's customer.

SECTION 2

TRUSTS

A. OVERVIEW

1. Corporate trust business carried out in and from the Cayman Islands is regulated pursuant to the Banks and Trust Companies Law (2013 Revision) (BTCL), and the Private Trust Companies Regulations (2013 Revision) (PTCR). The BTCL defines trust business as "the business of acting as trustee, executor or administrator".

2. "Trust business" may be divided into three categories for the purposes of the AMLRs and these Guidance Notes:
   (1) unit trusts which are therefore covered by the Sector Specific Guidance Notes relating to Mutual Funds, in relation to their creation and administration;
   (2) bare trusts or nomineeships where the trustee is acting both as a trustee and as an agent; and
   (3) all other express trusts, including trusts created under the Special Trust – Alternative Regime (STAR), where the trust is not a mutual fund and the trustee is a principal as a matter of law.

B. SCOPE

1. This guidance is intended for all providers of trusts, where the trust is not a mutual fund and the trustee is a principal as a matter of law.

C. ML/TF RISKS

1. The Trust sector is particularly exposed to the risk of being utilised to perpetrate a fraud or a ML scheme, or to facilitate TF.

2. Some of the core risk areas include:

   (1) At the layering and integration stages of money laundering there is greater potential for the misuse of trusts.

   (2) Once the illegal proceeds have already entered the banking system, trusts could be exploited to further confuse the links between these proceeds and the illicit activity that generated them.

D. RISK BASED APPROACH

1. There is no single approach that will detect and prevent all money laundering or terrorist financing.

2. However, a risk-based approach aims to balance the cost burden placed on individual businesses and on their customers with a realistic assessment of the threat of the business being used in connection with money laundering or terrorist financing.

3. FSPs must adopt a risk-based approach to managing ML and TF risks. The risk based approach to AML/CFT aims to support the development of prevention and mitigation measures that are commensurate to the ML/TF risks identified. This applies to the way FSPs allocate their compliance resources, organize their internal controls and internal structures, and implement policies and procedures to deter and detect ML/TF.

4. In identifying and assessing the ML/TF risk to which they are exposed, FSPs should consider a range of factors which may include:

    (1) the nature, scale, diversity and complexity of their business;
    (2) target markets;
    (3) the number of customers already identified as high risk;
    (4) the jurisdictions the FSP is exposed to, either through its own activities or the activities of customers (including: settlors, protectors, beneficiaries), especially in jurisdictions with relatively higher levels of corruption or organised crime, and those jurisdictions that are not listed on the AMLSG country list; and
    (5) the internal audit function and regulatory findings.

5. The FSP's risk-based approach will ensure that its strategies are focused on deterring, detecting and disclosing in the areas of greatest perceived vulnerability.

6. The FSP needs to take a number of steps, documented in a formal policy which assesses the most effectual and proportionate way, to manage ML and TF risks. These steps include:
    (1) identifying the ML and TF risks that are relevant to the FSP;
    (2) assessing the risks, including those presented by the FSP's:
        (a) ownership and Management;
        (b) products;
        (c) delivery channels;
        (d) geographical areas of operation;
    (3) designing and implementing controls to manage and mitigate the assessed risks; and
    (4) monitoring and improving the effective operation of these controls.

E. SYSTEMS, POLICIES AND PROCEDURES

Who is a Customer/Applicant for Business?

Settlor

1. Where a new trust is being created, the Applicant for Business will be the settlor (or all of the settlors if more than one).

Settled Assets

2. FSPs should also make appropriate inquiry as to the source of the assets a settlor intends to settle.

3. Assets settled, and their source, will necessarily vary from case to case and depend on many factors, such as the type of trust intended to be created, the relative and absolute value of the assets intended to be settled, the objectives of the settlor in creating the trust and the timeframe within which the parties are working.

Transfer of an Existing Trust

4. Where an FSP is approached to become an additional or successor trustee, it is recognised that the concept of an "Applicant for Business" can be another trustee.

Customer Due Diligence

Ongoing Obligations

5. FSPs must recognise the need to adopt ongoing procedures for vetting any settlors to a trust and the source of the funds that are introduced to the trust. In particular, each time assets are added to the trust by a new or existing settlor the same procedures should be followed.

Trust Companies and Private Trust Companies

6. In the case of a private trust company PTCRs, consider whether some or all of the due diligence recommended to be obtained in accordance with the Company Formation and Management Section of these Guidance Notes should be obtained, save to the extent not already obtained in respect of the settlor(s).

7. A trust company acting as trustee of a trust should collect due diligence documentation on:
   (1) the settlor (including any person subsequently settling funds into the trust) and any person who directly or indirectly provides trust property or makes a testamentary disposition on trust or to the trust;
   (2) any co-trustee;
   (3) any protector;
   (4) any enforcer (in respect of trusts created under STAR);
   (5) any named beneficiary with a vested right;

(6) any other beneficiary with a vested right; and
(7) any other person exercising ultimate effective control over the trust.

Previous Due Diligence

8. Trustees act as a body. Additional or successor trustees "step into the shoes" of the existing or predecessor trustees.

9. An FSP who is an additional or successor trustee should inquire of the existing or predecessor trustees whether appropriate inquiries were made of the settlor or settlors at the time of creating the trust and at the time of addition of any assets to the trust, and seek to obtain the originals or copies of the relevant due diligence documentation (e.g. verification of the settlor's identity and source of funds). Having done so, the FSP should consider whether it is adequate, according to the circumstances of the particular case.

10. However, in some cases, such documentation may not be available or upon review may not be adequate. In such cases the FSP should make reasonable inquiries of its own:

(1) Where the Settlor is Alive: Where the settlor is still alive, the FSP should make the relevant inquiries of the settlor.

(2) Where the Settlor is dead: Where the settlor is dead, the FSP should make reasonable inquiries about the settlor of such persons as may be appropriate in the circumstances of the particular case e.g. the existing or predecessor trustees or the beneficiaries. In particular, if the beneficiaries are relatives of the deceased settlor, as will often be the case, appropriate inquiry of the oldest beneficiaries may be the most fruitful.

Simplified/Enhanced Due Diligence

Simplified Due Diligence

11. Section 21 of the AMLRs states that, "a person carrying out relevant financial business may apply simplified customer due diligence measures where lower risks have been identified, and the simplified customer due diligence shall be commensurate with the lower risk factors".

12. The simplified measures shall be commensurate with the lower risk factors but are not acceptable whenever there is suspicion of money laundering or terrorist financing, or higher risk scenarios apply.

Enhanced Due Diligence

13. Risk factors that may indicate high risk, and should therefore be carefully assessed to determine if there is indeed high risk and need for EDD include circumstances where:
    (1) a customer is resident in another country or territory;
    (2) a customer is not physically present for identification purposed; or
    (3) a customer is a company with nominee shareholders.

F. ML/TF WARNING SIGNS

1. FSPs are urged to be particularly vigilant in the following areas:

    (1) Links with high risk and non-cooperative jurisdictions.

    (2) Certain countries are associated with crimes such as drug trafficking, fraud and corruption and consequently pose a higher potential risk to FSPs. Conducting a business relationship with such a country exposes the FSP to reputational risk and legal risk.

2. FSPs are advised to consult publicly available information to ensure that they are aware of those countries/territories described in 1(1) above. A source of relevant information for FSPs is the FATF website at www.fatf-gafi.org. Other useful websites include: the Financial Crimes Enforcement Network (FinCEN) at www.ustreas.gov/fincen/ for country advisories; the Office of Foreign Assets Control (OFAC) www.treas.gov/ofac for information pertaining to US foreign policy and national security; and Transparency International, www.transparency.org for information on countries vulnerable to corruption.

3. FSPs should exercise additional caution and conduct enhanced due diligence on individuals and/or entities based in high-risk countries. Caution should also be exercised in respect of the acceptance of certified documentation from individuals/entities based in high-risk countries/territories and appropriate verification checks undertaken on such individuals/entities to ensure their legitimacy and reliability.

Total Changes of Beneficiaries

4. Where all of the existing beneficiaries are removed and different beneficiaries are added, or where this is intended, or where the trust is intentionally structured to permit this, heightened scrutiny is required by the FSP. The FSP should ensure that it documents a clear rationale for changes to the originally stated beneficiaries or classes of beneficiaries.

5. There may be perfectly legitimate reasons for this occurring or for this to be possible, but FSPs should endeavour to ascertain what these are.

Unexplained Requests for Anonymity

6. Where the settlor's stated reason for establishing a trust is the need for anonymity or confidentiality in relation to himself or the beneficiaries, the FSP should ensure that it is clear on the legitimacy of settlor's purposes and rationale prior to taking on such business.

7. It should not be automatically inferred that this in itself is an illegitimate need. There are many instances where a settlor may desire that the extent or nature of his wealth is not known to third parties – such as children, the media, business or industry colleagues, potential kidnappers, industry competitors etc. The legitimate need for privacy is acknowledged and supported in the Cayman Islands as in other countries and may be a reason for establishing a trust.

8. However, FSPs are encouraged to adopt a conservative and cautious approach in this area. In particular, where the reasons given by the settlor for the need for anonymity or confidentiality are not clear or are unconvincing, FSPs should take appropriate further action.

Beneficiaries with no apparent connection to the settlor

9. Another red flag or warning sign is where there is no readily apparent connection or relationship of the settlor to the beneficiaries.

10. Since the economic nature of a trust is a mechanism for the settlor to benefit a beneficiary, typically not in return for any consideration (payment, transfer of assets or provision of services), FSPs should endeavour so far as possible to ascertain the settlor's reasons for wanting to benefit a beneficiary with whom he seemingly has no connection.

11. This can be a matter of great sensitivity (for example, where the beneficiary turns out to be an illegitimate child of the settlor) and FSPs are encouraged to take this into account while pursuing necessary or appropriate inquiries.

Unexplained Urgency

12. FSPs are encouraged to inquire as to the reasons for any urgency, especially where the settlor is indicating that some of the due diligence process can or will be completed after the trust has been established or a transaction has been entered into by the trustees or an underlying company owned by the trust.

Potentate Risk

13. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose FSPs to

significant reputational and/or legal risk. The risk occurs when such persons abuse their public powers for either their own personal benefit and/or the benefit of others through illegal activities such as the receipt of bribes or fraud. Such persons commonly referred to as 'politically exposed persons' (PEPs) or 'potentates' include heads of state, ministers, influential public officials, judges and military commanders.

14. Provision of financial services to corrupt PEPs exposes FSPs to reputational risk and costly information requests and seizure orders from law enforcement or judicial authorities. In addition, public confidence in the ethical standards of a whole financial system can be undermined.

15. FSPs are encouraged to be vigilant in relation to PEPs from all jurisdictions; in particular High Risk Countries who are seeking to establish business relationships. FSPs should, in relation to politically exposed persons, in addition to performing normal due diligence measures:
    (1) have appropriate risk management systems to determine whether the customer is a politically exposed person;
    (2) obtain senior management approval for establishing business relationships with such customers;
    (3) take reasonable measures to establish the source of wealth and source of funds; and
    (4) conduct enhanced ongoing monitoring of the business relationship.

16. FSPs should obtain senior management approval to continue a business relationship once a customer or beneficial owner is found to be, or subsequently becomes a PEP.

17. See Section 7 of Part II of these Guidance Notes – Politically Exposed Persons.

Private Trust Companies (PTCs)

18. In the case of FSPs that provide registered office services to PTCs, when a PTC is the applicant for business, including in respect of registered office services, the applicant for business will usually be the settlor(s) of the trusts of which the private trust company will be trustee.

19. The due diligence recommended for registered office service providers to PTCs is the same as recommended in the Company Formation and Company Management Sections of these Guidance Notes.

20. PTCs must have in place controls to comply with the ML/TF framework in the jurisdiction.

21. In the case that a PTC is managed by an FSP, the FSP must ensure that its ML/TF controls extend to the services that it provides to the PTC, including training and record retention controls.

Trusts established under STAR

22. Where any of the objects of a trust is a purpose, whether or not Charitable, FSPs are encouraged to understand the rationale for establishing the trust. In such circumstances additional attention should be paid to the parties to the trust and the source of any funds settled in the trust.

23. In cases where any of the objects of a trust is a charity, FSPs should make best effort to determine the legitimate nature of the charity and make best efforts to satisfy themselves that the beneficiary charity is not being utilized to facilitate ML/TF activity. FSPs should document the results of any research or investigation of the legitimacy and goals of the charity in such situations.

Other warning signs

24. Additional warning signs to which FSPs should be particularly alert include the following:

(1) situations where there is no clear rationale for the structure proposed and/ or result in a lack of transparency without an acceptable explanation or where it is inordinately difficult to identify (where relevant) the beneficiaries;

(2) complex structures that span a number of different jurisdictions, with no clear rationale;

(3) structures involving legal persons and legal arrangements that involve high value goods and/or transactions;

(4) structures or customers that are involved with or connected to higher risk jurisdictions;

(5) structures that involve trust assets that originate or reside in higher risk jurisdictions;

(6) involvement of PEPs in the structures, including where the PEP may not be the CSP's customer/client;

(7) customers that invest or settle using cash or request cash distributions;

(8) customers that insist on retaining control of the trust assets;

(9) In the case of express trusts, an unexplained relationship between a settlor and beneficiaries with a vested right, other beneficiaries and persons who are the object of a power;

(10) an unexplained nature of classes of beneficiaries and classes within an expression of wishes.

(11) customers who request third party signatories on bank accounts (including themselves);

(12) beneficial owners who wish to retain control over assets through powers delegated; customer does not cooperate with FSP's requests for information;

(13) customers who are introduced by an overseas source based in a country noted for drug production or distribution or a customer

introduced by an overseas branch, affiliate in a country not on the AMLSG List;

(14) customers who are introduced by or engaged as a service providers by other TCSPs, financial institutions, and other designated non-professional businesses and professions who are not subject to adequate AML/CFT laws and measures and who are not adequately supervised

(15) customers who transfer funds or shares to accounts in a country other than those that are on the AMLSG List; or

(16) any transaction involving an undisclosed party.

GUIDANCE NOTES ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING AND TERRORIST FINANCING IN THE CAYMAN ISLANDS

PART V

SECTOR SPECIFIC GUIDANCE: INSURANCE SECTOR

The purpose of this part of the Guidance Notes is to provide some guidance specifically for the Insurance sector. This Insurance sector specific guidance (Part V) covers Insurance Business and, in Part V Section 2, additional guidance for Insurance Managers and should be read in conjunction with Part I and Part II of the Guidance Notes.

SECTION 1

INSURANCE BUSINESS

A. OVERVIEW

1. The insurance market of the Cayman Islands is composed of two broad segments: the foreign market, which comprises of captive insurance companies that insure non-domestic risks (Class "B" licence) and of fully collateralised insurance linked securities structures (Class "C" license), and the domestic market (Class "A" licence), where insurers, directly or through intermediaries, sell insurance to Cayman Islands residents and business organisations. In addition, reinsurers (Class "D" license) offer reinsurance products for domestic or foreign risks.

