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)

[Date **]**

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 clarify, explain and in some instances amplify 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 a 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 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 PART III 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 the requirements under the AMLRs are 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 of these Guidance Notes. As such, FSPs should consider all the three 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 institutions 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, have 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, 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 a 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 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 legitimate 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 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 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 if they discover a relationship that contravenes any applicable sanctions orders. 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 highest 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 a 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 for all employees 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.

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 customers additional questions in circumstances of unusual activity. Any failure by the customer to provide credible answers will almost always give grounds for further enquiry about his activities, make the FSP reconsider the wisdom of doing business with him, 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 corporations.

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 a FSP in the Cayman Islands operates branches or controls 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

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

L. OUTLINE OF THE OFFENCES

1. The AML/CFT legislation criminalised 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 knows or has reasonable grounds to suspect that the property he 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 enters into or becomes concerned in an arrangement which he 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 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 would also constitute an indictable offence had it taken place within the Islands, that is- an offence, which is sufficiently serious to be tried in the Grand Court. This is known as the concept of dual criminality.

5. No duty is imposed on a 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. A 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.

M. OUTLINE OF THE DEFENCES

1. There are general defences enabling a defendant to prove, for example, that he 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. The Law provides that a person making a report does not put himself at risk of prosecution by continuing the relevant action (e.g. immediate execution of a transaction or a mandate), before receiving consent to do so from the authorities. Whether or not it will be appropriate for the FSP to stop the relevant transaction must depend on the circumstances.

3. 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.

4. 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.

5. A report of a suspicious activity made to the FRA does not give rise to any civil liability to the client 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.

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

N. 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, who 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 represent Supervisory Authorities' minimum expected standards as it relates to the interpretation and application of national AML/CFT measures, and although they are described as guidance, it is expected that they will be studiously complied with by FSPs. As such, 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.

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

This part of the Guidance Notes is applicable to FSPs as specified under Part I of these Guidance Notes[4]. They are to be read and applied in conjunction with the relevant Sector Specific Guidance Notes ("SSGN") that are provided in PART III.
Sections in 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] Under Part I, see section 1 "Purpose and Scope"

Section 1

GENERAL MATTERS[5]

A. INTRODUCTION

1. This part of the Guidance Notes is applicable to FSPs as specified under Part I of these Guidance Notes[6]. They are to be read and applied in conjunction with the relevant Sector Specific Guidance Notes ("SSGN") that are provided in PART III hereof.

2. Sections in 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.

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

Section 2

COMPLIANCE PROGRAMME, SYSTEMS AND TRAINING OBLIGATIONS[7]

A. INTRODUCTION

1. This section provides guidance on the systems, policies and procedures that a 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.

[7] 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 pieces of legislation 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");

   (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 the 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 the 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[8] the compliance function. 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 the 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. 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 the 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 limitations, if any, for doing so in the countries in which the other group entities operate.

[8] Where a FSP has outsourced the AMLCO function, the FSP shall refer to the Statement of Guidance on the outsourcing issued by the Monetary Authority, if applicable.

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 a 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 the 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[9]

A. THE RISK-BASED APPROACH[10]

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 risk-based approach 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 risk 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 FSPs operate;

      (c) Products, services and transactions that they offer; and

      (d) Their delivery channels[11].

[9] Part III of the AMLRs
[10] FATF R.1 and IN- 1
[11] Delivery channel in this context is the way/means whereby a 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.[12] 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[13].

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 the available information.

2. FSPs should identify and assess inherent risks they face with regard to their products, services, delivery channels, client 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

~~FATF R.1 and IN- 2 areas.~~

(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[14] 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.[15] 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

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

not intended to be comprehensive, and although they are considered to be helpful indicators, they may not be relevant in all circumstances.

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[16] 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[17].

(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

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

[17] 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.

designated terrorist organisations operating within their country.

(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 purposes.

(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 are encouraged to establish their risk tolerance. Such establishment should be done by senior management and 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 the 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.

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 the legal and regulatory requirements.[18]

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 and 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 customer, products and 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.

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.

