Cayman Monetary Regulatory Authority International

At the forefront of financial regulation, the Cayman Monetary Regulatory Authority International (CMRAI) is dedicated to upholding the highest standards of financial oversight and compliance. Our mission is to safeguard the stability and integrity of the global financial system by ensuring that financial services operate within a framework of transparency, accountability, and excellence.

As a trusted partner to financial institutions worldwide, CMRAI provides rigorous supervision, innovative solutions, and strategic guidance to foster a secure and thriving financial environment. With decades of experience and a commitment to global standards, we stand as a pillar of trust and security in an ever-evolving financial landscape.

With a legacy of excellence in financial oversight, the Cayman Monetary Regulatory Authority International (CMRAI) is a beacon of trust in the international financial community. Our role extends beyond regulation; we are innovators, collaborators, and protectors of the global financial ecosystem. By fostering compliance, promoting best practices, and embracing technological advancements, CMRAI ensures that financial services remain resilient and adaptable in a dynamic global market.

Our comprehensive approach to regulation encompasses a deep understanding of financial risks and a proactive stance on emerging challenges. We are committed to empowering financial institutions with the tools and guidance necessary to navigate complex regulatory landscapes, thereby contributing to global economic stability and growth.

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

Issued by the Cayman Monetary Regulatory Authority International Pursuant to section 34 of the Monetary Authority Act (2020 Revision) (as amended) [February 2024] These Guidance Notes replace the Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing issued on 5 June 2020 (the GNs of 5 June 2020); and related amendments. This document is intended to establish the minimum requirements in addition to providing 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 (2020 Revision) (as amended) (AMLRs) as they relate to supervisory or regulatory guidance. Contact: Cayman Monetary Regulatory Authority International SIX, Cricket Square P.O. Box 10052 Grand Cayman KY1-1001 Cayman Islands :345-949-7089 Fax: 345-945-6131 Website: : Guidance Notes ML/TF/PF Page 3 of 245 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 Monetary Regulatory Authority International (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 establish the requirements and 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), terrorist financing (TF) and proliferation financing (PF) The 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 content of assistance. Cindy Scotland Managing Director Guidance Notes ML/TF/PF Page 4 of 245 FOREWORD

  Table of Amendments

Amendment Title	Applicable Part	Date Amended
1. Virtual Asset Service Providers Application of the Travel Rule to Part IX Section 1, Sector Specific Guidance Notes, Gazetted February 2024	Part IX	February 2024
2. e-KYC and Remote CDD/Ongoing Monitoring Provisions Gazetted 30 August 2023, Ex. Gazette No. 66/2023	Parts I, V and VII	August 2023
3. Securitization - Consolidation of Part X Sector Specific Guidance Notes (Amendment) (No.2), Gazetted May 2021, Gazette No.45/2020	Part X	May 2021
4. Virtual Asset Service Providers - Consolidation of Part IX, Sector Specific Guidance Notes (Amendment) (No.1), Gazetted February 2021, Gazette No.16/2020	Part IX	February 2021

GUIDANCE NOTES ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION 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.

5. The Guidance does not codify or amend any existing Act. Where the Guidance is incompatible

with existing Act, the Act takes precedence and prevails. 6. In the event of non-compliance with this measure by an FSP, the Authority s policies and procedures as contained in its Enforcement Manual will apply, in addition to any other powers provided in the AMLRs and the Monetary Authority Act (as amended). B. PURPOSE AND SCOPE 1. These Guidance Notes are applicable to all persons conducting relevant financial business as defined under the Proceeds of Crime Act (2020 Revision) (PoCA or the Act). For the purpose of this document, the term FSPs refers to all the persons carrying on relevant financial business specified in the Act. 2. These Guidance Notes are designed to assist FSPs in complying with the AMLRs. They are intended to supplement the AMLRs and the Acts by clarifying and Guidance Notes ML/TF/PF Page 9 of 245 explaining the general requirements of the AMLRs. It is expected therefore, that all FSPs will pay due regard to the Guidance Notes in developing an effective AML/CFT framework suitable to their business. If an FSP appears not to be doing so, the relevant Supervisory Authority will seek an explanation and may conclude that the FSP is carrying on business in a manner that may give rise to enforcement actions under the applicable legislation. 3. It is recognised that FSPs may have systems and procedures in place which, whilst not identical to those outlined in the 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, all guidance provided in relation to AML in this document are applicable to CFT. FSPs shall apply this guidance to new business relationships, existing customers and one- off transactions. 6. Throughout the 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 the 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 Monetary Authority s website) for convenience and informational purposes only. Referenced external websites are not under the control of the Monetary Authority and thus the Monetary Authority is not responsible for the contents of any external website or any link contained in, or any changes or updates to such external websites. The Monetary Authority is not responsible for any transmission received from a referenced external website. The inclusion of a reference site does not imply endorsement by the Monetary Authority of the external website, its content, advertisers or sponsors. External websites may contain information that is copyrighted with restrictions on use/reuse. Permission to use copyrighted materials must be obtained from the original source and cannot be obtained from the Monetary Authority. Guidance Notes ML/TF/PF Page 10 of 245 C. PART II AND PARTS III TO IX OF THESE GUIDANCE NOTES 1. This part of the Guidance Notes provides information on the AML/CFT