2. While domestic insurers generally have staff or agents in the Cayman Islands, this is not always the case for captive insurance companies, which can be self-managed or managed by an insurance manager. The Insurance Law, 2010, requires Class B and C insurers to either have a physical presence or appoint an insurance manager. Insurance managers are licensed and supervised by CIMA both for prudential and AML/CFT purposes, and the insurance managers manage the day to day activities of the insurer and provide it with insurance expertise. The insurance companies within the domestic market offer their products directly as well as through intermediaries, namely insurance brokers and insurance agents.

3. The Class "B" licence is sub-divided into three categories. Class "B(i)" which includes insurers with at least 95% of the written net premiums originating from the insurer's related business. Class "B(ii)" is for insurers with over 50% of the net premiums written originating from the insurer's related business, and Class "B(iii)" includes insurers with 50% or less of the written net premiums originating from the insurer's related business.

B. SCOPE

1. The AMLRs are mainly applicable to insurance business as specified in its Schedule, which includes life and annuity business, and all of which are described as long term insurance. Whilst the AMLRs do not apply directly to general insurers, from a sound risk management and internal controls perspective, such insurers are still expected to have policies and procedures in place to prevent ML/TF, in accordance with these Guidance Notes.

2. Section 4 of the AMLRs states that the AMLCO shall ensure that measures set out in the AMLRs are adopted by companies carrying out relevant financial business. For insurance business, this means companies involved in long-term business as defined within the Insurance Law (2010) (i.e. insurers, insurance managers, insurance agents, and insurance brokers). The AMLRs will therefore

apply directly to insurance managers, insurance agents or insurance brokers in relation to long-term business. However, managers, agents and brokers are still expected to have policies and procedures in place to prevent ML/TF in respect of any general insurance business they are involved in.

3. This sector specific guidance seeks to provide practical assistance to all insurers and insurance intermediaries in complying with the AMLRs, interpreting and applying the general provisions of these Guidance Notes and to adopt sound risk management and internal controls for their operations.

4. The principal obligation to perform AML/CFT procedures under the AMLRs falls on each FSP in respect of the parties with which it directly transacts, that is to say its own applicants/customers. For example, in the case of an insurance manager, its applicants will largely be insurance companies, which themselves, as licensees also, will have their own independent obligations to perform AML/CFT checks as appropriate on policyholders and beneficiaries, or others with whom they conduct relevant financial business.

5. As a practical matter, however, many insurers, particularly those without their own dedicated staff, may often delegate the operation of AML/CFT procedures to insurance managers. However, each FSP retains ultimate responsibility for ensuring that appropriate steps are taken in respect of its own applicants/customers. Where an insurer is un-staffed, section 9 of part II of the Guidance Notes as to the MLRO/AMLCO will still be applicable. In the absence of the MLRO, the Deputy MLRO shall discharge the MLRO functions.

C. ML/TF RISKS:

1. As an international financial centre, the Cayman Islands face greater external, rather than internal, ML/TF threats. Theft, corruption and drug trafficking are the main threats emanating from domestic origins. Fraud, the evasion by foreigners of taxes overseas, and drug trafficking in other jurisdictions, present potential threats to the Cayman Islands from foreign origins.

2. The ability to use the insurance sector for ML/TF is generally regarded as lower than that of other sectors such as banking, and securities, which present better opportunities for criminals to quickly deposit and withdraw funds.

3. Regardless, there is some ML/TF risk within the international insurance sector. As with many other financial vehicles, captive insurance companies may be misused for ML/TF purposes. As such, FSPs (such as ILs structures) must be vigilant to prevent criminals from using them for ML/TF purposes. Some of the risks can be mitigated by ensuring the source of funds and identity of investors is understood and appropriate due diligence is performed accordingly.

4. Generally, international insurers operating as commercial insurance companies, especially those engaged in long-term insurance business or annuity products, as well as domestic insurers engaged in long-term insurance business and annuity products, may present a higher ML/TF risk compared to other insurers. Insurance fraud, including staged motor vehicle accidents, has been known to be used as a means of raising funds for terrorist organizations.

5. Even international insurers covering their own risk/related risks, (i.e. pure captives) still have ML/TF risks and captive owners and insurance managers need to be aware and mitigate such risks. Insurance managers managing captives need to ensure they understand the rationale for the set-up of the captive and monitor any potential ML/TF risks, especially as it relates to money flows, including inter-company loans.

D. RISK BASED APPROACH

1. Companies conducting insurance business must apply a risk-based approach to mitigate the risk that their company will be used for ML/TF. The risk-based approach requires an FSP to take steps to identify the risks relating to:

   (1) its type of customers, such as retail or corporate, and new or existing customer;
   (2) the country or geographic area in which its customers reside or originate: for example, is it a country that has robust ML/TF regulations or not;
   (3) the products, services and transactions of the company: for example, does the product have a cash-in value and can it easily be used for ML/TF purposes;
   (4) the delivery channels used by the company: for example, does the company distribute its own products or does it use other intermediaries and are these intermediaries licensed by a reputable regulator or not.

2. Section 3 of Part 2 of these Guidance Notes explains how FSPs should operationalize the risk based approach. Section E below provides specific guidance for insurers and intermediaries about risk factors applicable to the business of insurance.

E. NATURE OF PRODUCTS UNDERWRITTEN/SOLD

1. The risk-based approach should lead the FSP to consider the inherent risk within the nature of the product being underwritten/sold**,** the amounts involved, the ability to surrender the product for a cash value, the ability to add riders to the policy, amongst other things. A few examples of these risks are provided in this section.

GENERAL (NON-LIFE)

(1) In relation to insurance business, significant factors that will affect the level of risk of any transaction or business relationship include:

(a) the mode/method of payment of the premium (e.g. cash, credit card, bank transfer etc.);

(b) the nature product to be underwritten or sold e.g. does it have a cash-in value or surrender value and can loans be taken against the policy;

(c) the amount of premium (e.g. higher premium policies could be more attractive to ML/TF).

(2) A significant factor determining the level of ML/TF risk in any product is the level of premium payable on the policy and method of payment. For example, a motor policy with an annual premium of $1000 will present a much lower risk than one on a luxury car or car fleet in the case of a commercial motor policy, which commands a much higher premium and value at risk.

(3) Premium payments made in cash present a higher risk than payments made via a bank account. For example, premiums for property and casualty policies in the case of condominium developments may be significant and insurers should be especially vigilant when requests are made for large premiums to be paid in cash. Electronic/card or cheque payments may present a lower risk than cash, especially where large premium payments are involved, but both domestic and international insurers must be aware of the inherent risks that might emanate from electronic/card payments, such as fraud, and put appropriate controls in place.

(4) In addition to vigilance about the means of payment, sound claims management is essential as ML/TF can occur through inflated or bogus claims, e.g. by arson or other means causing a fraudulent claim to be made.

Features of High Risk and Low Risk General Insurance Products with examples:

(5) Some of the features of high risk and low risk **general insurance** products are listed below:

Low risk	Low premiums, inability to make claims without substantial reliable evidence of loss. Note that products rated as low AML/CFT risk may also be rated a low fraud risk, but not always.
Example of low risk	A single, individual travel policy may be considered low risk simply because the premium is low and the term date is short. Other travel policies, however, for example, annual or group, may be considered to pose a relatively increased risk and thus controls should be applied appropriately.
High risk	High premium amounts and the ability to pay in cash, to overpay premiums, and to cancel the policy to seek a premium refund. Also the greater risk of fraud will generally mean a greater risk of AML/CFT.
Example of high risk	May include Cash-In-Transit policies or Fidelity Guarantees where the likelihood of manipulation and conspiracy is greater.

LONG TERM (LIFE)

Features of high risk and low risk

Long term (life) insurance products with examples:

(6) Significant factors that will affect the level of risk of any transaction or business relationship for long-term policies include:

(a) The nature of the product to be underwritten or sold; e.g. does it have a cash-in value or surrender value and can loans be taken against the policy.

(b) The mode/method of payment of the premium; e.g. cash, credit card bank transfer etc.

(c) The manner of transaction; e.g. face-to-face, online etc. FSPs must apply a risk-based approach and consider any additional risks that might apply to digital transactions.

(d) The amount of premium e.g. higher premium policies could be more attractive to ML/TF.

(7) Some of the features of low risk and high risk **life and long-term insurance** products are listed below:

Low	1. Life insurance policies where the total premium payable annually is no more than CI$800, or a single premium of no more than CI$2000.
	2. Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral
	3. A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.
High	1. Unit-linked or with profit single premium contracts
	2. Single premium life insurance policies that store cash value
	3. Fixed and variable annuities
	4. (Second hand) endowment policies[63].

F. SYSTEMS, POLICIES AND PROCEDURES

1. Companies conducting insurance business must establish and fully implement robust systems, policies and procedures to forestall their products and services from being used for ML/TF.

2. This will include, amongst other things, conducting risk assessments, identifying who is a customer/applicant; customer due diligence; simplified/enhanced due diligence; internal controls, ongoing monitoring, record keeping and reporting.

G. APPLICANTS - ESTABLISHING A BUSINESS RELATIONSHIP

1. Before an insurance contract is concluded between an applicant/customer and insurer there is already a pre-contractual business relationship between the customer and the person selling the policy, be that the insurer or an intermediary.

2. After a policy is taken out:
   (1) the insurer covers a certain risk described in the contract and policy conditions;

[63] Secondhand endowment policies are also known as traded endowment policies (TEPs). Endowment policies are investment funds made up of savings, bonds, and shares. An individual wanting to cash in an endowment policy has two choices: to surrender it back to the life insurance company, generally for a poor return, or to sell it on the second-hand market, often at a much better price.

(2) certain transactions may take place such as premium payments, payments of advance or final benefits; and

(3) certain events may occur such as a change in cover or a change of beneficiaries.

3. The insurer will need to carefully assess the specific background, and other conditions and needs of the customer. This assessment is already being carried out for commercial purposes (determining the risk exposure of the insurer and setting an adequate premium) as well as for reasons of active client management. This will lead to a customer profile, which could serve as a reference to establish the purpose of the contract and to monitor subsequent transactions and events.

4. The insurer should realise that creating a customer profile is also of importance for AML/CFT purposes and therefore for the protection of the integrity of the insurer and its business. Generally, it will be appropriate to obtain information as outlined below, but other circumstances may require alternative information.

H. INSURANCE SPECIFIC INFORMATION THAT MAY BE REQUESTED TO SUPPLEMENT AS NECESSARY THAT OUTLINED IN PART II OF THESE GUIDANCE NOTES

1. The following are some of the insurance specific information that may be requested to supplement the other information required under the section "CDD" of Part II of the Guidance Notes.

Applicant for business (proposer)	Insurance specific information
Personal	1. That the person is the proposer and has an insurable interest in the risk to be insured 2. The property or other risk to be insured and its valuation. 3. Any other beneficiaries with insurable interests and/or claims on the policy. 4. The source of funds for the payment of the premium.
Corporate	1. That the person proposing represents and is authorised to represent the company, which has an insurable interests in the risk to be insured 2. The property or other risk to be insured, and its valuation. 3. Any other beneficiaries with insurable

	interests and/or claims on the policy. 4. Source of funds for the payment of the premium.

When must identity be verified?

2. In principle, identification and verification of customers and beneficial owners should normally take place when the business relationship is established. This means that the policyholder (or its owner / controller) needs to be identified and their identity verified before, or at the very latest at the moment when, the insurance contact is concluded.

3. That said, identification and verification of the beneficiary may take place after the insurance contract has been concluded with the policyholder, provided the ML/TF risks are not significantly high and are effectively managed. One example could be an insurer providing a customer with immediate temporary motor insurance. However, that might be subject to the customer providing evidence of proof of his/her address within an agreed timeline. Another example is where an insurance contract permits an applicant to delay naming a beneficiary, or permits changes to beneficiaries during the life of the insurance policy, the identity of the beneficiary may be obtained as soon as the beneficiary is identified or designated and no later than at the time of the pay-out.

4. However, subject to (6) below, where the verification information is not forthcoming at the outset or within a reasonable time after initial contact the proposed business relationship must be re-evaluated and transactions must not proceed.

5. Where the ML/TF risks are assessed as standard or lower than standard, and appropriate risk-mitigation measures are applied, verification of a beneficiary's identity may take place:

   (1) At or before the time of any payout or premium refund;

   (2) At or before the time the beneficiary exercises any vested right under the policy.

Simplified/Enhanced due diligence

6. An FSP may apply simplified customer due diligence measures where lower risks have been identified, through an adequate analysis of risks by the country or the FSP itself. The simplified measures Customer Due Diligence (CDD) shall be commensurate with the lower risk factors, but are not

acceptable whenever there is suspicion of ML or TF, or higher risk scenarios apply. CDD is required on all life policies. FSPs must take due care and ensure that CDD is also carried out on life insurance beneficiaries. As outlined in the 'Systems, Policies and Procedures section' above, CDD and EDD must be ongoing and not just at the time a policy is placed on risk.

7. It is recommended that EDD be applied for high risk situations and in situations where the insurer is particularly exposed to reputational risk. There will be certain occasions where enhanced due diligence will be required, for example:

(1) when there is no face-to-face contact with the insurer;
(2) where the customer is a PEP;
(3) where the beneficiary of a policy can be transferred; and
(4) when the customer is involved in a business that is considered to present a high risk for ML/TF.

8. With respect to EDD, in addition to those listed in Part II of the Guidance Notes, the following additional information might be requested in relation to the proposed transaction, business or source of funds:

(1) In insurance, various transactions or 'trigger events' occur after the contract date and indicate where due diligence may be required. These trigger events include claims notification, surrender requests and policy alterations, including changes in beneficiaries.
(2) The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors.

(3) In this respect "transactions" should be interpreted in a broad sense, meaning inquiries and applications for an insurance policy, requests for changes in cover, redemption, cancellation, claim submission premium payments, requests for changes in benefits, beneficiaries, duration, etc.

How should the business of the customer be monitored?

9. In general, the FSP should pay attention to all requested changes to the policy and/or exercise of rights under the terms of the contract.

10. It should assess if the change/transaction does not fit the profile of the customer and/or beneficial owner or is for some other reason unusual or suspicious.

I. ML/TF WARNING SIGNS

What warning signs or "red flags" should FSPs (i.e., insurance entities covered under this section) be alert to?