[18] FATF R.1 and IN- 9

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 (customers or business relationships), the FSP should increase (strength or quantity) 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.

13. Additionally, FSPs shall assess the effectiveness of their risk mitigation procedures and controls, and identify areas of 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; and

(7) changes in relevant laws or regulatory requirements.

F. DOCUMENTATION

1. FSPs must document their RBA. FSPs shall update their systems as appropriate to suit the change in risks. 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 it assesses the ML/TF/PF risks;

(2) details of the implementation of the appropriate systems and procedures, including due diligence requirements, in the 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 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 that is at least annually.

G. NEW PRODUCTS AND TECHNOLOGIES

1. FSPs should have systems in place to identify and assess the 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:

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

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 and could result in FSPs not complying with the ALMRs.

4. FSPs should also:

(1) Undertake the risk assessments prior to the launch or use of such products, practices and technologies; and

(2) Take appropriate measures to manage and mitigate the risks[19].

1. 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

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

FSPs' activities. The unregulated nature of the Internet is attractive to criminals, opening up alternative possibilities for ML/TF, and fraud.

2. 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.

3. 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.

4. 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.

5. The appropriate system must embrace keeping 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[20]

A. CUSTOMER DUE DILIGENCE [21]

1. FSPs shall take steps to know who their customers are. FSPs shall not keep anonymous accounts[22] 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 customer due diligence ("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 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;

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

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

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

(5) The FSPs have 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. Two or more transactions may be related or linked if they involve the same sender or receiver.

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[23]

14. When performing CDD measures in relation to applicants that are legal persons[24] 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 powers 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 having 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.

[23] FATF- R.10 and IN 5

[24] 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[25]

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 AMLR.

20. For both the 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

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

7. It is also recognised that the guidance relating to corporate customers (other than those regulated or listed) is principally directed at relatively small,

[25] FATF- R.10 and IN 6

closely controlled private companies without substantial physical activities. 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 during the course of on-site inspections.

8. 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 other. 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.

9. There may be cases where the intermediary applicant 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 an AMLSG List country.

10. 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.

11. 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.

12. 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.

13. Whenever appropriate and practical the applicant should be interviewed personally. If the applicant fails or is unable to provide adequate evidence of 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 customer's identity and whether or not a report to the FRA ought to be made.

14. 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.

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

16. 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

17. 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.)

18. In the case of non-resident applicants, identification documents of the same sort which bear a photograph and are pre-signed by the applicant should normally be obtained. This evidence should, where possible, be supplemented by 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.

19. 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.

20. 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

21. Information and documentation should be obtained and retained to support, or give evidence to, the details provided by the applicant.

22. Identification documents, either originals or certified copies, 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

23. 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.

24. Any photocopies of documents showing photographs and signatures should be plainly legible. Where applicants put forward documents with which a 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.

25. CDD documents in electronic form are acceptable provided that the FSP has suitable documented policies and procedures are in place to ensure the authenticity. 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

26. 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.

27. If information cannot be obtained from the sources referred above to enable verification to be completed and the account to be opened, a request may be made to another institution or institutions 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

28. 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; or

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

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

30. 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.

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

32. The form in Appendix B may be used for verification of identity, to supplement the identification documentation already held, and is an alternative to the procedures specified above.

33. 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

34. A certifier must be a suitable person, such as for instance a lawyer, accountant, director or manager of a regulated entity or 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.

35. 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.

36. Where certified copy 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

37. 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**.**

Non Face-to-Face

38. 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.

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

40. 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

41. 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

42. 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 persons (if any – as ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control of the legal person or arrangement through ownership) who ultimately have a controlling ownership interest in a legal person;

(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 director, manager, general partner, president, chief executive officer or such other person who is in an equal senior management position.

43. The following paragraphs provide detailed guidance as to the required documented information concerning corporate (legal persons) customers :

(1) Certificate of Incorporation or equivalent, details of the registered office, and 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;

(9) Satisfactory evidence of identity must be established for directors, one of whom should, if applicable, be an executive director where different from account signatories.