framework of the Cayman Islands. The mandatory requirements and general guidance in relation to the requirements under the AMLRs is provided under Part II of the Guidance Notes. In addition to the general guidance provided under Part II, some sector specific guidance is provided under Part III to Part IX of the Guidance Notes. As such, FSPs should consider all parts of these Guidance Notes, as appropriate. D. WHAT IS MONEY LAUNDERING? 1. ML is the process by which the direct or indirect benefit of crime is channelled through the economy/financial system to conceal the true origin and ownership of the proceeds of criminal activities. Generally, to launder criminal proceeds, a money launderer places the funds/proceeds in the financial system without arousing any suspicion, moves it in a series of complex transactions to disguise its original (criminal) source and finally, if successful, integrates it into the economy to make the funds appear to be derived legitimately. 2. For the purpose of the Guidance Notes, FSPs shall refer to the meaning of the term Money Laundering provided in the AMLRs. E. THE NEED TO COMBAT MONEY LAUNDERING 1. In recent years there has been a growing recognition that it is essential in the fight against crime that criminals be prevented, wherever possible, from legitimising the proceeds of their criminal activities by converting funds from "dirty" to "clean". 2. The laundering of the proceeds of criminal activity through the financial system is vital to the success of criminal operations. Those involved must exploit the facilities of the world's financial system if they are to benefit from the proceeds of their activities. The increased integration of the world's financial systems, and the removal of barriers to the free movement of capital, has meant that it is potentially easier for criminals to launder dirty money, and more complicated for the relevant authorities to trace. The long-term success of any of the world's financial sectors depends on attracting and retaining legitimately earned funds. The unchecked use of the financial system for laundering money has the potential to undermine FSPs, and ultimately the entire financial sector. 3. Because of the international nature and both market and geographical spread of business conducted in or from the Cayman Islands, local institutions which are less than vigilant may be vulnerable to abuse by money launderers, particularly in the layering and integration stages (see below). FSPs which, albeit unwittingly, become involved in ML/TF/PF risk the imposition of administrative fines, enforcement actions, prosecution and substantial costs both in management time and money, as well as face the severe consequences of loss of reputation.
 F. THE STAGES OF MONEY LAUNDERING 1. There is no single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g. a car, or jewellery), to passing of money through a complex international web of legitimate businesses or shell companies. Initially, however, in the case of drug trafficking and some other serious crimes such as armed robbery, the proceeds usually take the form of cash which needs to enter the financial system by some means. Street purchases of drugs are almost always made with cash. 2. Despite the variety of methods employed, the laundering process is accomplished in three stages. These may include numerous transactions by the launderers that could alert an FSP to criminal activity: (1) Placement - the physical placement of proceeds derived from criminal activity into the financial system. (2) Layering - separating the illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity. (3) Integration - the provision of apparent legitimacy to wealth derived from crime. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds. 3. The three basic steps may or may not occur

as separate and distinct phases. They may occur simultaneously or, more commonly, they may overlap. How the basic steps are used depends on the available laundering mechanisms and the requirements of the criminal organisations. Some typical examples of these three stages are listed below. Table - Stages of Money Laundering Placement Stage Layering Stage Integration Stage Cash paid into an FSP (Sometimes with staff complicity or mixed with proceeds of legitimate business) Wiring transfer abroad (often using shell companies or funds disguised as proceeds of legitimate business) False loan repayments and forged invoices used as cover for laundered money Cash exported Cash deposited in overseas banking system Complex web of transactions (both domestic and/or international) makes tracing source of funds virtually impossible Guidance Notes ML/TF/PF Page 12 of 245 Cash used to buy high value items Resale of goods or assets Income from property or legitimate business assets appears clean 4. Certain points of vulnerability have been identified in the laundering process which the money launderer finds difficult to avoid, and where his/her activities are therefore more susceptible to being recognised, such as: (1) entry of cash into the financial system; (2) cross-border flows of cash; (3) acquisition of financial assets; (4) transfers within and from the financial system; (5) incorporation of companies; and (6) establishment of financial vehicles (e.g. ostensible pooled investment funds, merchant and barter companies). G. WHAT IS TERRORIST FINANCING? 1. Terrorism is an unlawful action which is intended to compel a government or an international organisation, or intimidate the public to do or abstain from doing any act for the purpose of advancing a political, religious, racial, or ideological cause. These actions include serious violence against a person, endangering a person s life, serious damage to property, creating serious risk to public health and safety, or serious interference with or disruption to the provision of emergency services, or essential infrastructure, or to an electronic or computer system. By contrast, financial gain is the main objective of other types of financial crimes. Nonetheless, terrorist groups, like criminal organisations, must develop sources of funding, a means of laundering those funds, and a way of using those funds to obtain materials and logistical items to commit terrorist acts. 2. For the purpose of these Guidance Notes, FSPs shall refer to the meaning of terms terrorism and terrorist financing in the Terrorism Act (2018 Revision) (TA). 3. Sources of funding for terrorism could be unlawful sources such as kidnapping, extortion, smuggling, various types of fraud (e.g. through credit cards or charities), theft and robbery, and narcotics trafficking. FSPs must be aware however, that funding for terrorist groups, unlike for criminal organisations, may also include funds derived from legitimate sources or from a combination of lawful and unlawful sources. This funding from legal and legitimate sources is a key difference between terrorist groups and traditional criminal organisations. 4. Terrorist groups find ways of laundering the funds in order to disguise links between them and their funding sources, and to be able to use the funds without drawing the attention of authorities. Some of the particular methods detected with respect to various terrorist groups include cash smuggling (both Guidance Notes ML/TF/PF Page 13 of 245 by couriers or bulk cash shipments), structured deposits to or withdrawals from bank accounts, purchases of various types of monetary instruments (travellers cheques, bank cheques, and money orders/money transfers), use of credit or debit cards, and wire transfers. 5. Charities or other non-profit organisations (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 TA 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 Act 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 (UN) and European Union (EU) sanctions are implemented in the Cayman Islands by way of Overseas Orders in Council. FSPs must take actions such as filing suspicious activity reports (SAR), freezing funds, and informing the Governor as required under the relevant Acts/orders if they discover a relationship that contravenes any applicable sanctions orders or directions. For the list of applicable sanctions orders, see Sections 13 and 15 on Sanctions Compliance and Targeted Financial Sanctions 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 Acts or, where applicable, international obligations. 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. Guidance Notes ML/TF/PF Page 14 of 245 2. For the purpose of these Guidance Notes, FSPs shall refer to the meaning of term Proliferation in the Proliferation Financing (Prohibition) Act(2017 Revision), (PFPA). 3. The TA deals with matters relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. The TA 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. 4. The PFPA 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 PFPA 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 PFPA to person(s) in the financial sector and impose requirements such as conducting enhanced customer due diligence (EDD); monitoring designated persons; or restricting FSPs from entering or continuing the business