1. The following are some of the warning signs or "red flags" to which FSPs should be alert. The list is not exhaustive, but includes the following:

    (1) Requests for a return of premium to be remitted to persons other than the policy holder.
    (2) Claims payments paid to persons other than policyholders and beneficiaries.
    (3) Unusually complex holding company or trust ownership structure.
    (4) Making a false claim.
    (5) A change in beneficiaries (for instance, to include non-family members).
    (6) A change/increase of the premium payment (for instance, which appear unusual in the light of the policyholder's income or where there are several overpayments of policy premiums after which the policyholder requests that reimbursement is paid to a third party).
    (7) Use of cash and/or payment of large single premiums.
    (8) Payment/surrender by a wire transfer from/to foreign parties.
    (9) Payment by banking instruments that allow anonymity of the transaction.
    (10) Change of address and/or place of residence of the policyholder.
    (11) Lump sum top-ups to an existing life insurance contract.
    (12) Lump sum contributions to personal pension contracts.
    (13) Requests for prepayment of benefits.
    (14) Use of the policy as collateral/security (for instance, unusual use of the policy as collateral unless it is clear that it is required for financing of a mortgage by a reputable financial institution).
    (15) Change of the type of benefit (for instance, change of type of payment from an annuity to a lump sum payment).
    (16) Early surrender of the policy or change of the duration (particularly where this results in penalties).
    (17) Requests for multiple policies to be taken out for premiums slightly below any publicised limits for performing checks, such as checks on the source of wealth or cash payments.

2. As the above list is not exhaustive, insurers should consider other types of transactions or trigger events, which are appropriate to their type of business.

J. RECORD KEEPING

1. FSPs must ensure that their record-keeping procedures are maintained in accordance with Part VIII of the AMLRs.

2. All records, including discharge documents must be "readily accessible" and available without delay upon request by competent authorities.

SECTION 2

INSURANCE MANAGERS

A. NATURE OF THE PRODUCTS UNDERWRITTEN/SOLD

1. ML/TF can occur either by establishing fictitious (re)insurance companies or reinsurance intermediaries, and fronting arrangements, or by the misuse of normal reinsurance transactions.

2. Examples include:
   (1) the deliberate placement via the insurer of the proceeds of crime or terrorist funds with reinsurers in order to disguise the source of funds;

   (2) the establishment of bogus reinsurers, which may be used to launder the proceeds of crime or to facilitate terrorist funding; and

   (3) the establishment of bogus insurers, which may be used to place the proceeds of crime or terrorist funds with legitimate reinsurers.

3. For Class B insurers the line of business or risk assumed is much less relevant to the assessment of AML/CFT risk, than the persons or applicants involved. This is because even the typically lowest risk product could potentially be used for ML. For example, workers compensation schemes may be established for fictitious personnel or be funding mechanisms for terrorists awaiting assignment.

4. One factor that should help to mitigate this risk is the involvement of independent third parties e.g. medical practitioners, claims adjusters and government agencies to substantiate claims. In the international market the scope for lines of business in insurers is unlimited.

5. The focus for FSPs entering into relationships with Class B insurers should be the operators and owners of the insurer, the business rationale for the insurer, its relationships and source of funding.

B. APPLICANTS

6. The applicant for business may be either an existing insurer, possibly already under management and regulated, or it may be a company or group of individuals seeking to establish a new insurer.

7. The following guidance regarding due diligence and documentation to be obtained falls outside and is separate from that which the manager may necessarily obtain in preparing a licence application for an insurer or insurer to be formed as per the Insurance Law and Regulations thereunder.

C. EXISTING INSURER TO BE MANAGED

1. It is recognized that where insurers already formed and licensed are transferred to an Insurance Manager, although the insurer, as an applicant, may be regarded as an acceptable applicant for the purpose of verification requirements as per section 22 of the AMLR, the nature of the relationship between the manager and the insurer may require that additional commercial due diligence is obtained and maintained in order to discharge its obligations as manager and for on-going monitoring. See in particular Sections 27 – 29 of the AMLR.

How should the business of the customer be monitored?

2. All changes to the nature of the business of the Class B insurer should be assessed and a decision made whether such constitutes a trigger requiring further verification or investigation/information.

3. At a minimum the Annual Statement of Operations filed with the Monetary Authority provides a periodic opportunity to review the relationship and the business of the customer, or upon renewal of the service agreement.

D. ML/TF WARNING SIGNS

What warning signs or "red flags" should Insurance Managers be alert to?

1. The following are some of the warning signs or "red flags" to which service providers should be alert. The list is not exhaustive, but includes the following:

   (1) Requests for a premium refund to be remitted to persons other than the policy holder.
   (2) Dividends paid to persons other than shareholders.
   (3) Unusually complex holding company or trust ownership structure.
   (4) Concealment of identity of the customer or the beneficial owner; or of the ownership of funds.
   (5) Incomplete application details and lack of willingness to provide evidence to answers required.
   (6) Unexplained changes in investment pattern; investment taken against advice or not appropriate to insurer's real needs;
   (7) Sudden changes in intermediary transaction pattern;
   (8) Unexplained receipt of bulk premiums from intermediary accounts.
   (9) Third party transactions (payments or withdrawals);

(10) Multiple sources of payment or cross jurisdiction funding for payment;
(11) Payment of premiums from early surrender of another investment in unusual circumstances;
(12) Payment from obscure or unregulated organisations;
(13) Unnecessarily complex transactions or intentions;
(14) Requests for part investment and return of surplus funds;
(15) Immediate interest in surrender penalties or requests for large withdrawals or policy loans;
(16) Early surrender of a contract;
(17) Receipt of unexplained wire transfers and requests to return wire transfers;
(18) Requests for no correspondence to go to customer.

E. RECORD KEEPING

What specific AML/CFT records should be kept and where?

1. See Sections 31 and 32 of the AMLRs and, in addition, all documentation listed above together with initial and subsequent information necessary for on-going monitoring should be held, whether as duplicate or back up by the Manager at its office in Cayman.

F. OTHER RELEVANT SECTORS

1. Catastrophe bonds and other Insurance Linked Securities (ILS) may be a source for ML/TF due to the large amount of money that is invested into them. FSPs need to apply a risk-based approach to ensure they understand who the customer/investors are; the source of funds; the jurisdictions of the customer/investors; the beneficial owners of the policy, where a trust structure might be in place; and means of payments such as cash and bank transfers.

PART VI

SECTOR SPECIFIC GUIDANCE: MUTUAL FUNDS AND MUTUAL FUNDS ADMINISTRATORS

The purpose of Part VI of the Guidance Notes is to deal with AML / CFT matters pertaining to Mutual Funds ("MFs") and Mutual Fund Administrators ("MFAs") that require more explanation or are more complex issues than are dealt with in the general body of these Guidance Notes. This section must be read in conjunction with Part I and Part II of the Guidance Notes and the Appendices. MFs and MFAs may also find Part VIII of these Guidance Notes to be of some relevance.

SECTION 1
MUTUAL FUNDS AND MUTUAL FUND ADMINISTRATORS

A. OVERVIEW

1. The Mutual Funds Law (2015 Revision) (the "MFL") gives the Authority responsibility for regulating certain categories of Mutual Funds (defined below) operating in and from the Cayman Islands, as well as Mutual Fund Administrators (defined below).

2. The Authority regulates Mutual Funds and Mutual Fund Administrators in accordance with:

   (1) the laws and regulations applicable to all regulated entities and those specifically governing this sector, namely, the MFL; the Mutual Funds (Annual Returns) Regulations; the Retail Mutual Funds (Japan) Regulations; and the Mutual Fund Administrators Licence (Applications) Regulations;

   (2) the relevant rules, guidance, policies and procedures issued by the Authority from time to time; and

   (3) relevant international standards set by international bodies such as, but not limited to, the International Organization of Securities Commissions ("IOSCO") and the Offshore Group of Collective Investment Scheme Supervisors ("OGCISS").

3. The definition of a Mutual fund, as established in the MFL, can be summarised as follows: any company, trust or partnership either incorporated or established in the Cayman Islands, or if outside the Cayman Islands, managed from the Cayman Islands, which issues equity interests redeemable or purchasable at the option of the investor, the purpose of which is the pooling of investors' funds with the aim of spreading investment risk and enabling investors to receive profits or gains from investments.

4. Note that funds commonly referred to as hedge funds fall within the definition of a Mutual Fund and are thus covered by the MFL.

5. The Cayman Islands has company, trust, partnership and related laws that allow a high degree of flexibility for establishing Mutual Funds. The four vehicles commonly used for operating Mutual Funds are the exempted company, the segregated portfolio company, the unit trust and the exempted limited partnership.

6. A Mutual Fund Administrator is a person who conducts mutual fund administration as defined in the MFL; that is: a person managing (including controlling all or substantially all of its assets) or administering a Mutual Fund; a person providing the principal office of a Mutual Fund in the Cayman Islands; or providing an operator to the Mutual Fund as defined in section 2 of

the MFL (a trustee of a unit trust, a general partner of a partnership or a director of a company).

B. SCOPE

1. The sector specific guidance contained in this section is applicable to regulated Mutual Funds and Mutual Fund Administrators, separated accordingly where applicable.

C. MONEY LAUNDERING AND TERRORIST FINANCING RISKS

1. As is the case with most financial products, Mutual Funds carry a certain degree of ML/TF risks.

2. Listed below are some, but not all, of these relevant risks.

   (1) **Country Risk** – having investors located in multiple international locations can increase the risk of money laundering and terrorist financing. Mutual Funds and Mutual Fund Administrators should be especially careful when dealing with investors who are politically exposed persons ("PEPs") of a foreign jurisdiction or those from a country on a sanctions list.

   (2) **Investor Profile** – in addition to the country of domicile of investors, the types of individuals/entities that make up the investor base can also increase the risk of money laundering and terrorist financing. All things equal, institutional investors from large financial institutions that are regulated and/or listed on a stock exchange could be considered less risky than investors in the form of trusts, charities or high net worth individuals for example.

   (3) **Source of Funds** – Mutual Funds with lower minimum investment thresholds pose a greater risk of money laundering, especially if those funds are not coming from a regulated financial institution. Mutual Fund Administrators and Operators must remain cognizant of, and have controls in place surrounding, subscription and redemption activity in Mutual Funds, in the same way bankers must do so for bank account deposits and withdrawals.

   (4) **Redemption Terms** – persons attempting to partake in money laundering need the ability to move funds out of the Mutual Fund in order to effectively layer transactions. Some Mutual Funds have liquidity structures with limited or no lock-up periods and/or redemption restrictions.

D. RISK-BASED APPROACH (refer also to Section 3 of Part II)

1. Low and high risk indicators including the ML/TF risks outlined in section C above and the ML/TF warning signs outlined in section I below should be considered when the Mutual Fund and/or Mutual Fund Administrator is conducting risk assessments.

2. FSPs should be aware of, and take into account, additional risk factors or risk variables that may be introduced where services, functions or activities of the FSP itself or the FSPs customers are outsourced or delegated, particularly so if the service provider is not subject to adequate AML/CFT laws and measures and / or is not adequately supervised.

3. One risk factor set out in Part II Section 3 that is of particular relevance (to mutual funds and (perhaps to a lesser degree) fund administrators is the non-face-to-face basis for subscriptions, redemptions and transfers. While the presence of a high-risk factor does not necessarily make the customer high risk, FSPs should consider this factor along with all the other relevant risk factors and mitigants, and undertake appropriate CDD measures. A possible mitigating measure, which in turn requires robust systems and controls, is the use of reputable and regulated Eligible Introducers.

4. Other risk factors or risk variables to consider may include:

   (1) A history of frequent and / or unexplained changes in service providers; and
   (2) A customer, or principals of a customer, that is or has been the subject of criminal / civil or regulatory proceedings for crime, corruption, misuse of public funds or known to associate with such persons

5. Risk Assessments should take place as a customer or investor is on-boarded and be reviewed and changed if necessary during periodic reviews of the customers and investors as discussed in the Ongoing Monitoring section below. The methodology used by the entity to assess the risk should be based on the ML/TF risks posed, including the factors discussed above. Customers and investors that are risk classified as low (or the equivalent) may be subject to simplified CDD procedures. However, entities must be aware that their risk classification of a Customer/Investor being low-risk is only valid if the finding is consistent with the findings of the national risk assessment or the Supervisory Authority, whichever is most recently issued. Customers and investors that are risk classified as medium risk (or the equivalent) may be subject to normal CDD procedures. Customers and investors risk classified as high risk must be subject to enhanced CDD procedures.

6. On-Going Monitoring should take place to ensure that documents, data, information collected during the various due diligence procedures on the customers or investors are kept up-to-date and relevant. Entities should ensure that the customers or investors are periodically screened against the

vigilance databases/sanction lists and periodic reviews should also be conducted on the customers or investors based on their risk rating.

E. APPLICANT FOR BUSINESS (refer also to Part II)

Who should be treated as the Applicant for Business?

10. **The applicant for business may be any one of the following:**

Eg.	FSP	Applicant for Business
1.	The Mutual Fund.	(1) Investors should be treated as such for the purposes of the Guidance Notes.
2.	FSP incorporating a company/setting up a limited partnership/unit trust as part of a Mutual Fund structure (including acting as investor, shareholder and/or providing initial registered office).	(1) Promoters (as defined in the MFL). (2) Where the mutual fund is a unit trust, the trustees; or (3) Where the mutual fund is a limited partnership, the general partner; or (4) Where the mutual fund is a corporation, the directors (see the section on Company Formation and Management).
3.	FSP providing registered office for Mutual Fund/general or limited partner (other than at the date of incorporation). FSP providing a principal office for a Mutual Fund Administrator.	(1) The Mutual Fund. (2) The Mutual Fund Administrator
4.	Mutual Fund Administrator.	(1) The Mutual Fund (and the relevant Operators thereof). (2) When the Mutual Fund for which documentary evidence should be obtained is a unit trust or a limited partnership, it will usually be sufficient to obtain evidence of the identity of the Trustee or the controlling General Partner.

		(3) Given the special circumstances of mutual funds, it is recommended as good practice that a Mutual Fund Administrator should not rely on the Mutual Fund falling into the specified scenarios in which simplified CDD would apply by virtue of it being subject to the Regulations. However, the Administrator may be satisfied that the Mutual Fund, if not itself carrying out customer identification or record keeping, has in place appropriate safeguards to ensure that its obligations under the Regulations are met. (4) Promoters: Whilst promoters are not to be treated as applicants for business for the purposes of these Guidance Notes, it is industry best practice to ascertain the identity and background of any promoter relied upon.
	FSP otherwise issuing and administering subscriptions/redemptions.	(1) The Mutual Fund.

F. CUSTOMER DUE DILIGENCE (refer also to Section 4 of Part II)

When must the identity be verified?

1. The Regulations provide that there should be procedures in place requiring, as soon as reasonably practicable after contact is first made with an applicant for business, either satisfactory evidence of the applicant's identity or that steps are taken which will produce satisfactory evidence of identity.

2. The time span in which satisfactory evidence has to be obtained depends on the particular circumstances and the practicalities of obtaining evidence before commitments are entered into between parties and before money passes.

How might identification of existing customers be carried out?

3. Refer to Section 4 (Customer Due Diligence) of Part II of the Guidance Notes.

4. If, after having conducted a risk assessment, verification procedures or identification of an investor have not been completed prior to the date on which redemption is due to take place, the Mutual Fund should use the opportunity of redemption to seek satisfactory evidence of identity. Payment of the redemption proceeds should be made only to the investor and not to a third party and only when the outstanding due diligence documentation has been collected and verified. If payment is to be made to or from an account in the name of the investor with a regulated bank in the Cayman Islands or in an AMLSG List country and the requirements set out in Section 5 of Part II of the Guidance Notes are adhered to, that will be sufficient evidence of identity

Particular Issues on Verification of Identity of Investors.