44. Consideration should also be given to whether it is desirable to obtain a copy of the memorandum and articles of association, certificate of good standing, or by-laws of the customer.

45. Where the FSP feels that there may be additional operational or ML/TF risk, it may obtain further evidence in order to reassure itself, which might include a full list of shareholders.

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, 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. These are sometimes referred to as 'shell companies'. FSPs shall not engage in business relationship with shell companies.

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 (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 in which, for example, the general partner does not fall within the exempted category set out in this section, FSPs should obtain, where relevant:

(1) Identification evidence for at least two partners/controllers 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 should be obtained and a copy of the latest 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, if the trustee or fiduciary does not carry out adequate procedures.

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]:

(1) Trusts – the identity of the settlor, the trustee(s), the protector (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).

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

53. Where the customer or the owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies. The relevant identification data may be obtained from a public register, from the customer or from other reliable sources.

54. Particular care is needed on the part of the FSP when the applicant is a trustee or fiduciary who is not an entity listed as an "acceptable applicants" or an Eligible Introducer under the section 5 'Simplified Due Diligence Measures' of this document.

55. In such cases the FSP should normally, in addition to obtaining identification evidence for the trustee(s) and any other person who has signatory powers on the account:

[26] FATF- R.10 and IN 5

(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 private trust company (as defined in the Private Trust Company Regulations, 2013), 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).

56. In some cases it may be impractical to obtain all of the above (e.g. if the settlor has died). Discretion must be exercised but in a manner consistent with the spirit of these Guidance Notes.

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

IDENTIFICATION INFORMATION AND VERIFICATION PROCEDURES FOR NPOS (INCLUDING CHARITIES)

58. 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.

59. 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.

60. 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.

61. 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, these bodies will not hold exhaustive lists of all legitimate NPOs in those jurisdictions.

62. Whilst it is not practical to obtain documentary evidence of identity of all donors, FSPs should undertake a basic "vetting" of **foreign** NPO 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 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

63. 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

64. 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.

65. 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.

66. Where the delegate is located in a 5(2)(a) 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.

67. Where the function is sub-delegated to a person in a country that is not a 5(2)(a) country, then it is the responsibility of the FSP to ensure that the sub-delegate complies with the obligations required by the Cayman Islands.

68. Where the Compliance function is outsourced or where the managed FSP is relying on an Eligible Introducer ("EI") from another 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:

   (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.

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

(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. FSPs will need to adopt risk management procedures with respect to the conditions under which an applicant may utilise the business relationship prior to verification.

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 the 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 consider 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 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.

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

3. A 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 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. Simplified customer due diligence is unacceptable for specific higher-risk scenarios. Higher-risk scenarios may include, but are not limited to the following:

   (1) a customer is not physically present for identification purposes; or

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

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

   (4) 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 increases.

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 institutions will need to ensure they have alternative systems in place.

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 whenever there is a suspicion of ML/TF, or where specific higher-risk scenarios apply.

5. SDD is not acceptable 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.

6. Where the risks are low and where there is no suspicion of ML/TF, the AMLRs allows 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.

7. 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.

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

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, the countries listed in the Schedule 3 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 persons 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 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 (previously, known as Schedule 3 country 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

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

(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.

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 if it does not fall within the following categories:

   (1) the circumstances of the payment are such that a person handling the transaction knows or suspects that the applicant for business is engaged in ML/TF, or that the transaction is carried out on behalf of another person engaged in ML/TF;

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

   (3) onward payment is to be made in such way that it is not or does not result in a payment directly to the applicant or any other person.

3. If the payment does fall into one of the above categories then the evidence of identity of the applicant must be obtained in accordance with the full identification procedures as outlined in the previous section of this part of the Guidance Notes 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.

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

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 the 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, a 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

[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.

principal or beneficial owner, or to make the same available to the FSP on request without delay.

PROCEDURE FOR INTRODUCED BUSINESS[34]

FSPs may place reliance on the due diligence procedures of third party "Eligible Introducers" ("EI") with respect to applicants for business who are introduced by the EI and for whom the EI provides a written assurance meeting the criteria in Section 5.D.5 above confirming that they have conducted customer verification procedures substantially in accordance with the AMLRs and the Guidance Notes. The AMLRs further specify and limits EIs to a person that is listed under acceptable applicants above in C. 1. (4).