relationship with designated persons. The PFPA imposes both civil and criminal sanctions for failure to comply with the aforementioned obligations. 6. For applicable international targeted financial sanctions in relation to terrorism and, proliferation, FSPs shall refer to the websites of the Supervisory Authorities, FRA and Gazettes published by the Cayman Islands Government. I. AREAS OF CONCERN 1. No financial sector is immune to abuse, and all FSPs should consider the ML, TF and PF risks posed by the products and services that they offer, and establish appropriate systems to mitigate and manage those risks. 2. The high-risk category relates to those products or services where unlimited third party funds can be freely received, or where funds can be regularly paid to, or received from third parties without evidence of identity of the third parties being taken. Examples of products in the high-risk category are- (a)products offering money transfer facilities through chequebooks, telegraphic transfers; (b)deposits from third parties; (c)cash withdrawals by means of credit and debit cards or any other means. 3. Some of the low risk products are those in which funds can only be received from a named investor by means of a payment from an account held in the name of the investor, and where the funds can only be returned to the same account of the named investor. No third-party funding or payments are 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. Guidance Notes ML/TF/PF Page 15 of 245 possible. However, despite their apparent low risk, they are not immune from ML/TF/PF. For instance, other risk factors such as the geographical location of an FSP s customer base will also affect the ML risk and TF analysis. As such, FSPs shall consider all the relevant risks and take a risk-based approach in conducting business with their customers. Further guidance on risks and risk factors is provided in Part II of this document and the sector specific guidance. 4. While conducting the risk assessments, FSPs should also take into account the ML/TF/PF threats/risks identified in the National Risk Assessment (NRA). The Cayman Islands Government conducted a NRA in 2014/2015 and published the results which can be found at: results-of-the-mltf-national-risk-assessment-nra 5. FSPs must also consider the ML/TF/PF threats/risks identified in risk assessments conducted at the national level and by the relevant Supervisory Authority. J. NEED FOR VIGILANCE 1. All FSPs should be constantly vigilant in deterring criminals from engaging in any form of ML or TF. Although the task of detecting crime falls to law enforcement agencies, FSPs will be called upon to assist law enforcement agencies in the avoidance and detection of ML, TF and PF activities and to react in accordance with the law in the reporting of knowledge or suspicion of such. 2. Due to the diversity of FSPs, the nature and scope of their vigilance systems will vary according to the size and nature of the institution. However, irrespective of these factors, all institutions must exercise sufficient vigilance to ensure consistency with the Procedures as outlined in the AMLRs and these Guidance Notes. 3. FSPs senior management must be engaged in the decision-making processes and take ownership of the risk-based approach. Senior management must be aware of the level of ML/TF risk the FSP is exposed to and take a view on whether the FSP is equipped to mitigate that risk effectively. Staff must be adequately trained to enable them to identify suspicious activities and be trained in the internal reporting systems required for compliance with the AMLRs. 4. All FSPs must maintain and periodically review their procedural manuals relating to entry, verification and recording of customer information and reporting procedures. The frequency of review should be based on the size, nature and complexity of the FSP, however, it must be done at least

annually or where there are significant changes to the AML/CFT systems and obligations. 5. In dealing with customers the duty of vigilance starts with the commencement of a business relationship or a significant one-off transaction and continues until that relationship ends. However, retention of records upon the cessation of the Guidance Notes ML/TF/PF Page 16 of 245 relationship must be in conformity with the record keeping procedures outlined in the AMLRs and the Guidance Notes. 6. FSPs shall ask their applicants/ customers additional questions in circumstances of unusual or suspicious activity. Any failure by the applicant/customer to provide credible answers will almost always give grounds for further enquiry about his/her activities, make the FSP reconsider the wisdom of doing business with the applicant/customer, and potentially, lead to the submission of a SAR.