One-off transactions.

5. For the purpose of the Guidance Notes a subscription to a Mutual Fund should not be treated as a one-off transaction (for which see section 4 of Part II of the Guidance Notes).

If the investor is a fund domiciled outside an AMLSG List Country but is administered in an AMLSG List Country.

6. In such a case, the investor may fall within one of the specified scenarios in which simplified CDD would apply.

7. Evidence may also be satisfactory if the investor's administrator**:**
   (1) is subject to the Anti-Money Laundering regime of the AMLSG List country; and

   (2) confirms in writing that it has obtained and maintains customer verification evidence in accordance with the procedures of the AMLSG List Country.

Payment on an Account in a Bank In the Cayman Islands or an AMLSG List Country

8. See Section 5 D of Part II of these Guidance Notes.

Corporate Group Introduction

9. It will not be necessary for identity to be re-verified or records duplicated if the identity of an investor has been verified by another entity within a group in a manner compatible with the Regulations and provided that written

confirmation is obtained that the identification records will upon request be provided.

10. This is so even in circumstances when neither the investor nor the Bank from which he sends funds or investment is located in an AMLSG List country.

G. INTERNAL CONTROLS AND ONGOING MONITORING (refer also to Part II)

1. Regulated Mutual Funds and Mutual Fund Administrators must have internal reporting procedures in place to (1) identify and report suspicious activity, (2) monitor and ensure internal compliance with laws relating to money laundering, and (3) test the AML/CFT system consistent with the Regulations and the Guidance Notes (the "Procedures").

2. Both Mutual Funds and their Mutual Fund Administrators subject to the Regulations have separate obligations to maintain and implement such Procedures in respect of their relevant financial business.

3. Although ultimate responsibility for maintaining and implementing satisfactory Procedures remains with the Mutual Funds and Mutual Fund Administrators, the obligations may be met by delegating or outsourcing those functions.

4. A mutual fund can meet its obligations in relation to the Procedures in one of four ways:
   (1) It can implement Procedures directly.
   (2) Where a Fund has no staff in the Islands and the administration of subscriptions and redemptions is done by a person subject to the anti-money laundering regime of the Cayman Islands or a AMLSG list country, the Fund will be regarded by the Monetary Authority as being compliant with the Regulations and the Guidance Notes in relation to the Procedures if the Fund's reliance on such a person is acknowledged in an appropriate agreement (e.g., an administration or registrar and transfer agency agreement) and if the person administering subscriptions and redemptions does so in compliance with the applicable Procedures of such jurisdiction.
   (3) Where a Fund has delegated any of the Procedures to a person subject to the anti-money laundering regime of the Cayman Islands or an AMLSG List country, consistent with the requirements of section 4 of Part II of these Guidance Notes, where applicable, the Fund will be regarded by the Monetary Authority as being compliant with the Regulations and the Guidance Notes with respect to the Procedures if the delegate complies with the applicable Procedures of such jurisdiction.
   (4) A Fund may also delegate any or all of its obligations with respect to the maintenance of Procedures to a suitable third party or parties, whether within or outside the Cayman Islands, provided that such

appointment is consistent with the requirements of Section 4 of Part II of these Guidance Notes, where applicable.

5. It should be noted that all mutual funds must designate an MLRO and DMLRO[64]. Mutual funds may delegate this function to their mutual fund administrators[65].

6. A Mutual Fund Administrator may delegate any of the Procedures to a regulated person in the Cayman Islands or a person in an AMLSG List country that is subject to the AML/CFT regime of that country, consistent with the requirements of sections 4 and 10 of Part II of these Guidance Notes, where applicable.

7. The Mutual Fund Administrator will be regarded by the Monetary Authority as being compliant with the Regulations and the Guidance Notes with respect to the Procedures if the delegate complies with the Procedures of such jurisdiction.

8. A Mutual Fund Administrator may also delegate any or all of its obligations with respect to the maintenance of Procedures to a suitable third party or parties, whether within or outside the Cayman Islands, provided that such appointment is consistent with the requirements of Sections 4 and 10 of Part II of the Guidance Notes.

9. The operators of the Mutual Fund or Mutual Fund Administrator should document, either as a board resolution or otherwise, the manner in which the entity has met its obligation to maintain Procedures.

H. RECORD KEEPING (refer also to Section 8 and 11 of Part II)

What specific records should be kept and where?

1. Refer to Sections 54 and 55 of the Companies Law (2016 Revision)

2. It may be impractical for a regulated Fund itself to maintain records but it must ensure that all appropriate records are maintained on its behalf.

3. Mutual Fund Administrators must ensure that they have customer verification evidence appropriate to the administration of Mutual Funds and, if the function is delegated to them, must maintain records on behalf of the Mutual Fund for the requisite period.

When procedures required by the Regulations may be maintained by a party not based in the Cayman Islands.

4. Maintenance by a person or institution regulated in an AMLSG List country of all records and compliance with the procedures of such an AMLSG List country

[64] Reg. 33 AMLRs (2017)
[65] Reg. 3(2) AMLRs (2017) as amended by the Anti-Money Laundering (Amendment) Regulations, 2017

will be regarded as compliance with the Regulations and the Guidance Notes, subject to compliance with the provisions of Section 5 of Part II of the Guidance Notes.

When may a successor Mutual Fund Administrator rely on the customer verification evidence obtained by its predecessor?

5. Where a successor firm is acquiring administration of an existing Mutual Fund, the successor must ensure that the necessary due diligence has been performed prior to performing the administration.

6. It may be possible to rely upon the evidence of identity obtained by a predecessor Mutual Fund Administrator provided that the original files, or certified copies of the original files, are transferred to the successor Mutual Fund Administrator and the successor firm has assessed the quality of the evidence on investor identity.

7. Where insufficient evidence exists, it may be appropriate to supplement with additional evidence to meet the standards required by these Guidance Notes.

8. At no time would it be appropriate to rely upon an eligible introducer letter as a method for the customer verification evidence obtained by its predecessor.

I. MONEY LAUNDERING/TERRORIST FINANCING WARNING SIGNS

1. In addition to the risk factors in section 3 of Part II and the warning signs set out in Appendix D of the Guidance Notes, risk factors and ML/TF warning signs to which Mutual Funds and/or Mutual Fund Administrators must have regard to in order to satisfactorily assess the ML/FT risks pertaining to a particular business relationship or transaction include:

    (1) When an investor is more concerned about the subscription and redemption terms of the Mutual Fund than with other information related to the investment strategy, service providers, performance history of the investment manager, etc.
    (2) Lack of concern by an investor regarding losses or (large) fees or offering to pay extraordinary fees for early redemption;
    (3) Sudden and unexplained subscriptions and redemptions;
    (4) Quick purchase and redemption of units despite penalties;
    (5) Requests to pay redemptions proceeds to a third (*unrelated*) party;
    (6) A fund, or principals of a fund (i.e. a client of a mutual fund administrator) that exhibits unusual concern with compliance with AML/CFT reporting requirements or other(AML/CFT) policies and procedures; and
    (7) When a promoter/manager attempts to launch a new Mutual Fund with large amounts of seed capital from one source, either from an internal or external source. (The source of funds must be properly verified.)

PART VII

SECTOR SPECIFIC GUIDANCE: MONEY SERVICES BUSINESS, OTHER REGULATED FINANCIAL INSTITUTIONS & UNSUPERVISED LENDERS

The purpose of this part of the Guidance Notes is to provide some guidance specifically for the Money Services Business Sector, the Cayman Islands Development Bank ("CIDB") and Un-supervised Lenders. This guidance (Part VII) covers MSB sector in section 1 and CIDB in section 2 and un-supervised lending activity in section 3. This Part VII should be read in conjunction with Part I, Part II and the Appendices of the Guidance Notes.

SECTION 1

MONEY SERVICES BUSINESS

A. OVERVIEW

1. Section 2 of the Money Services Law (2010 Revision) defines "money services business" (MSB) as-

(1) the business of providing (as a principal business) any or all of the following services-

(a) money transmission;

(b) cheque cashing;

(c) currency exchange;

(d) the issuance, sale or redemption of money orders or traveller's cheques; and

(e) such other services as the Governor in Council may specify by notice published in the Gazette; or

(2) the business of operating as an agent or franchise holder of a business mentioned in paragraph (1).

2. Money transmission business can be described as the business of accepting funds for their transmission to persons in another country or domestic location. MSBs cater primarily to the resident domestic market, in particular, the expatriate workers of lower income.

3. The cash-intensive nature of the industry raises potential ML/TF concerns. The money remittance sector has challenges accessing banking services, which is an increasing global trend. The lack of access to traditional banking services may increase the level of vulnerability.

4. Typically, users of money remittance services are individuals, expatriate workers and smaller entities that send cash to other individuals thereby bypassing a traditional bank. The speed with which transactions occur can help individuals dispose of illicit proceeds instantaneously. Cross border fund flows also increase the risk of illicit funds being introduced into the Cayman Islands economy/financial system. With the Cayman Islands being a major cruise destination, employees of the cruise lines are known to be users of the remittance system, although this would be a miniscule population.

B. SCOPE

1. This part of the sector specific guidance seeks to provide practical assistance to MSBs in complying with the AMLRs, interpreting and applying the general

provisions of the part II of these Guidance Notes, and for MSBs to adopt sound risk management and internal controls for their operations.

2. The AMLRs apply to MSBs as indicated in the list of activities falling within the definition of "Relevant Financial Business" in the Sixth Schedule of the Law. This section should be read in conjunction with Part I and II of these Guidance Notes.

3. It is the responsibility of each MSB to have systems and training in place to prevent ML/TF. Each MSB must maintain adequate AML/CFT systems which include CDD measures, record-keeping procedures, and such other procedures and controls appropriate for the purposes of forestalling and preventing ML/TF.

C. ML/TF RISKS

3. The fleeting relationship with their customers makes MSBs vulnerable to ML/TF. A person would typically have to be a customer with an account at a bank, for example, to be able to access the services of that bank, whereas a person does not have that type of relationship with the MSB and can repeatedly use different MSBs to transact business. The money transmission part of the MSB is particularly vulnerable, given the high volume of cash handled on a daily basis and the ability to transmit funds instantly to any part of the globe.

4. While the international remittance system is typically used by expatriate workers to send a part of their earnings back home, it can also be used to transmit the illegal proceeds of criminal activities and thereby poses ML/TF risk. The rapid movement of funds across multiple jurisdictions presents a challenge to investigators, particularly if the identity of the originator is unclear. For this reason, international standards have been developed with respect to payer (and payee) information that should accompany wire transfers to mitigate the above-mentioned risk.

5. Cheque cashing is another important segment of the business for some MSBs. MSBs should be aware that endorsed third party cheques from overseas are a ML/TF risk. Even where a Cayman Islands cheque, endorsed by a third party, is presented to the MSB for cashing, the MSB should take appropriate steps to ascertain the economic purpose behind the endorsement to that person presenting the cheque. Large value cheques originating from unknown individuals present a greater ML/TF risk compared to small cheques originating from well-established businesses. MSBs must have board approved AML/CFT policies and procedures that give staff clear guidance in dealing with these situations.

6. Currency exchange is another important segment of the business for some MSBs. MSBs who offer this type of service must have policies and procedures specific to the risks posed by this activity.

D. RISK BASED APPROACH

1. MSBs should adopt a risk-based approach to manage and mitigate ML/TF risks. In so doing, in addition to assessing risks inherent to their business, MSBs should develop risk profiles of their customers, thereby familiarising themselves to customers' personal or business needs for the services provided.

2. While conducting risk assessments, MSBs should take into consideration the factors such as-

   (1) the types of products and services that they offer;

   (2) their customer types (customer occupation or type of business operated);

   (3) the geographical location of customers or where funds are transmitted; and

   (4) the average cash value of typical transactions and the $15,000 customer identification threshold as per the AMLRs.

3. As much as possible, MSBs should use computer technology to conduct the risk assessment. As provided in Part II of these Guidance Notes, customers, products, geography and services should be ranked (for example as "high," "medium," or "low" risk). For instance, the transfer of a part of an expatriate worker's weekly wage to his/her family in his/her home country should be less risky compared to the transmission of a large sum by a visitor to numerous recipients.

4. High risk customers, products, geographical regions and services should be subject to EDD and transaction monitoring. The risk model should be documented, with its rationale clearly stated, and should be updated on a regular basis to keep in line with changes in the business, customer profile or the ML/TF risks. See detailed guidance provided in section 3 of Part II of these Guidance Notes.

E. CUSTOMER DUE DILIGENCE

1. MSBs shall adopt sound customer due diligence policies and procedures. Requiring appropriate due diligence information and documentation, verifying the information, and being alert to unusual or suspicious transactions can help an MSB deter and detect ML/TF schemes.

2. A customer identification and verification policy tailored to the operations of a particular business:

   (a) helps detect unusual/suspicious activity in a timely manner;

(b) promotes compliance with the relevant laws, regulations and guidance;

(c) promotes safe and sound business practices;

(d) minimises the risk that the MSB will be used for ML/TF and other criminal activities and as a result reduces the risk of government seizure and forfeiture of funds associated with customer transactions (such as outstanding money orders/traveller's cheques and outstanding money transfers); and

(e) protects the reputation of the MSB and reduces or minimises the risk of de-risking.

Whose Identity must be verified?

3. The applicant may be an individual, a corporate customer, a partnership or an unincorporated business.

4. The MSB must have documented steps that are utilized to distinguish between someone who is acting on his own behalf and someone who is acting on behalf of another (money mules/straw men). If it is determined that the person is acting on behalf of another, then the procedures for verifying the identity of the ultimate applicant must apply (see section 4 of Part II of these Guidance Notes).

5. All applicants for business undertaking money transmission via electronic funds transfer, in which case MSBs must comply with the requirements set out for wire transfers as specified in section 11 of Part II of the Guidance Notes and in the AMLRs. (Regulations in Part X of the AMLRs apply to transfers of funds which means "any transaction carried out on behalf of a payer through a payment service provider by electronic means…").

6. Notwithstanding that there may be some transaction that are definitely one-off, the nature of business for many of the MSBs licensed in Cayman, tend to be transactions carried out by customers on a frequent, habitual or regular basis or may be linked Given this and the ML / TF risks identified above, MSBs should therefore also:

(1) verify identity for applicants, for money transmission and other services, where the customer, product or geography risk is deemed to be high risk in the risk assessment conducted;

(2) Verify identity for applicants where there is an ongoing relationship akin to a business relationship as defined in the ALMRs;

(3) For services other than wire transfer money transmission, establish more diligent thresholds other than the $15,000 stipulated in the AMLRs. The threshold should be derived from the risk assessment, bearing in mind what- (1) the amount that the average customer would transact and (2) the reporting threshold of US$3,500 on the quarterly MSB form reported to the Monetary Authority.