7. The FSP is ultimately responsible for ensuring that adequate due diligence procedures are followed and that the documentary evidence of the Eligible Introducer ("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.

8. Only senior management should take the decision that reliance may be placed on the EI and 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).

9. 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 and that the CDD procedures of the EI are satisfactory;

   (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;

   (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.

10. To satisfy itself that an EI can be relied upon, FSPs should obtain satisfactory evidence to identify the status and eligibility of EIs. The FSP should maintain a written record of the basis on which it determines to rely on the EI.

[34] Regulation 25 of the AMLRs

11. In the case of an overseas financial institution for instance, such evidence may comprise corroboration from the EI's regulatory authority, or evidence from the EI itself of such regulation. When considering whether it is reasonable to rely on a professional intermediary, senior management must consider the following:

    (1) whether the intermediary is a member of and in good standing within the professional body to which it belongs;

    (2) 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;

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

    (4) whether the EI is itself established and reputable.

12. 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.

13. 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.

14. 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.

15. 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. Similarly, where applicants are introduced by non-EIs, FSPs must verify the identity of the applicant.

16. The information provided by the EI should be in written form. The EI's Form in Appendix A or its functional equivalent 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 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. 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.

19. 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.

20. 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.

21. The Cayman FSP should maintain a written record of the basis on which it determines to rely on the EI Form.

22. 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.

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. 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. One-off transaction valued less than KYD 15,000 - is a one-off transaction where the amount of the (single) transaction or the aggregate of a series of linked transactions is less than CI$15,000.

3. 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.

4. 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, which 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, they 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. 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.

4. Examples of enhanced CDD measures that could be applied for higher-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.), and updating more regularly the identification data of applicant/customer and beneficial owner.

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

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

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

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

   (6) 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.

[35] Part VI of the AMLRs

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

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 on 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. FSP 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 FSP. Conducting a business relationship with 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.

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

[36] FATF R.19 and IN- 19.1

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, MoneyVal evaluations and Transparency international corruption perception index. 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.

5. 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, in particular High Risk Countries, 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 and apply 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 levels; 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 PEPs 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 (ex) PEP who is no longer a PEP. The factors that they 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. However, FSPs should ensure that core records are maintained locally.

2. 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.

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. A 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 the FSP has delegated any or all of the foregoing functions to a person or institution in an AMLSG List country then it must be satisfied that the relevant records will be maintained in accordance with the relevant requirements of the AMLRs.

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 manuals 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 Part III of the Guidance Notes gives examples of such transactions, which are not intended to be exhaustive.

6. It is recognised that where 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) to be the MLRO. In these circumstances the FSP may:

   (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

[42] Part IX of the AMLRs

whom an internal report is to be made, provided that that person has the following characteristics:

(a) is a natural person; and

(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.

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

7. 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.

8. 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.

9. Where a 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.

10. 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.

11. 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 may 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? And,

(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 activity, 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. He 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. 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. As a result, it is recommended that the MLRO 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 undue 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. FSP should develop programmes against ML/TF. 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 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.

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 arrangements for 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 outsourced 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 service provider 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 ALMRs (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 consider to:

   (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 understands 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, 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 law 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 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 and relevant internal policies. They should also receive appropriate initial and ongoing training on the 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.

[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

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 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 III of these Guidance Notes in respect of MSB. 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. A 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 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 performed 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. With respect to "payable-through accounts[51]", be satisfied that the respondent has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank.

9. FSPs should not enter into, or continue, a correspondent relationship with a "shell bank"[52]; 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.

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

11. The similar relationships to which FSPs should apply criteria 6(1) to 6(4 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.[53]

[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] 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.
[52] 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
.
[53] 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 Section 3.C, take into account any sanctions that may apply (to 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 make efforts to ensure that the 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 a FSP's monitoring to be deficient.

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)

"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

"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 a 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

"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

"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

"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 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	