K. COMPLIANCE CULTURE 1. It is recognised that FSPs exist to make a profit. Nevertheless, each FSP must give due priority to establishing and maintaining an effective compliance culture. 2. The business objectives of customer care are closely aligned to the regulatory objectives of the Know-Your-Customer (KYC) principle. Similarly, linked are the philosophies behind the regulatory objectives of protecting the reputation of the Cayman Islands and the commercial desirability of protecting the reputation of individual entities. 3. In these respects, all FSPs must encourage an open and welcoming approach to compliance and AML/CFT issues amongst staff and management. 4. Where an FSP in the Cayman Islands operates branches or controlled subsidiaries, agencies or representative offices in another jurisdiction, it must have group-wide compliance programmes and comply with the relevant requirements under the AMLRs. Please see content on group-wide programmes under Section 2 of Part II of these Guidance Notes. Guidance Notes ML/TF/PF Page 17 of 245 SECTION 2 CAYMAN ISLANDS LEGISLATIVE AND REGULATORY FRAMEWORK A. INTRODUCTION 1. The Cayman Islands is committed to fighting ML, TF and PF. The Anti-Money Laundering Steering Group (AMLSG) appointed by the Cabinet is responsible for the general oversight of the AML policy of the Government and promoting effective collaboration between regulators and law enforcement agencies. Key elements of the legislative framework for the prevention of ML, TF and PF include: (1) Anti-Corruption Act (2019 Revision) (2) Penal Code (2019 Revision) (3) Proceeds of Crime Act (2020 Revision) (the Act) (4) Terrorism Act (2018 Revision) (5) Misuse of Drugs Act (2017 Revision) (6) Proliferation Financing (Prohibition) Act (2017 Revision) (7) Anti-Money Laundering Regulations (2020 Revision) (8) International Targeted Financial Sanctions and Orders B. OUTLINE OF THE OFFENCES 1. The relevant legislation criminalises ML, TF and PF and carries penalties and criminal sanctions for these offences. FSPs shall note that the commission of ML offences may lead to enforcement actions, and/or prosecution. ML offences under different Acts are listed below.

2. The ML offences under the Act, in summary: (1) Section 133 of the Act creates the offence of concealing or disguising property, which is the proceeds of criminal conduct, or converting or transferring that property or removing it from the jurisdiction. The section applies to a person s own proceeds of criminal conduct or where he/she knows or has reasonable grounds to suspect that the property he/she is dealing with represents the proceeds of another s criminal conduct. (2) Under Section 134 of the Act, a person commits an offence if he/she enters into or becomes concerned in an arrangement which he/she knows or suspects facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person. This may be by concealment, removal from the jurisdiction, transfer to nominees or otherwise. (3) The acquisition, possession or use (even temporary) of property knowing that it represents the proceeds

of criminal conduct is an offence under Section 135 of the Act. (4) According to Section 136 of the PoCA, a person commits an offence if the person fails to make a disclosure to the FRA or a nominated officer Guidance Notes ML/TF/PF Page 18 of 245 as soon as reasonably practicable after knowledge or suspicion of ML/TF, where such knowledge or suspicion is based on the information which comes to that person s attention in the course of his/her trade, profession, business or employment. Section 4(2) of Act further states that, notwithstanding any other Act 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 Act. 3. TF offences under the TA, in summary: (1) Section 19 of the TA 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 TA, 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 TA 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 TA, a person commits a ML offence if he enters into or become concerned in an arrangement that facilitates the retention or control by or on behalf of another person of terrorist property by concealment, by removal from the jurisdiction or by transfer to nominees . 4. It is not necessary that the original offence from which the proceeds stem was committed in the Cayman Islands if the conduct contravenes the law of the country in which it occurred and would also constitute an offence had it taken place within the Islands. This is known as the concept of dual criminality. 5. No duty is imposed on an FSP to inquire into the criminal law of another country in which the conduct may have occurred. However, FSP should be aware of and understand the laws of those jurisdictions in which they operate. The question is whether the conduct amounts to an indictable offence in the Cayman Islands or would if it took place in the Cayman Islands. An FSP is not expected to know the exact nature of criminal activity concerned or that the particular funds in question are definitely those which flow from the crime. C. OUTLINE OF THE DEFENCES 1. There are general defences enabling a defendant to prove, for example, that he/she did not suspect that an arrangement related to the proceeds of criminal conduct or that it facilitated the retention or control of the proceeds by the criminal. There are also specific defences provided by reporting a suspicious Guidance Notes ML/TF/PF Page 19 of 245 transaction. It will not be an offence to act in accordance with an arrangement which would otherwise be a crime if a report is made of the suspicion about the source of the funds or investment. If a disclosure of the arrangement is made before the action in question or volunteered as soon as it reasonably might be after the action, no offence is committed. 2. An employee who makes a report to his employer in accordance with established internal procedures is specifically protected by the Act in Sections 134, 135 and 136 as well as Sections 23 and 24 of the TA. 3. There is a risk that efforts to detect ML and follow the assets will be impeded by the use of alternative undetected channels for the flow of illegal funds consequent to an automatic cessation of business (because a service provider suspected that funds stemmed from illegal activity). To avoid that risk, FSPs are permitted to report their