7. Applicants/Customers may fall within the following categories:

	Applicant for Business	**Requirements** (Highlights and supplementary only– please refer to section 4 of Part II of the Guidance Notes for the full (normal) CDD requirements).
1.	Natural Persons	(1) Identification documentation should be obtained for the applicant/customer him/herself (2) Identification documentation should be obtained for beneficial owner of funds (3) Identification documentation should be obtained for Third Party sending funds (4) Satisfactory evidence of identity, name and address, confirmed by using one or more of the verification methods in section 4 of Part II of these Guidance Notes
2.	Corporate Customer	(1) The company (evidence that it exists) e.g. a trade and business licence or a certificate of registration. (2) Consistent with that required for direct personal customers, documentary evidence of identity for all directors; all those with signing powers, including third parties; and beneficial owners. (3) Documentary evidence of identity of the new owner/controller where there is a change in ownership or control, in accordance with that required for direct personal relationships. (4) Satisfactory evidence, confirmed by at least one of the following independent checks, of company's existence: (a) Memorandum and Articles of Association and Certificate of Incorporation (b) Information about the identity of controlling shareholders and directors, e.g., Register of Directors, Register of Members (c) Understanding of all relevant third party and inter-company relationships (d) It may be appropriate to obtain information relating to customers or suppliers and the background of major

		shareholders and directors
3.	Partnerships / Unincorporated Businesses	(1) The entity, evidence that it exists. (2) Consistent with that required for direct personal customers, documentary evidence of identity required for partners/managers; all those with signing powers, including third parties; and beneficial owners. (3) Documentary evidence of identity of the new owner/partner/controller where there is a change in ownership/partnership or control, in accordance with that required of direct personal relationships. (4) Satisfactory evidence, confirmed by at least one of the following independent checks, of existence of partnership / unincorporated business: (a) Partnership agreement or excerpt if relevant; (b) Certificate of Registration; (c) Information about the identity of controlling partners / shareholders, e.g., excerpt from partnership document; (d) Establish all relevant third party relationships.

When must identification documentation be obtained?

8. Customer identification documentation is to be obtained prior to a transaction being carried out.

9. If identification information is not obtained, the transaction should not proceed.

What should be done if there are Doubts as to the Identity of an Existing Customer?

10. If in the process of reviewing identification documentation, the MSB has doubts about the veracity or adequacy of previously obtained customer

identification data, then the MSB must take reasonable steps to verify the data.

11. Depending on the assessed ML/TF risk of the customer, the MSB could either wait for the customer to transact business again if he is a regular customer, or it can contact the individual by phone requesting that she/he submit the relevant additional documentation.

12. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of ML/TF in relation to that customer, or where the customer's pattern of transactions changes from what is deemed to be "normal" for that customer.

What Is Considered To Be An Appropriate Description Of "Source Of Funds"?

13. The appropriate description of a customer's "source of funds" include:

    (1) Salary supported by documentation on employment should be requested;
    (2) Sale of property including documentation evidencing the sale; and
    (3) Loan proceeds including documentation evidencing the grant of the loan.

14. The following on their own would not be considered appropriate descriptions of the ultimate "source of funds":

    (1) "Partners"[66];
    (2) Savings.

15. In the case of Partners, additional enquiries such as confirmation from the "banker" would be appropriate, while in the case of Savings, a bank statement should be provided. Partners and savings are nonetheless sources of funds for which additional proof of salary, dividends, sale proceeds, or loan (ultimate sources) should be provided.

Why Is It Important To Establish The Purpose Of The Transaction?

16. It is important to establish the purpose for those transactions that are large, complex or unusual (see section 2 B of this document for further guidance).

[66] Partners is an informal saving and credit scheme in the Caribbean in which a group of people regularly deposit a fixed amount of money with a main organiser, the 'banker', into a central fund. The banker distributes the total sum (the 'hand') to members in a pre-arranged order. This system of credit operates almost completely on trust, in that each person who collects his/her lump sum must be trusted to continue paying in the contributions until all members have collected their 'hand.' This scheme operates usually with no written agreement.

17. The threshold for large transactions should be determined from the MSB's risk assessment.

18. Similar to a Bank, an MSB should ask the customer about the purpose of the transaction that is beyond the MSB's threshold. In that way, the MSB should be able to establish if the purpose is lawful and whether the transaction will be a one-off event or part or a regular occurrence.

19. Information on the purpose of the transaction helps the MSB to develop a profile of "normal" activity for that customer. If the MSB is unable to establish what "normal" activity is, then it would be challenging to distinguish the unusual activities for further analysis to determine which ones are suspicious. It is therefore imperative for MSBs to consistently work towards developing customer profiles for all customers using the service.

20. Securing information on the relationship of the recipient of the transfer is useful in assisting with establishing the purpose of the transaction.

F. ELECTRONIC FUNDS TRANSFER

What Information Should Accompany The Transfer Of Funds?

1. MSBs must ensure that information on the payer and the payee accompanies the transfer of funds.

2. For guidance on the payer and payee information that need to accompany a transfer of funds, see section 11 of Part II of the Guidance Notes as that section and the regulations in Part X of the AMLRs apply to transfers of funds which means "any transaction carried out on behalf of a payer through a payment service provider by electronic means…".

G. SYSTEMS, POLICIES AND PROCEDURES

What policies and procedures should be documented?

1. At the very least, MSBs should have documented policies and procedures on:
   (1) the assessment of risks;
   (2) risk mitigation and management measures;
   (3) customer identification and due diligence;
   (4) when will enhanced due diligence be applied and what does it entail;
   (5) transaction monitoring, including complex and unusual transactions;
   (6) suspicious activity reporting;
   (7) internal controls; and
   (8) staff training.

How Should The Business Of A Customer Be Monitored?

2. Because of the large number of customers involved and the relative small amounts transacted, it is imperative for MSBs to have adequate systems in place to collate relevant information and monitor customers' activities.

3. The amount of information collected may be broadened to include details of the recipient of the funds. This information will assist MSBs to determine whether there is any ML/TF risk when the customer is utilising multiple recipients or whether multiple customers are remitting multiple small sums that are accumulated with one recipient.

What To Do About Complex And Unusual Transactions?

4. As mention in section 9 of the part II of these Guidance Notes, where a transaction is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, the transaction must be considered unusual, and the staff member put the transaction "on enquiry".

5. An example of an unusual pattern of transactions would be where an MSB's database reveals that several seemingly unrelated individuals are receiving or sending small amounts of money from or to one individual abroad. In such case, the MSB may request additional information on the receivers including the information on the relationship between sender and receiver(s). Additionally, the FSP may conduct an internet or screening database search to find out more about the senders and/or recipients.

6. MSBs should follow the procedures as explained in part II section 9 (and more particularly items D, E and F) of these guidance Notes for the purpose of identifying and dealing with unusual and suspicious transactions.

What Specific Records Should Be Kept And Where?

7. The MSB must keep adequate records of the identity of its customers and all transactions conducted by that customer for a period of 5 years following the last transaction, the closing of an account, or the termination of the business relationship.

8. Refer to section 8 of Part II of the Guidance Notes for guidance on "Record Keeping Procedures".

Filing A SAR

9. Refer to section 9 of Part II of the Guidance Notes, and section 34 of the AMLRs and section 136 of the Law for the role of the MLRO and reporting obligations.

10. It is important to note that SARs must be filed with the FRA in case of a suspicious transaction even if the transaction did not proceed.

Training

11. Staff should be educated in the "Know Your Customer" requirements for the prevention of ML/TF.

12. Training should therefore cover not only the need to know the customer's true identity, but also, where a business relationship is being established, the need to know enough about the type of business activity expected in relation to the customer at the outset (and on an ongoing basis) so that "normal" activity can be distinguished from suspicious activity in the future, as it relates to that person.

13. New frontline agents should not be allowed to process transactions until they have participated in the required training and successfully passed the requisite test(s). They should also be adequately trained on the factors which may give rise to suspicions about customers' activities and the procedures to adopt when a transaction appear suspicious.

14. For further details, refer to section 10 of Part II of the Guidance Notes.

Independent Audit Function

15. MSBs must have procedures of internal control including an appropriate internal audit function for the prevention of ML/TF. The internal audit function serves to test the MSB's system of internal control and is to be appropriate to the MSB's size and to the nature of its operations.

16. Testing should be risk-based, with particular emphasis on high-risk operations.

17. It should be independent, conducted periodically, and reported directly to the Board. The audit report should include, but not be limited to, the following:

    (1) review of high risk accounts, transactions, and customers;
    (2) one-off transactions in excess of the limit set by the MSB and suspicious activity reporting;
    (3) assessment of money remittance, currency exchange and check cashing transactions (to ensure whether they are in accordance with the relevant laws, regulations and guidance);
    (4) review of adequacy of customer identification information and customer due diligence; and
    (5) complex and unusual transactions.

H. ML / TF WARNING SIGNS OR "RED FLAGS"

Customer Profile

1. The following are some of the warning signs and red flags that money transmission/remittance provider (MRPs) should be alert to in respect of a customer's profile. The list is not exhaustive, but includes:

    (1) The Customer's area of residence is inconsistent with other profile details such as employment;
    (2) The size or frequency of the transaction(s) is not consistent with the normal activities of the customer;
    (3) The goods/currencies purchased, and/or the payment arrangements are not consistent with normal practice for the type of business concerned;
    (4) The customer's only address is a post office box or a c/o (in care of) address;
    (5) The customer's address is that of a company service provider (domiciliation service);
    (6) The customer's address information is difficult to verify;
    (7) The stated address does not exist;
    (8) A large number of persons are registered at the stated address, or there are a very large number of changing occupants, or other information is available indicating that it is not the real address of residence or domicile;
    (9) The address of customer's residence does not correspond to the customer's financial arrangements;
    (10) The customer changes address frequently;
    (11) The customer is a business whose name and purpose do not correspond with its transactions;
    (12) The customer cannot immediately provide additional identification documents;
    (13) Identification documents appear to be unused;
    (14) Identification documents are soiled making it difficult to read the necessary information;
    (15) The customer is known to have a criminal history;
    (16) The customer is close to a person who is known to have a criminal history;
    (17) Sudden change in the customer's life style;
    (18) The customer drives very expensive cars that do not correspond to his/her income situation;
    (19) The customer hires or leases costly assets (e.g., real estate or cars) that do not correspond to his/her income situation.

Customer Behaviour

2. The following are some of the warning signs and red flags that MRPs should be alert to in respect of a customer's behaviour. The list is not exhaustive, but includes:

(1) The customer is unwilling to provide details of his/her identification information and references;
(2) Use of false identification documents to send money;
(3) Customer changes a transaction after learning that he/she must show ID;
(4) The customer shows no interest in costs or rates;
(5) The customer does not choose the simplest way to carry out a transaction;
(6) The customer has no connection with the area where the customer relationship is established;
(7) Transaction is a price-raising link in a series of transactions with no obvious reasons for the choice;
(8) The customer gives a rather detailed explanation that appears to be rehearsed concerning the reasons for the customer relationship or the transaction;
(9) The customer does not respond to communication/letters to the stated address;
(10) The customer has many newly established companies;
(11) The customer contracts a loan secured on lodging of equivalent security;
(12) The customer has companies abroad that are not justified by the customer's business;
(13) The customer explains that expensive assets are a loan from or financed by a third party;
(14) The customer uses a payment card from a country which is not his country of residence.

Transactions

General

3. The following are some of the warning signs and red flags that MRPs should be alert to in respect transactions generally. The list is not exhaustive, but includes:

(1) The transaction seems to involve unnecessary complexity;
(2) Use of front/straw men and/or shell companies;
(3) Transactions in a series are structured just below the threshold for due diligence identity checks;
(4) The customer appears to be trying to avoid reporting requirements by using two or more locations or cashiers on the same day or in quick succession to break one transaction into smaller transactions;
(5) Two or more customers appear to be trying to avoid reporting requirements and seem to be working together to break one transaction into two or more transactions;
(6) Transactions are carried out by the customer on behalf of third parties without there being an appropriate business relationship with such parties;
(7) Frequent transaction orders are made by the same customer;

(8) Sudden increases in the frequency/value of transactions of a particular customer without reasonable explanation;
(9) An unusually large (cash) transaction;
(10) The amount of the transaction is unusually large for the typical customer or for the MSB;
(11) The transaction has no apparent purpose or no obvious economic/financial basis;
(12) Unnecessary routing of funds through third parties;
(13) A customer sends/receives funds to/from him/herself, for no apparent purpose;
(14) There is no genuine reason for the customer to use the services of the MSB;
(15) Transfers of large sums of money to or from overseas locations with instructions for payment in cash;
(16) One legal/natural person transfers sums to many legal/natural persons;
(17) One legal/natural person receives sums from many legal/natural persons (from various countries);
(18) Many legal/natural persons (who have no obvious blood/business relation) are beneficial owners of transfers ordered by one legal/natural person;
(19) An under-aged person receives funds from many legal/natural persons and/or from different locations;
(20) A customer sends/receives funds to/from counterparts located in jurisdictions which are known to be exposed to ML/TF risks, for example, drug trafficking, terrorism financing, smuggling;
(21) Non face-to-face customers that are not physically present for identification purposes;
(22) Transactions are accompanied by information which appears clearly false or contradictory;
(23) The customer is unwilling to provide routine information when requested or the information provided is insufficient, false, or hard for the MSB to verify;
(24) No or limited information about the origin of funds;
(25) The explanation for the business activity and/or the funds involved is not credible;
(26) Electronic transfers involving large sums of money does not include data allowing for the clear identification of such transactions;
(27) The customer is accompanied by others who keep a low profile or stay just outside the location;
(28) The customer reads from a note he apparently did not write himself;
(29) The customer receives instructions from others;
(30) The customer appears to be in doubt when asked for further details;
(31) Difficulty in obtaining details of the beneficial owners;
(32) No relationship between sender and beneficiary;
(33) The supporting documentation does not add validity to the other information provided by the customer;

(34) The customer is in a hurry to rush a transaction through, with promises to provide the supporting information later;
(35) The customer represents a business but seems to have no business experience;
(36) The authority for others to collect funds does not seem to be well-founded;
(37) Correspondence is to be sent to another person other than the customer;
(38) Form is filled in advance;
(39) The pattern of transactions has changed since the business relationship was established;
(40) Money transfers to high-risk jurisdictions without reasonable explanation, which are not consistent with the customer's usual foreign business dealings;
(41) Sudden increases in the frequency/value of transactions of a particular customer without reasonable explanation;
(42) Instruction on the form of payment changes suddenly just before the transaction goes through;
(43) The customer, without a plausible reason, repeatedly goes to agents located far from his/her place of residence or work;
(44) Funds are sent at a time not associated with salary payments;
(45) Remittance sent or received outside customers' remittance corridors.

Cash transactions

4. The following are some of the warning signs and red flags that MRPs should be alert to in respect of cash transactions. The list is not exhaustive, but includes:

(1) Unusually large cash payments in circumstances where payment would normally be made by cheque, bank draft, etc;
(2) Cash is in used notes and/or small denominations (possible indication that the money originates from the criminal offence) and dirty or has an unusual odour;
(3) Customer refuses to disclose the source of cash;
(4) Customer has made an unusual request for collection or delivery;
(5) Stains on the notes indicating that the funds have been carried or concealed, or the notes smell musty, are packaged carelessly and precipitately;
(6) When the funds are counted, there is a substantial difference between the actual amount and the amount indicated by the customer (over or under);
(7) Detection of counterfeit banknotes in the amount to be transferred or exchanged;
(8) Presenting funds in cash with further transfer of funds to another person on the same or next Day.

Other Indicators for Money Remittance /Transmission Providers

General

5. The following are some of other indicators to which MRPs should be alert. The list is not exhaustive, but includes:

   (1) Transferring funds without any apparent economic reason;
   (2) Money transfers to high-risk jurisdictions without reasonable explanation, which are not consistent with the customer's usual business dealing;
   (3) Transfers paid by large cash amounts in different sums in a short period of time;
   (4) Personal remittances sent to jurisdictions that do not have an apparent family or business link;
   (5) Remittance made outside migrant remittance corridors (e.g., Asian foreign domestic remits funds to South America);
   (6) Personal funds sent at a time not associated with salary payments;
   (7) The customer seems only after the counting to know which amount is being transferred;
   (8) The customer shows no interest in the transfer costs;
   (9) The customer has no relation to the country where he/she sends/receives the money and cannot sufficiently explain why money is sent there/received from there;
   (10) The customer has a note with information about payee but is hesitating if asked whether to mention the purpose of payment;
   (11) Large or repeated transfers between the account of a legal person and a private account, especially if the legal person is not a resident;
   (12) Large or frequent transfers of money;
   (13) Use of groups of people to send money;
   (14) Use of different money remittance businesses;
   (15) Amounts sent are higher than usual;
   (16) The operations are irregular;
   (17) Receiving money from different parts of the world (developed countries) from different people;
   (18) Money is received during short periods of time;
   (19) Money is received from different money remittance companies;
   (20) Multiple senders to a single individual.

Other Indicators for Currency Exchange Service Providers

General

6. The following are some of other indicators to which Currency Exchange Providers should be alert. The list is not exhaustive, but includes:

   (1) Exchange of large quantities of low denomination notes for higher denominations;
   (2) Exchange of large amounts or frequent exchanges that are not related to the customer's business;
   (3) Structuring of large amounts;

(4) Repeated requests for foreign exchange purchasing-selling transactions in the amounts slightly less than the transaction limit for identification in a short period of time;
(5) The customer requests currency in large denomination notes;
(6) The customer buys currency that does not fit with what is known about the customer's destination;
(7) The customer buys currency from an unusual location in comparison to his/her own location;
(8) The customer apparently does not know the exact amount being exchanged;
(9) The customer looks around all the time and does not watch the counting of money;
(10) The customer is happy with a poor exchange rate;
(11) Currency purchases with large cash amounts;
(12) Large exchanges between foreign currencies;
(13) Frequent exchange of cash into other currencies;
(14) Exchange of primarily one type of currency;
(15) The amounts exchanged are significantly higher than usual;
(16) There is no link between the amount of money exchanged and holiday periods;
(17) High frequency of currency exchange transactions over a period of time;
(18) Many currency exchange offices used by the same person;
(19) Requests to exchange large amounts of foreign currency which is not convertible (or not frequently used) to another kind of foreign currency.

Section 2

CAYMAN ISLANDS DEVELOPMENT BANK

A. OVERVIEW

1. The Cayman Islands Development Bank (the "CIDB") is solely owned by the Cayman Islands Government. The principal function of CIDB is to mobilise, promote, facilitate, and provide finance for the expansion and strengthening of the economic development of the Islands. The Bank does this by providing financing for tertiary education, housing, agriculture and the development of small businesses. The CIDB does not accept deposits and therefore the sector guidance is geared toward ML/TF risks in loans.

B. Scope

1. This section is applicable to the Cayman Islands Development Bank (the "CIDB").

C. ML/TF

1. The involvement of multiple parties may increase the risk of ML/TF when the source and use of the funds are not transparent. This lack of transparency can create opportunities in any of the three stages of ML/TF schemes. These schemes could include the following:

   (1) Loans are made for an ambiguous or illegitimate purpose.

   (2) Loans are made for, or are paid for, a third party.

   (3) The customer attempts to sever the paper trail between the borrower and the illicit funds.

D. RISK BASED APPROACH

1. The CIDB must adopt a risk-based approach to managing ML/TF risks. The RBA aims to support the development of mitigation measures that are commensurate to the ML/TF risks identified. Entities should refer to section 3 of the Part II of these Guidance Notes.

E. CUSTOMER DUE DILIGENCE

Who is the customer/applicant for business?

1. The applicant may be any one of the following:

(1) Natural persons;

(2) Corporate persons or persons holding a trade and business licence.

2. The below table shows minimum identification information requirements; however, FSPs shall consider the relevant guidance provided under section 4 of Part II of these Guidance Notes.

	Applicant for Business	**Minimum Requirements**
1.	Natural Person	(1) Identification documentation should be obtained for the applicant/customer him/herself (2) Satisfactory evidence, confirmed by using one or more of the verification methods: (a) Current valid passport; (b) Any valid uniquely numbered government-issued ID card showing the photograph of the applicant, such as a driver's licence or a voter's registration card; and (c) A Cayman Islands employer ID card bearing the photograph and signature of the applicant.
2.	Corporate Customer	(1) The company (evidence that it exists) e.g. a trade and business licence or a certificate of registration. (2) Consistent with that required for direct personal customers, documentary evidence of identity for all directors; all those with signing powers, including third parties; and beneficial owners. (3) Satisfactory evidence, confirmed by at least one of the following independent checks, of company's existence: (a) Memorandum and Articles of Association and Certificate of Incorporation (b) Copy of Trade and Business Licence

When must identification be obtained?

3. Customer identification information is to be obtained prior to extending any loan facility to the customer.

4. If identification information is not obtained, the loan facility should not proceed.

F. INDEPENDENT AUDIT FUNCTION

1. The CIDB must have internal control procedures including an appropriate internal audit function for the prevention of ML/TF. The CIDB should have policies, procedures, and processes to monitor, identify, and report unusual and suspicious activities. The sophistication of the systems used to monitor lending account activity should conform to the size and complexity of the lending business.

2. The CIDB must liaise with the internal auditor to ensure that AML/CFT audits are regularly conducted in order to strengthen the processes and procedures and readily identify and address any risks of ML/TF.

G. WHAT WARNING SIGNS OR "RED FLAGS" SHOULD THE CIDB BE ALERT TO?

1. The following are some of the warning signs and red flags that the CIDB should be alert to in respect of a customer's profile. The list is not exhaustive, but includes:

    (a) Sudden/unexpected payment on loans. A customer may suddenly pay down or pay off a large loan, with no evidence of refinancing or other explanation.
    (b) Reluctance to provide the purpose of the loan, or the stated purpose is ambiguous, inconsistent or inappropriate (use of loan proceeds).
    (c) Loan payments by third parties. Loans that are paid by third party could indicate that the assets securing the loan are really those of the third party who may be attempting to hide the ownership of illegally gained funds.
    (d) Collateral pledged by a third party.
    (e) Financial statement composition of a business differs greatly from those of similar businesses.
    (f) Mortgage financing with a request for an unusually short maturity term.

H. TRAINING

1. Staff should be educated in various areas of AML/CFT compliance, and mainly in relation to CDD requirements and identification of suspicious activities for the prevention of ML/TF. Training should therefore cover not only the need to

know the customer's true identity, but also, where a business relationship is being established, the need to know enough about the (type of business) activity expected in relation to the customer at the outset (and on an ongoing basis) so that "normal" activity can be distinguished from suspicious activity in the future, as it relates to that person.

2. For further guidance, refer to section 10 of Part II of the Guidance Notes.

I. DOCUMENTATION OF POLICIES AND PROCEDURES

1. The CIDB should have documented policies and procedures in relation to various AML/CFT systems such as:

    (1) the assessment of risks;
    (2) Risk management and mitigation measures;
    (3) customer identification and due diligence;
    (4) when will enhanced due diligence be applied and what does it entail;
    (5) suspicious activity reporting;
    (6) internal controls; and
    (7) staff training.

J. RECORD KEEPING

1. The CIDB must keep adequate records of the identity of its customers, all transactions conducted by and any information relevant to that customer for a period of 5 years following the last transaction, the closing of an account, or the termination of the business relationship.

2. Refer to section 8 of Part II of the Guidance Notes for further guidance on record keeping procedures.

K. FILING A SAR

3. Refer to section 9 of Part II of the Guidance Notes, and section 34 of the AMLRs and section 136 of the Law for the role of the MLRO and reporting obligations.
4. It is important to note that SARs must be filed with the FRA in case of a suspicious transaction even if the transaction did not proceed.

Section 3

LOANS BY UN-SUPERVISED LENDERS

A. OVERVIEW

1. The Monetary Authority does not supervise all lenders within the Cayman Islands; however, there has been and continues to be a need for persons/organisations engaged in facilitating short term loans to adhere to the AML/CFT legislative requirements. These facilities usually include "Pay Day Loans".

2. Un-supervised lenders[67] are governed by the AMLRs and these Guidance Notes, and must operate their businesses in line with the laws of the Cayman Islands.

B. SCOPE

1. This section of the Guidance Notes provides guidance to the un-supervised lenders.

C. ML/TF RISKS

1. The Un-supervised lenders' risk assessments should take into consideration factors such as:
   (1) Its customer types (taking into account customer occupation or type of business operated);

   (2) The geographical location of customers or where funds are transmitted; and

   (3) The purpose of the loan.

D. RISK BASED APPROACH

1. Un-supervised lenders must adopt a risk-based approach to managing the ML/TF risks inherent to their business and associated with their customers. The RBA aims to support the development of mitigation measures that are commensurate to the ML/TF risks identified. Entities should refer to section 3 of the Part II of these Guidance Notes.

E. CUSTOMER DUE DILIGENCE

Who is the Customer/Applicant for business?

1. The applicant may be any one of the following:
   (1) Natural persons;

[67] FSPs that are conducting lending activity but are not supervised (by any supervisory authority)

(2) Corporate persons; or

(3) Persons holding a trade and business licence.

2. The below table shows minimum identification information requirements; however, Un-supervised lenders shall consider the relevant guidance provided under section 4 of Part II of these Guidance Notes.

	Applicant for Business	**Minimum Requirements**
1.	Natural Person	(1) Identification documentation should be obtained for the customer him/herself (2) Satisfactory evidence, confirmed by using one or more of the verification methods: (a) Current valid passport; (b) Any valid uniquely numbered government-issued ID card showing the photograph of the applicant, such as a driver's licence or a voter's registration card; and (c) A Cayman Islands employer ID card bearing the photograph and signature of the applicant.
2.	Corporate Customer	(1) The company (evidence that it exists) e.g. a trade and business licence or a certificate of registration. (2) Consistent with that required for direct personal customers, documentary evidence of identity for all directors; all those with signing powers, including third parties; and beneficial owners. (3) Satisfactory evidence, confirmed by at least one of the following independent checks, of company's existence: (a) Memorandum and Articles of Association and Certificate of Incorporation (b) Copy of Trade and Business Licence

3. Un-supervised lenders are required to collect identification documentation for all loans issued. (See section 4 of Part II of the Guidance Notes)

F. WHAT WARNING SIGNS OR "RED FLAGS" SHOULD FSPs BE ALERT TO?

1. The following are some of the warning signs and red flags that should be alert to in respect of a customer's profile. The list is not exhaustive, but includes:

   (1) Sudden/unexpected payment on loans. A customer may suddenly pay down or pay off a large loan, with no evidence of refinancing or other explanation;
   (2) Reluctance to provide the purpose of the loan, or the stated purpose is ambiguous, inconsistent or inappropriate use of loan proceeds; and
   (3) Loan payments by third parties. Loans that are paid by a third party could indicate that the assets securing the loan are really those of the third party who may be attempting to hide the ownership of illegally gained funds.

GUIDANCE NOTES ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING AND TERRORIST FINANCING IN THE CAYMAN ISLANDS

PART VIII

SECTOR SPECIFIC GUIDANCE: SECURITIES INVESTMENT BUSINESS

This purpose of Part VIII of the Guidance Notes is to deal with AML / CFT matters pertaining to Securities Investment Businesses that require more explanation or are more complex issues than are dealt with in the general body of these Guidance Notes. This section must be read in conjunction with Part I and II of the Guidance Notes and the Appendices.

SECTION 1

SECURITIES INVESTMENT BUSINESSES ("SIBS")

A. OVERVIEW

1. Schedule 1 of the Securities Investment Business Law (2015 revision) ("SIBL") defines securities as:
   (1) shares, or stock of any kind in the share capital of a company;
   (2) debentures, loan stock, bonds certificates of deposit and any other instrument that creates or acknowledges debt (excluding various banking and monetary instruments e.g. cheques, mortgage instruments and land charges);
   (3) warrants and other instruments which confer contractual or property rights;
   (4) options on any security and on any currency, precious metal or an option on an option;
   (5) futures, and
   (6) rights under contracts for differences (e.g. cash-settled derivatives such as interest rate and stock index futures, forward rate agreements and swaps).

2. The SIBL provides for the regulation of persons carrying on securities investment business, including the regulated activities of market makers, broker-dealers, securities arrangers, securities advisors and securities managers, in or from the Cayman Islands.

3. Pursuant to the SIBL, persons engaged in securities investment business must hold a Securities Investment Business Licence, unless the person falls in one of the categories set out in Schedule 4 of the SIBL who do not require a licence to conduct securities investment business.

4. Under the SIBL, the Monetary Authority is directly responsible for licensing, and for supervision and enforcement in respect of licensees. It is also responsible for the investigation of persons where it believes that they are, or have been undertaking securities investment business without a licence or an exemption as an Excluded Person under Section 5(2) and Schedule 4 of the SIBL to do so.

5. The Monetary Authority regulates securities investment business in accordance with:

   (1) the SIBL and its regulations, namely:
      (a) The Securities Investment Business (Licence Applications and Fees) Regulations, 2003;
      (b) The Securities Investment Business (Conduct of Business) Regulations, 2003; and

(c) The Securities Investment Business (Financial Requirements and Standards) Regulations, 2003;

(2) the relevant rules, guidance, policies and procedures issued by CIMA; and

(3) international supervisory standards issued by the International Organisation of Securities Commissions ("IOSCO").

6. The Monetary Authority's powers and duties are more particularly set out in sections 16 and 17 of the SIBL. Under Section 18, the Monetary Authority can apply to the Grand Court for injunctions and restitution and disgorgement orders.

B. SCOPE

1. The sector specific guidance contained in this section is applicable to persons carrying on "securities investment business" ("SIB") as defined in the POCL wherein SIB has the meaning assigned in the SIBL. Although not required to be licensed, persons specified In Schedule 4 of the SIBL are considered to be carrying on SIB and therefore required to comply with the AMLRs and POCL. Parts I and II and this Part (VII) of the Guidance Notes are therefore applicable to persons licensed under the SIBL and to persons specified in Schedule 4 of SIBL.