suspicions to the FRA but continue the business relationship or transaction. In carrying out transactions where an institution is considering making a SAR, the institution should consider duties owed to third parties such as in the case of a constructive trustee. In such cases, it is recommended that independent legal advice is sought. 4. A report of a suspicious activity made to the FRA does not give rise to any civil liability to the customer or others and does not constitute, under Cayman Islands Acts, a breach of a duty of confidentiality. There are statutory safeguards governing the use of information received by the FRA. 5. To avoid tipping-off, caution must be adopted in determining what may be disclosed to a customer in the event that a report of suspicious activity is made, or information obtained about ML investigations. D. REGULATORY ACTS, RULES AND GUIDANCE 1. The regulatory Acts 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 Monetary Authority requires that FSPs (1) will understand and comply with all applicable Acts, 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 Acts, rules, or regulations. 3. FSPs that knowingly participate or assist in the violation of the laws, rules, or regulations of any jurisdiction Guidance Notes ML/TF/PF Page 20 of 245 (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. The Guidance Notes are also intended to assist FSPs in applying national AML/CFT/APF measures, and in particular, in detecting and reporting suspicious activities 3 . They embody best practices and set out the requirements and minimum criteria that the Supervisory Authorities expect FSPs to follow as it relates to the interpretation and application of national AML/CFT measures. FSPs are reminded that in deciding whether a person committed an offence under the relevant sections of the Act or complied with the AMLRs, the Courts shall consider whether that person followed any relevant supervisory guidance issued or adopted by the relevant Supervisory Authority at the time. It is expected therefore that FSPs will studiously comply with these Guidance Notes. Failure to fully comply with the obligations established herein may result in enforcement action being taken against an FSP. 5. FSPs should also be aware of the enforcement powers of the Supervisory Authorities under the Anti-Money Laundering Regulations (2020 Revision) (as amended) (AMLRs) as they relate to supervisory or regulatory guidance. 3 FATF R. 34 and Methodology 34.1 Guidance Notes ML/TF/PF Page 21 of 245 GUIDANCE NOTES ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING IN THE CAYMAN ISLANDS PART II GENERAL AML/CFT GUIDANCE Guidance Notes ML/TF/PF Page 22 of 245 SECTION 1 GENERAL MATTERS 4 A. INTRODUCTION 1. This part of the Guidance Notes is applicable to FSPs as specified under Part I of these Guidance Notes 5 . They are to be read and applied in conjunction with the relevant sector specific guidance that are provided in Part III to Part IX hereof. 2. Sections in Part II of this document are arranged to correspond with Parts in the AMLRs. However, FSPs shall take note of the fact

that such arrangement of sections is only for ease of reference and requirements and guidance for certain aspects may have been provided in different sections of this document. As such, FSPs shall consider these Guidance Notes in their entirety and adopt and comply with all relevant sections as appropriate and not restrict themselves to any particular section of these Guidance Notes. 4 Regulations 1 and 2 AMLRs 5 Under Part I, see Section 1 Purpose and Scope Guidance Notes ML/TF/PF Page 23 of 245 SECTION 2 COMPLIANCE PROGRAMME, SYSTEMS AND TRAINING OBLIGATIONS 6 A. INTRODUCTION 1. This section provides guidance on the systems, policies and procedures that an FSP shall establish and maintain to prevent and report ML/TF. The systems should be appropriate to the size of the FSP and the ML/TF risks to which the FSP is exposed. B. PROGRAMMES AGAINST ML AND TF 1. FSPs should develop and maintain AML/CFT systems and programmes which should include: (1) Customer due diligence measures; (2) Policies and procedures to undertake a Risk Based Approach (RBA); (3) Internal policies, procedures and controls to combat ML/TF, including appropriate compliance management arrangements; (4) Adequate systems to identify ML/TF risks relating to persons, countries and activities which should include checks against all applicable sanctions lists; (5) Record keeping procedures; (6) Internal reporting procedures; (7) Screening procedures to ensure high standards when hiring employees; (8) An appropriate employee training programme; (9) An audit function to test the AML/CFT system; and (10) Group-wide AML/CFT programmes. 2. Senior management of an FSP is responsible for the effective management of its business. Therefore, it is the responsibility of the senior management to ensure that appropriate systems are in place to prevent and report ML/TF/PF and the FSP is in compliance with the applicable legislative and regulatory obligations. 3. Detailed guidance on the above listed programmes are 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 Acts and obligations and prevent and report ML/TF/PF. FSPs senior management should set a culture of compliance with a top-down approach. 6 Part II of the AMLRs Guidance Notes ML/TF/PF Page 24 of 245 2. To oversee the compliance function, FSPs shall appoint an AML Compliance Officer (AMLCO) at the management level, who shall be the point of contact with the supervisory and other competent authorities. 3. Where a Supervisory Authority requires FSPs to provide notification or obtain prior approval for the appointment of an AMLCO, FSPs should comply with such requirements in the manner prescribed, if any, by the relevant Supervisory Authority. 4. AMLCOs must have the authority and ability to oversee the effectiveness of FSPs AML/CFT systems, compliance with applicable AML/CFT legislation and guidance and the day-to-day operation of the AML/CFT policies and procedures. 5. An AMLCO must be a person who is fit and proper to assume the role and who: (1) has sufficient skills and experience; (2) reports directly to the Board of Directors (Board) or equivalent; (3) has sufficient seniority and authority so that the Board reacts to and acts upon any recommendations made; (4) has regular contact with the Board so that the Board is able to satisfy itself that statutory obligations are being met and that sufficiently robust measures are being taken to protect the FSP against ML/TF risks; (5) has sufficient resources, including sufficient time and, where appropriate, support staff; and (6) has unfettered access to all business lines, support departments and information necessary to appropriately perform the AML/CFT compliance function. 6. An FSP may demonstrate clearly apportioned roles for countering ML and TF where the