C. MONEY LAUNDERING AND TERRORIST FINANCING RISKS

1. Securities investment business activities carry a certain degree of ML/TF risks due to having exposure to factors including but not limited to:

Products and services:

(1) Securities arranging and advising may be deemed less risky than broker dealers, market makers and investment managers because a securities advisor may not be directly involved with the exchange of funds from their customers; and a securities arranger may bring two parties together to facilitate a transaction only.

(2) At times, particular activities may not involve face to face identity verification as for example phone calls to place trades may be executed by a securities investment business and/or access to remotely execute such trades may occur although identity theft, cybersecurity and pretexting may be prevalent in such circumstances.

(3) Other factors for consideration with products can be based on the complexity, liquidity, volume and value of products being bought or sold on behalf of customers. Are there ethical agreements for discretionary trading accounts between customers and security investment businesses? Are third party deposits accepted? Are credit cards accepted for payment?

(4) Full due diligence should be conducted for all parties that have outsourcing responsibilities for registered and/or licensed securities investment businesses and should be monitored on a regular basis.

Country Risk

(5) Having customers located in multiple international locations can increase the risk of money laundering and terrorist financing.

(6) Security investment businesses should be especially careful when dealing with investors who are PEPs of a foreign jurisdiction or those from a country on a sanctions list.

(7) Customers based in/controlled or owned by persons based in high risk jurisdictions should also be particularly monitored.

Customer Type/Investor Profile

(8) In addition to the country of domicile of customers, the types of individuals/entities that make up the customer base can also increase the risk of money laundering and terrorist financing.

(9) All things being equal, institutional customers from large financial institutions that are regulated and/or listed on a stock exchange could be considered less risky than investors in the form of companies and trusts with complex structures, PEPs, charities or high net worth individuals for example.

(10) Smaller institutions may have less awareness/insufficient staff to deal with potential "red flags" and/or ML/TF issues.

Source of Funds/Transparency

(11) Investments with higher return rates such as equities, derivatives and options pose a greater risk of money laundering, especially if those trades are not coming from a regulated financial institution/trading platform – i.e. OTC – or a regulated jurisdiction.

(12) Securities investment businesses must remain cognizant of, and have controls in place surrounding, types of trading activities in discretionary accounts, locations of funds and understand the risks posed by allowing such trading on their accounts.

Market Manipulation

(13) Market manipulation – tactics can be undertaken if securities investment businesses do not highly monitor the trading activities of their customers. For example, commission based trading may lead to conflicts of interest/churning tactics.

D. RISK BASED APPROACH (refer also to section 3 of Part II)

1. FSPs carrying on Securities Investment Business are required to adopt a risk-based approach to managing ML and TF risks as set out in the AMLRs and in section 3 of Part II of these Guidance Notes.

2. SIBS should pay particular attention to risk assessment factors and risk variables that are in addition to those in Part II Section 3 or which present higher risks or greater inherent risks for SIBs. Such factors and variables may include the ML/TF risk included in Section C above, the warning signs included in Section I below and other customer, product, service, transaction or delivery issues contained in these (P)art VII) SSGs.

E. SYSTEMS, POLICIES & PROCEDURES

Who is the applicant for business?

1. The applicant for business may be one of the following:

Where the *Financial Services Provider*	**Applicant for Business is**
acts as agent in buying, selling, managing, subscribing for or underwriting securities	the principal
acts as principal or makes arrangements in buying, selling, managing, subscribing for or underwriting securities	the counterparties
advises an investor or potential investor on the merits for buying, selling, managing subscribing for or underwriting securities	the investor or potential investor

Customer Due Diligence (refer also to section 4 of Part II)

When must the identity be verified?

2. The Regulations provide that there should be procedures in place requiring, as soon as reasonably practicable after contact is first made with an applicant for business, either satisfactory evidence of the applicant's identity or that steps are taken which will produce satisfactory evidence of identity.

3. The time span in which satisfactory evidence has to be obtained depends on the particular circumstances and the practicalities of obtaining evidence

before commitments are entered into between parties and before money passes.

How might identification of existing customers be carried out?

4. Refer to section 4 of Part II of these Guidance Notes.

5. If, after having conducted a risk assessment in accordance with section 4 of Part II of the Guidance Notes, verification procedures or identification of an investor have not been completed prior to the date on which a redemption is to take place, the Securities Investment Business should use the opportunity of the redemption to seek satisfactory evidence of identity.

6. Payment of the redemption proceeds should be made only to the investor and not to a third party and only when the outstanding due diligence documentation has been collected and verified.

7. If payment has been made from an account in the name of the investor with a regulated bank in the Cayman Islands or in an AMLSG List country and the criteria set out in section 4 of Part II of these Guidance Notes are adhered to, that will be sufficient evidence of identity.

8. It is important to note that the above scenarios are only permissible in circumstances where simplified due diligence is permissible.

Particular issues on Verification of identity of investors

One-off transactions.

9. Refer to section 4 of Part II of these Guidance Notes.

Payment on an Account in a Bank in the Cayman Islands or an AMLSG List country

10. Refer to section 4 of Part II of these Guidance Notes.

Enhanced Due Diligence

11. SIBs should carry out EDD in situations as stipulated in the ALMRs and or in Part II of these GNs and or where the SIB has identified or assessed that it is exposed to high ML/ FT risks. Examples of where EDD may be required include categories of customers specified in Section 4 of Part II of these Guidance Notes such as Associations, Not for Profit (Including Charities), Politically Exposed Persons (PEPs), and those from High-Risk Countries.

12. Additional examples would include cases in which a customer is confidentiality-driven, or presents a multi-layered structure of beneficial ownership for no apparent business reason, or when "red flags" are noticed.

Information that should be obtained in relation to the proposed transaction, business and source of assets in addition to that listed in the Guidance Notes.

13. Where the principal, counterparty(ies), or investor or potential investor is a natural person, sufficient information should be collected to anticipate normal business activity, including type of products required and general level of likely activity and investment goals.

14. Where the principal, counterparty(ies), or investor or potential investor is a legal person or legal arrangement, in addition to the information needed to establish normal business activity, sufficient information regarding intra-group relationships, if any; customers; service providers; and trading partners should also be collected to establish a trading profile which can be monitored against transactions.

Internal Controls and Ongoing Monitoring

15. For each investment transaction, the Securities Investment Business should record the information required under section 8 of Part II of these Guidance Notes. In addition, the Securities Investment Business should consider whether the transaction is consistent with the customer profile and customer's stated investment goals and expectations, and should also be alert to the "red flags" listed below.

16. Securities Investment Businesses must have internal reporting procedures in place to (1) identify and report suspicious activity, (2) monitor and ensure internal compliance with laws relating to money laundering, and (3) test the AML/CFT system consistent with the Regulations and the Guidance Notes ("Procedures"). Although ultimate responsibility for maintaining and implementing satisfactory Procedures remains with the Securities Investment Businesses, the obligations may be met by delegating or outsourcing those functions.

17. A Securities Investment Business may delegate any of the Procedures to a regulated person in the Cayman Islands or a person in an AMLSG List country that is subject to the AML/CFT regime of that country, consistent with the requirements of section 4 of Part II of these Guidance Notes, where applicable. The Securities Investment Business will be regarded by the Monetary Authority as being compliant with the Regulations and the Guidance Notes with respect to the Procedures if the delegate complies with the Procedures of such jurisdiction.

18. A Securities Investment Business may also delegate any or all of its obligations with respect to the maintenance of Procedures to a suitable third

party or parties, whether within or outside the Cayman Islands, provided that such appointment is consistent with the requirements of section 4 Part II of these Guidance Notes, where applicable.

19. The operators of the Securities Investment Business should document, either as a board resolution or otherwise, the manner in which the entity has met its obligation to maintain Procedures.

Record Keeping

What specific records should be kept and where?

20. Refer to section 8 and 11 of Part II of these Guidance Notes.

When may a successor Securities Investment Business Rely on the customer verification evidence obtained by its predecessor?

21. Where a successor firm is acquiring existing Securities Investment Business, the successor must ensure that the necessary due diligence has been performed prior to performing the additional transactions. It may be possible to rely upon the evidence of identity obtained by a predecessor Securities Investment Business provided that the original files, or certified copies of the original files, are transferred to the successor Securities Investment Business and the successor firm has assessed the quality of the evidence on investor identity. Where insufficient evidence exists, it may be appropriate to supplement with additional evidence to meet the standards required by these Guidance Notes.

22. At no time would it be appropriate to rely upon third parties, such as eligible introducers.

F. MT/TF WARNING SIGNS

1. It should be acknowledged that although the presence of any of the below-referenced behaviours does not necessarily indicate an inappropriate or illegal act, the Securities Investment Business should make enquiries and be satisfied with any explanations provided especially as more and more of the these activities are present.

    (1) Some of the warning signs are as follows:

        (a) customers who are unknown to the securities investment business and verification of identity / incorporation proves difficult;

        (b) customers who wish to deal on a large scale but are completely unknown to the securities investment business;

(c) customers who wish to invest or settle using cash;

(d) customers who use a cheque that has been drawn on an account other than their own;

(e) customers who change the settlement details at the last moment;

(f) customers who insist on entering into financial commitments that appear to be considerably beyond their means;

(g) customers who accept relatively uneconomic terms, when with a little effort they could have a much better deal;

(h) customers who have no obvious reason for using the services of the Securities Investment Business (e.g.: customers with distant addresses who could find the same service nearer their home base; customers whose requirements are not in the normal pattern of the service provider's business which could be more easily serviced elsewhere);

(i) customers who refuse to explain why they wish to make an investment that has no obvious purpose;

(j) customers who are introduced by an overseas agent based in a country noted for drug trafficking or distribution or a customer introduced by an overseas branch, affiliate or other service provider based in non-AMLSG List country;

(k) customers who transfer funds or shares to accounts in a non- in an AMLSG List country;

(l) customers who indulge in much activity with little or no profit over a number of jurisdictions;

(m) customers who carry out large numbers of transactions with the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction, particularly if the proceeds are also then credited to an account different from the original account;

(n) customers who purchase low grade securities in an overseas jurisdiction, sell locally and then purchase high grade securities with the proceeds;

(o) customers who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments;

(p) customers who wish to maintain a number of trustee or customers' accounts which do not appear consistent with the type of business, including transactions which involve nominee names;

(q) any transaction involving an undisclosed party;

(r) transfer of the benefit of an asset to an apparently unrelated third party, or assignment of such benefit as collateral;

(s) significant variation in the pattern of investment without reasonable or acceptable explanation.

(2) Securities investment businesses also need to be aware that their employees could be targeted by money launderers and therefore should be aware of among the other characteristics or behaviour:

(a) changes in employee characteristics (eg: lavish life styles or avoiding taking holidays), and

(b) changes in employee or agent performance, (eg: a dealer has remarkable or unexpected increase in performance).

GLOSSARY & ACRONYMS

"Account" could refer to bank accounts but should be read as including other similar business relationships between relevant financial persons and their customers e.g. insurance policies, mutual funds or other investment product, trusts or a business relationship.

"AML/CFT" means Anti-Money Laundering and Countering the Financing of Terrorism

"AMLCO" means Anti-Money Laundering Compliance Officer

"AMLRs" means Anti-Money Laundering Regulations (2017 Revision)

"AMLSG" means The Anti-Money Laundering Steering Group

"Applicant for business" means a person seeking to form a business relationship, or carry out a one-off transaction, with a person who is carrying out relevant financial business

"CDD" means Customer Due Diligence

"CIDB" means the Cayman Islands Development Bank

"CSPs" means company management and formation services professionals

"Designated person" means a person, including any subsidiary or other entity owned or controlled by that person, to whom Security Council of the United Nations anti-proliferation financing measures relates.

"DMLRO" means Deputy Money Laundering Reporting Officer

"EDD" means Enhanced Customer Due Diligence

"EI" means Eligible Introducer

"Eligible Introducer" means a person that "introduces' applicants for business to an FSP and who satisfies the conditions set out in Regulation 25 of the ALMRs i.e. a person who falls within one of the categories under regulation 22(d) and who provides a written assurance pursuant to regulation 24(2)(b)

"FATF" means Financial Action Task Force

"FATF Recommendations" or "the 40 Recommendations" means the 40 Recommendations set out in the Financial Action Task Force ("FATF") document 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation', adopted by the FATF in February 2012.

"Financial Service Providers" means, for the purpose of this document, all the persons carrying on relevant financial business specified in the Law.

"FRA" means the Financial Reporting Authority

"FSPs" means Financial Service Providers

"KYC" means Know-Your-Customer

"ML" means money laundering

"MLRO" means Money Laundering Reporting Officer

"NPOs" means non-profit organisations

"NRA" means the (Cayman Islands) National Risk Assessment

"OSP" means outsourced service provider

"PEPs" means politically exposed persons

"PFPL" means the Proliferation Financing (Prohibition) (Amendment) Law, 2016

"PTA" means Payable-Through Accounts

"PTCs" means Private Trust Companies

"RBA" means Risk Based Approach

"Relevant Financial Business" has the meaning assigned in the Proceeds of Crime Law (2017)

"SAR" means Suspicious Activity Report

"SDD" means simplified customer due diligence

"SIBL" means the Securities Investment Business Law (2015 revision)

"SIBs" means Securities Investment Businesses

"Source of Funds" refers to the origin of the particular funds or assets (for example an immediate source from which property has derived e.g. from a bank account in the name of the applicant for business or a third party) that will be used for the purposes of the business relationship or transaction (e.g. the amount being invested, deposited or remitted)

"Source of wealth" refers to the origin of the entire body of wealth (i.e. total assets). This information will usually give an indication as to the volume of wealth the customer would be expected to have, and a picture of how the customer (applicant/owner/PEP) acquired such wealth.

"Supervisory Authority" means, for the purpose of this document, the Cayman Islands Monetary Authority, the Department of Commerce and Investment and any other

supervisory authority charged with the responsibility of supervising FSPs, with respect to compliance with the ALMRs or any other regulatory laws.

"TF" means terrorist financing

"TL" means the Terrorism Law (2017 Revision)

"WMD" means weapons of mass destruction

APPENDIX A
ELIGIBLE INTRODUCER'S (ASSURANCE) FORM

Name of Eligible Introducer	
Eligible Introducers Contact details	Address:
	Email:
	Telephone number:
Name and address of Eligible Introducer's (or EI's parents) Regulatory Authority / Stock Exchange on which EI is listed	

Name of Applicant for Business (in full)	
Former name(s), trading name(s) / or any other name used where applicable	
Applicant for Business address: (residential address for individuals or place of business or registered office address for legal persons)	
Type of legal entity/arrangement (for legal persons or arrangements)	
Does the EI consider the customer to be, or associated with, a Politically Exposed Person	

The Eligible Introducer hereby confirms that it is a person who is:- *[Please tick as appropriate]*		
1	Required to comply with the regulation 5 of the AMLRs or is a majority-owned subsidiary of the relevant financial business	
2	A central or local government organisation, statutory body or agency of government in a country specified in the AMLSG List	
3	Acting in the course of a business or is a majority-owned subsidiary of the business in relation to which an overseas regulatory authority exercises regulatory functions and is based or incorporated in, or formed under the law of, a country specified in the AMLSG List. Specify which country.	
4	A company that is listed on a recognised stock exchange and subject to disclosure requirements which impose requirements to ensure adequate transparency of beneficial ownership, or majority owned subsidiary of a such company.	

	Specify which stock exchange.	
5	A pension fund for a professional association, trade union or is acting on behalf of employees of an entity referred to in 1 to 4 above.	

The Eligible Introducer also confirms that, with respect to the applicant for business that it is introducing, it has:	
(a)	identified and verified the identity of the principal and, where applicable, the beneficial owner on whose behalf the applicant may act under procedures maintained by the EI
(b)	The nature and intended purpose of the business relationship is *[provide details*]
(c)	identified the source of funds of the principal
(d)	will upon request and without any delay provide the copies of the identification and verification data or information and relevant documentation it has obtained after satisfying the CDD requirements in respect of the principal and the beneficial owner

Signature	
Name (of signatory)	
Job/position title	
Date:	
Contact details of signatory	Address:
	Email:
	Telephone:

APPENDIX B
REQUEST FOR VERIFICATION OF CUSTOMER IDENTITY

Financial Service Providers *using this form must obtain the prior consent of the customer to avoid breaching confidentiality).*

To: (Address of FSP to which request is sent)

From: (Stamp of FSP Sending the letter)

Dear Sirs,

REQUEST FOR VERIFICATION OF CUSTOMER IDENTITY

In accordance with the Cayman Islands Anti-Money Laundering Guidance Notes for Financial Services Providers, we write to request your verification of the identity of our prospective customer detailed below.

Full name of customer
_____

Title:(Mr/Mrs/Miss/Ms)
SPECIFY_____

Address including postcode (as given by customer)
_____

Date of birth:_____ Account No. (if known) _____

A specimen of the customer's signature is attached.

Please respond promptly by returning the tear-off portion below. Thank you.

To: The Manager (originating institution) From: (Stamp of sending FSP)
Request for verification of the identity of [title and full name of customer]

With reference to your enquiry dated _____ we:

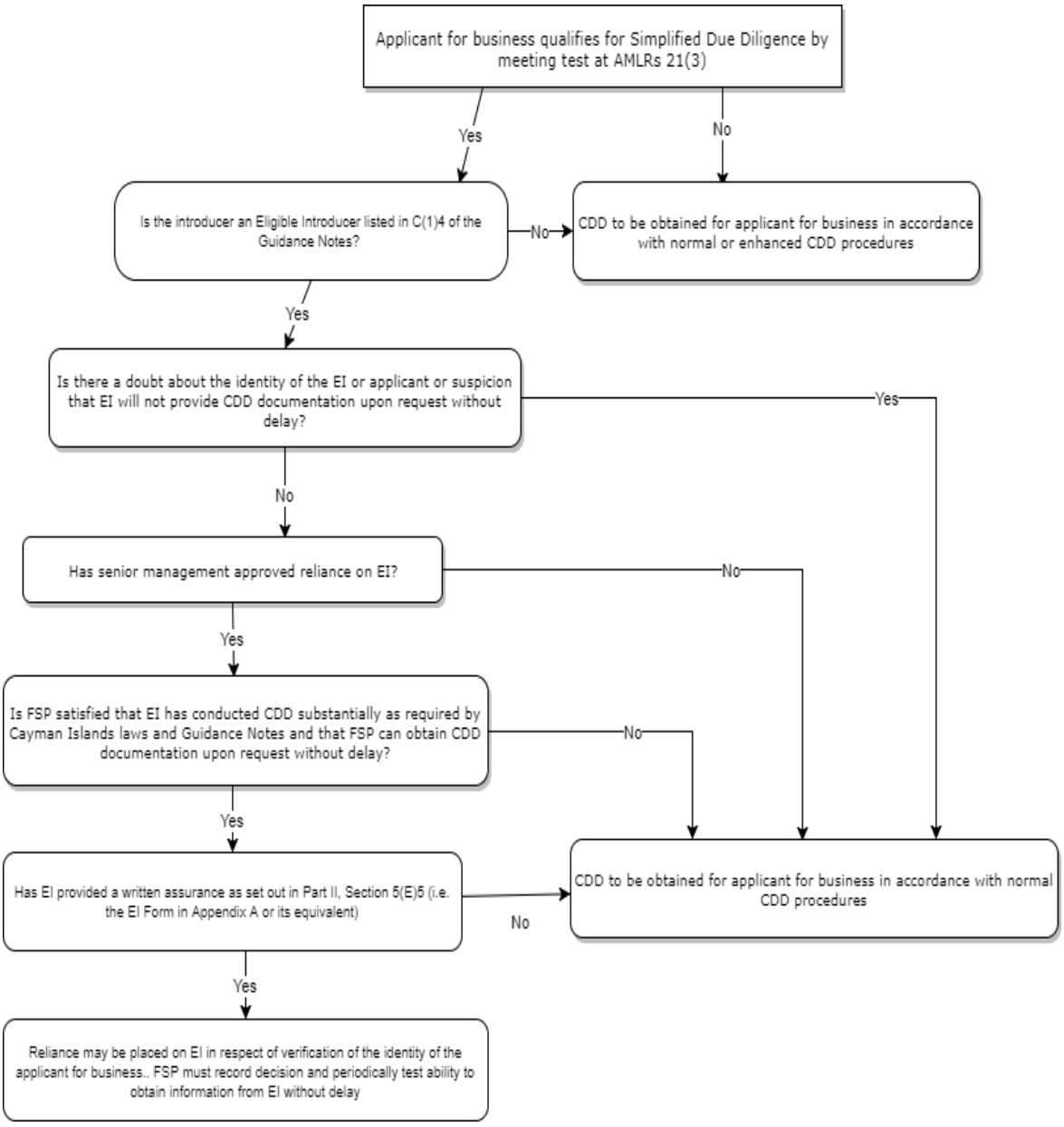
(*Delete as applicable)

1. Confirm that the above customer *is/is not known to us. If yes, for _____years.
2. *Confirm/Cannot confirm the address shown in your enquiry. If yes, the nature of evidence held is_____
3. *Confirm/Cannot confirm that the signature reproduced in your enquiry appears to be that of the above customer.

Name:_____ Signature:_____

Job Title: _____ Date: _____
The above information is given in strict confidence, for your private use only, and without any guarantee or responsibility on the part of this institution or its officials.

APPENDIX C
FLOW CHART WHERE APPLICANT IS INTRODUCED BY EI



APPENDIX D
EXAMPLES OF UNUSUAL OR SUSPICIOUS ACTIVITIES

The examples within this Appendix are not exhaustive nor are they exclusive to any one type of business. The fact that a particular kind of behaviour or type of transaction is mentioned does not of course mean that it is sinister. It may well have an entirely innocent explanation. The examples are intended to promote awareness and stimulate a culture of deterrence to money laundering.

FSPs should pay particular attention to:

Accounts

(1) Accounts that receive relevant periodical deposits and are dormant at other periods. These accounts are then used in creating a legitimate appearing financial background through which additional fraudulent activities may be carried out.

(2) A dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals that continue until the transferred sum has been removed.

(3) When opening an account, the customer refuses to provide information required by the financial institution, attempts to reduce the level of information provided to the minimum or provides information that is misleading or difficult to verify.

(4) An account for which several persons have signature authority, yet these persons appear to have no relation among each other (either family ties or business relationship).

(5) An account opened by a legal entity or an organisation that has the same address as other legal entities or organisations but for which the same person or persons have signature authority, when there is no apparent economic or legal reason for such an arrangement (for example, individuals serving as company directors for multiple companies headquartered at the same location, etc.).

(6) An account opened in the name of a recently formed legal entity and in which a higher than expected level of deposits are made in comparison with the income of the founders of the entity.

(7) The opening by the same person of multiple accounts at a bank or at different banks for no apparent legitimate reason. The accounts may be in the same names or in different names with different signature authorities. Interaccount transfers may be evidence of common control.

(8) Multiple accounts maintained or controlled by the same person into which numerous small deposits are made that in aggregate are not commensurate with the expected income of the customer.

(9) An account opened in the name of a legal entity that is involved in the activities of an association or foundation whose aims are related to the claims or demands of a terrorist organisation.

(10) An account opened in the name of a legal entity, a foundation or an association, which may be linked to a terrorist organisation and that shows movements of funds above the expected level of income.

Deposits, withdrawals or other transactions or attempted transactions

(1) Deposits for a business entity in combinations of monetary instruments that are atypical of the activity normally associated with such a business (for example, deposits that include a mix of business, payroll and social security cheques).

(2) Large cash withdrawals made from a business account not normally associated with cash transactions.

(3) Large cash deposits made to the account of an individual or legal entity when the apparent business activity of the individual or entity would normally be conducted in cheques or other payment instruments.

(4) Mixing of cash deposits and monetary instruments in an account in which such transactions do not appear to have any relation to the normal use of the account.

(5) Multiple transactions carried out on the same day at the same branch of a financial institution but with an apparent attempt to use different tellers.

(6) The structuring of deposits through multiple branches of the same financial institution or by groups of individuals who enter a single branch at the same time.

(7) The deposit or withdrawal of cash in amounts which fall consistently just below identification or reporting thresholds.

(8) The presentation of uncounted funds for a transaction. Upon counting, the transaction is reduced to an amount just below that which would trigger reporting or identification requirements.

(9) The deposit or withdrawal of multiple monetary instruments at amounts which fall consistently just below identification or reporting thresholds, particularly if the instruments are sequentially numbered.

(10) Early redemption of certificates of deposit or other investments within a relatively short period of time from the purchase date of the certificate of deposit or investment with no apparent legitimate reason. The customer may be willing to lose interest and incur penalties as a result of the early redemption.

(11) Refusal or reluctance to proceed with or a transaction after being informed that additional verification or other information (source of funds confirmation etc) is required.

(12) A non-account holder conducts or attempts to conduct transactions such as currency exchanges, the purchase or redemption of monetary instruments, etc., with no apparent legitimate reason.

(13) The customer exhibits a lack of concern regarding the costs associated with a transaction or the purchase of an investment product but exhibits undue or much interest in early termination, withdrawl or loan features of the product.

(14) Funds are received from or sent to a foreign country when there is no apparent connection between the customer and the country

Wire Transfers

(1) Wire transfers ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.

(2) Wire transfers to or for an individual where information on the originator, or the person on whose behalf the transaction is conducted, is not provided with the wire transfer, when the inclusion of such information would be expected.

(3) Use of multiple personal and business accounts or the accounts of non-profit organisations or charities to collect and then funnel funds immediately or after a short time to a small number of foreign beneficiaries.

(4) Foreign exchange transactions that are performed on behalf of a customer by a third party followed by wire transfers of the funds to locations having no apparent business connection with the customer or to countries of specific concern.

Characteristics of the customer or his/her business activity

(1) Funds generated by a business owned by individuals of the same origin or involvement of multiple individuals of the same origin from countries of specific concern acting on behalf of similar business types.

(2) Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (for example student, unemployed, self-employed, etc.).

(3) Stated occupation of the transactor is not commensurate with the level or type of activity (for example, a student or an unemployed individual who receives or sends large numbers of wire transfers, or who makes daily maximum cash withdrawals at multiple locations over a wide geographic area).

(4) Regarding non-profit or charitable organisations, financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organisation and the other parties in the transaction.

(5) A safe deposit box is opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

(6) Unexplained inconsistencies arising from the process of identifying or verifying the customer (for example, regarding previous or current country of residence, country of issue of the passport, countries visited according to the passport, and documents furnished to confirm name, address and date of birth).

Transactions linked to locations of concern

(1) Transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (for example, countries designated by national authorities; and counties where major AML/CFT deficiencies have been identified by international organisations, such as the FATF).

(2) Deposits are followed within a short time by wire transfers of funds, particularly to or through a location of specific concern (for example, countries designated by national authorities; and counties where major AML/CFT deficiencies have been identified by international organisations, such as the FATF).

(3) A business account through which a large number of incoming or outgoing wire transfers take place and for which there appears to be no logical business or other economic purpose, particularly when this activity is to, through or from locations of specific concern.

(4) The use of multiple accounts to collect and then funnel funds to a small number of foreign beneficiaries, both individuals and businesses, particularly when these are in locations of specific concern.

(5) A customer obtains a credit instrument or engages in commercial financial transactions involving movement of funds to or from locations of specific concern when there appears to be no logical business reasons for dealing with those locations.

(6) The opening of accounts of financial institutions from locations of specific concern.

(7) Sending or receiving funds by international transfers from and/or to locations of specific concern.

Financial Services Providers

The examples given for intermediaries/introducers may also be relevant to the direct business of *Financial Services Providers*. The product provider will often effectively be the counterparty of the intermediary and should be alert to unusual transactions or investment behaviour, particularly where under the Regulations the *Financial Services Provider* is relying on the intermediary/introducer for identification of the customer. The systems and procedures of the *Financial Services Providers* are geared to serving the needs of the "normal" or "average" investors, as this is the most cost-effective solution. Hence, unusual behaviour should be readily identifiable.

Particular care should be taken where:-

(a) settlement of purchases or sales involves (or appears to involve) third parties other than the investor;

(b) bearer shares (if available) are requested;

(c) bearer or unregistered securities/near-cash instruments are offered in settlement of purchases;

(d) there is excessive switching;

(e) there is early termination despite front-end loading or exit charges;

(f) they become aware that the customer's holding has been pledged to secure a borrowing in order to gear up his investment activities;

(g) they are managing or administering an unregulated collective investment scheme or pooled funds arrangement.

The routes and devices used to launder criminal money are limited only by the imagination and ingenuity of those concerned. These are only some examples of potentially suspicious transactions. FSPs are encouraged to refer also to the examples or cases issued by international bodies such as the FATF who also publish numerous typologies and also national bodies or agencies such as their own and other jurisdictional Financial Intelligence units / Financial Reporting Authorities

APPENDIX E
FSP INTERNAL (SUSPICIOUS ACTIVITY) REPORT FORM

Name of customer:	
Full account name(s):	
Account no(s):	
Date(s) of opening:	
Date of customer's birth:	
Nationality:	
Passport number:	
Identification and references:	
Customer's address:	

Details of transactions arousing suspicion: (*provide information below where known and relevant*)	
Amount (currency)	
Date of receipt	
Source(s) of funds	
Any other relevant information:	

Name of Person making report	
Whether Report made to MLRO or DMLRO	
Date of report	

For MLRO / DMLRO only

The Reporting Officer should briefly set out the reason for regarding the transactions to be reported as suspicious or, if he decides against reporting, his reasons for that decision.

MLRO/DMLRO Comments	
Further Action	