AMLCO (or other audit, compliance, review function): (1) Develops and maintain systems and controls (including documented policies and procedures) in line with evolving requirements; (2) Ensures regular audits of the AML/CFT programme; (3) Maintains various logs, as necessary, which should include logs with respect to declined business, PEPs, and requests from competent authorities particularly in relation to investigations; (4) Advises the Board of AML/CFT compliance issues that need to be brought to its attention; (5) Reports periodically to the Board or Board committees (e.g. audit committee), as appropriate, on the FSP s systems and controls; and (6) Responds promptly to requests for information by the relevant competent authorities. 7. An FSP may designate its AMLCO to act as a Money Laundering Reporting Officer (an MLRO) or vice versa as far as the person is competent and has sufficient time to perform both roles efficiently. Where an individual is both an MLRO and AMLCO, that person should understand the roles and responsibilities Guidance Notes ML/TF/PF Page 25 of 245 of each function. The role of MLRO is discussed in Section 9 of Part II of this document. 8. According to the AMLRs, an FSP must designate a natural person at the managerial level as its AMLCO. However, either subsequent to or at the time of such designation the FSP may choose to delegate the performance of the compliance function to a person or rely on a person to perform the compliance function. In any event, FSPs shall not contract or transfer their compliance obligations under the AMLRs. As such, irrespective of whether the AMLCO is an employee and the FSP is performing the function on its own, or has delegated the performance of the compliance function to a person or relied on a person to perform the compliance function, the FSP is ultimately responsible for complying with the applicable AML/CFT obligations. Guidance on provisions in relation to reliance and delegation arrangements is provided in the below paragraphs. Reliance/Delegation AML/CFT Functions 9. The AMLRs allow FSPs to rely on a person to perform any function required to be formed or delegate the performance of any function to a person. Irrespective of entering into a reliance or a delegation arrangement (for the performance of any function), the FSP is ultimately responsible for compliance with the applicable requirements under the AMLRs. 10. It is a general understanding of the Monetary Authority that a person on whom reliance is being placed would apply its own procedures to perform the function in question, which is in contrast with delegation scenario. Under a delegation scenario, the delegate would usually perform the function in accordance with the FSP s procedures and is subject to the FSP s control of the effective implementation of those procedures by the delegate. 11. For example, delegation occurs in the instance where an FSP has drafted its own policies and procedures, which are then undertaken by a person on the FSP s behalf to perform the function to the FSP s exact specifications. In a reliance scenario, an FSP will assess the AML/CFT and other relevant policies and procedures of a person (on whom the FSP intends to rely to perform the function). Where the FSP is satisfied that the person s policies and procedures would enable the FSP to comply with the AML/CFT obligations of the Cayman Islands then the FSP may rely on the person to perform the function using the person s policies and procedures. 12. Since, the person on whom reliance is placed applies its own policies and procedures to perform the function, the FSP should ensure that the person s policies and procedures are consistent with the FSP s nature of business, and are adequate to comply with the applicable regulatory requirements. Where an FSP chooses to rely on a person for the performance of the compliance or any other function, the FSP shall: Guidance Notes ML/TF/PF Page 26 of 245 (1) ensure that the person on whom reliance is being placed has adequate and appropriate knowledge and expertise to

perform the function; (2) conduct a risk assessment of the person before entering into an agreement with the person upon whom reliance is to be placed and, where the person operates from a country outside the Cayman Islands, the FSP must document and demonstrate its considerations for country risk; (3) have a formalised agreement with the person on whom reliance is being placed, setting out the responsibilities of each party; (4) review policies and procedures of the person prior to entering into the reliance agreement and test them, from time to time, subsequent to entering into the relationship to ensure that the policies and procedures are adequate to perform the function and satisfy the relevant obligations in the Cayman Islands; and (5) ensure that the person adopts the Cayman Islands standards in relation to the performance of the function (for which reliance is being placed), where the person operates from a country outside the Cayman Islands in which the relevant standards are lower when compared to the Cayman Islands. 13. An FSP should ensure that the person on whom reliance is being placed has the capability to perform the function efficiently. Where the risks associated (with placing reliance on the person for the performance of the function) cannot be effectively managed or mitigated, the FSP shall not rely on the person for the performance of the function. 14. In the case of an FSP who chooses to delegate the performance of the compliance function to a person, reference should be made to the guidance on delegation principles provided under Part II, Section 10 C (Outsourcing) of the Guidance Notes. D. GROUP-WIDE PROGRAMMES 1. The AMLRs require a financial group or other person carrying out relevant financial business through a similar financial group arrangement to have group-wide AML/CFT programmes. 2. In relation to branches and majority-owned subsidiaries, FSPs shall consider conducting a gap analysis between their group-wide AML/CFT programmes and the Cayman Islands AML/CFT legislative and regulatory requirements to ensure that they, at a minimum, comply with the applicable Cayman Islands requirements. 3. The gap analysis should be conducted initially before relying on the group-wide programmes and as and when there are any changes to applicable AML/CFT obligations or group-wide programmes. Where gaps are identified during the gap analysis, FSPs shall address those by making amendments to their AML/CFT programmes, as appropriate, subject to the legislative limitations, if any, for doing so in the countries in which the other group entities operate. Guidance Notes ML/TF/PF Page 27 of 245 4. The group-wide policies should be appropriate to all branches and majority- owned subsidiaries of the FSP and include: (1) Policies and procedures for sharing information required for conducting Customer Due Diligence (CDD); (2) AML/CFT risk management policies and procedures; and (3) Adequate safeguards on the confidentiality and use of information exchanged. 5. Where the AML/CFT requirements of foreign branches and subsidiaries are less strict than those of the Cayman Islands, FSPs shall ensure that the group entities apply AML/CFT measures consistent with the requirements of this jurisdiction. 6. Where the host countries (i.e., countries in which a branch or a subsidiary of an FSP is located) do not permit the proper implementation of AML/CFT measures consistent with those of the Cayman Islands, the FSP shall inform the same to the relevant Supervisory Authority along with the appropriate additional measures that they wish to apply to manage ML/TF risks. Where the proposed additional measures are not sufficient to mitigate the risks, the Supervisory Authority may make recommendations to the FSP on further action. Guidance Notes ML/TF/PF Page 28 of 245 SECTION 3 ASSESSING RISK AND APPLYING A RISK BASED APPROACH A. INTRODUCTION 1. The purpose of this section is to provide guidance to FSPs on applying a risk- based

approach (RBA) to their anti-money laundering/countering terrorist financing (AML/CFT) framework. B. THE RISK-BASED APPROACH 7 1. The AMLRs require FSPs to apply an RBA to their AML/CFT framework. The adoption of an RBA is an effective way to prevent or mitigate money laundering and terrorist financing (ML/TF) as it will enable FSPs to ensure that AML/CFT measures are commensurate to the risks identified and allow resources to be allocated in the most efficient ways. As such, FSPs should develop an appropriate RBA for their particular organisation, structure and business activities. Where appropriate and feasible, the RBA should be articulated on a group-wide basis. 2. As is the case for an FSPs overall risk management, FSPs senior management should understand the nature and level of the risks that they are exposed to and ensure that systems and processes are in place to identify, assess, monitor, manage and mitigate ML/TF risks. ` 3. FSPs should, before determining what the level of overall risk is and the appropriate level and type of mitigation to be applied, consider 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. FSPs, in conducting their risk assessments, should take into account all relevant information from various sources which may include, but is not limited to: (1) the Cayman Islands NRA of ML/TF; (2) the NRA of other jurisdictions in which the FSPs have subsidiaries or customers; (3) sectoral risk assessments of ML/TF/PF at a national level and by the relevant Supervisory Authority; (4) reports from law enforcement agencies and the FRA; 7 FATF R.1 and IO.1 Guidance Notes ML/TF/PF Page 29 of 245 (5) rules, guidance, circulars and other communication from the Monetary Authority or other relevant authorities; (6) information from industry associations; (7) information from international standard setting bodies such as FATF; and (8) other credible and reliable sources that can be accessed individually or through commercially available databases or tools that are determined necessary by an FSP on a risk sensitive basis. 6. Following their risk assessment, FSPs should categorise their business relationships and occasional transactions according to the perceived level of ML/TF risk. Each FSP should decide on the appropriate way to categorise risk. 7. As a part of the RBA, FSPs should: (1) identify ML/TF risks relevant to them; (2) assess ML/TF risks in relation to: (a) their applicants/customers (including beneficial owners); (b) Country or geographic area in which persons under (a) above reside or operate and where the FSP operates; (c) products, services and transactions that the FSP offers; and (d) their delivery channels 8 , including remote onboarding 9 and ongoing monitoring of business relationships. (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. 8. Under the RBA, where there are higher risks, FSPs should implement 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 MF/TF. In the case of some very high-risk situations or situations which are outside the FSPs risk tolerance, the FSP may decide not to take on the applicant/customer, or to exit from the relationship. 8 Delivery channel in this context is the way/means whereby an FSP carries its business relationship and/or occasional transaction with a customer, e.g. directly or through other means such as , internet, intermediary, or any correspondent institution. 9 Remote onboarding is the establishment of new business relationships via technology solutions and non-face-to- face means where the customer is not physically present at the place where the relationship is being established. Guidance Notes ML/TF/PF Page 30 of 245 C. IDENTIFICATION AND ASSESSMENT OF RISKS 1. When identifying and assessing risk, FSPs should adopt risk assessment policies and procedures appropriate to their size, nature and complexity. ML/TF risks should be measured considering all information that is relevant and available. 2. FSPs should identify and assess the inherent and residual risks they face regarding their products, services, delivery channels, customer types, geographic locations in which they or their customers operate and any other relevant risk category. 3. 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 whether a customer issues bearer shares 10 or has nominee shareholders. 4. 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. 5. 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 weighting risk factors, FSPs must 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. When weighting risk, FSPs should ensure that: (1) weighting is not unduly influenced by any one factor; (2) economic considerations do not influence the risk rating; (3) situations do not arise where it is not possible for any business relationship to be classified as high risk; (4) situations which are identified by relevant legislation as always presenting high ML/TF risks, are not overruled by the FSPs weighting; and (5) they are able to override any automatically generated risk score, where necessary. 6. 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 applicant/customer acceptance measures, but EDD for ongoing monitoring, or vice versa. Similarly, allowing a high-risk applicant/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 applicant/customer wishes subsequently to acquire a higher risk product or service. 10 Note that bearer shares are not permitted under the Acts of the Cayman Islands. Guidance Notes ML/TF/PF Page 31 of 245 7. Customer identification and verification methods should align with the FSP s risk assessment of its customers; so the decision to onboard a customer remotely, using e-KYC methods and digital ID technologies, should be dependent on the risks presented and assessed, and, where applicable consider the application of tiered CDD. 8. Where the customer, product, service, or jurisdiction is identified as higher risk for ML/TF, the FSP should conduct additional verification measures to ensure the accuracy of

e-KYC procedures. The FSP may also consider not using e-KYC or remote onboarding for the establishment of the business relationship or for performing ongoing CDD but reverting to face-to-face interactions or reviewing original certified documents, for example. 9. 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, size and complexity of the business. D. RISK CLASSIFICATION FACTORS 1. Risk classification factors may be categorised by types of applicants/customers, countries or geographic areas, and particular products, services, transactions or delivery channels. FSPs should consider all risk factors in the assessment that is available from credible and reliable sources. Customer Risk Factors 2. When identifying the risk associated with their customers, including their customers beneficial owners, FSPs should consider the risk related to the customer s and the customer s beneficial owner s: (1) business or activity; (2) reputation insofar as it informs about the customer s or beneficial owner s financial crime risk; and (3) nature and behaviour. 3. These factors considered individually may not be an indication of higher risk in all cases, however a combination of them may warrant greater scrutiny. High-risk Classification Factors (Customer) 4. FSPs should consider the following high-risk factors when assessing customer risk with regard to: (1) customer s business or activity when: Guidance Notes ML/TF/PF Page 32 of 245 (a) the customer is connected to sectors that are commonly associated with higher ML/TF/PF, such as cash-intensive businesses; (b) the customer is a politically exposed person (PEP); (c) the customer is a public body or state-owned entity from a jurisdiction with high levels of corruption and/or organised crime; (d) the business relationship or occasional transaction is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the FSP and the applicant/customer); (e) legal persons or arrangements that are personal asset-holding vehicles; (f) companies that have nominee shareholders or shares in bearer form 11 ; and (g) the customer has a background which is inconsistent with what the FSP s records. (2) reputation insofar as it informs about the customer s or beneficial owner s financial crime risk when: (a) the customer holds a prominent position or enjoys a high public profile that might enable them to abuse this position for private gain; (b) there are adverse media reports or other relevant sources of information about the customer (e.g. there are allegations of criminality or terrorism against the customer which are reliable and credible); (c) the customer or anyone publicly known to be closely associated with them had their assets frozen due to administrative or criminal proceedings or allegations of terrorism or terrorist financing; (d) the customer has been the subject of a SAR in the past; and (e) the FSP has any in-house information about the customer integrity, obtained, during the course of the business relationship. (3) nature and behaviour, where: (a) the customer is unable to provide robust evidence of their identity; (b) the FSP has any doubts about the veracity or accuracy of the customer s identity; (c) the ownership structure of the applicant/customer appears unusual or excessively complex given the nature of the applicant/customer s business. (d) there are indications that the customer might seek to avoid the establishment of a business relationship (e.g. the customer seeks to carry out a number of separate wire transfers, or other 11 FSPs are reminded that Cayman Islands Companies are not allowed to issue shares in bearer form. Please refer to the Companies

Act for further details. As a best practice, FSPs should restrict themselves from conducting business with persons whose shares are in bearer form. Guidance Notes ML/TF/PF Page 33 of 245 services and does not open an account, where the establishment of a business relationship might make more economic sense); (e) the customer requests transactions that are complex, unusually or unexpectedly large or have an unusual or unexpected pattern without an apparent economic or lawful purpose or a sound commercial rationale; (f) the customer requests unnecessary or unreasonable levels of secrecy (e.g. the customer is reluctant to share CDD information, or appears to want to disguise the true nature of their business); (g) the customer s source of wealth or source of funds cannot be easily explained; (h) the customer does not use the products and services it has taken out as expected when the business relationship was first established; (i) the customer is a non-profit organisation whose activities could be abused for terrorist financing purposes; (j) the risk posed by the combination and complexity of products, services and delivery channels that the applicant/customer uses; (k) the risk posed by the geographical location of the applicant/customer (e.g. countries in which the applicant/customer (and its beneficial owner) resides or from which it operates); and (l) the risk posed by the customer s characteristics, nature and purpose of the relationship or nature of transaction. Low-Risk Classification Factors (Customer) 5. When assessing customer risk factors, FSPs may consider the low-risk classifications for applicants/customers that satisfy the requirements under Regulation 22 1 (d) of the AMLRs. Country/Geographic Risk Factors 6. Country/geographic risk, in conjunction with other risk factors, provides useful information as to potential ML/TF risks. FSPs should consider jurisdictions they are exposed to, either through their own activities or the activities of customers, especially jurisdictions with relatively higher levels of corruption or organised crime, and/or deficient AML/CFT controls and listed by FATF. High-risk Classification Factors (Country/geographic area) 7. When identifying higher risks relating to country/geographic areas, FSPs should consider: (1) whether the country has been identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow- up reports by international bodies such as the FATF, as not having adequate AML/CFT systems; (2) whether the country is subject to sanctions, embargos or similar measures issued (e.g., sanctions imposed by the UN); Guidance Notes ML/TF/PF Page 34 of 245 (3) whether the country or geographic area has been identified by reliable and credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their jurisdiction; (4) the nature and purpose of the customer s business relationship within the jurisdiction; (5) the level of ML/TF risk within the jurisdiction; (6) the level of predicate offences relevant to money laundering within the jurisdiction; and (7) the level of legal transparency and tax compliance within the jurisdiction. Low-risk Classification Factors (Country/geographic area) 10. In identifying lower risks relating to country/geographic areas, FSPs may consider: (1) countries identified by reliable and credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems; and (2) countries identified by credible sources as having a low level of corruption or other criminal activity. Product, Services and Delivery Channels Risk Factors 11. The overall risk assessment of an FSP should include determining the potential risks presented by products, services and delivery channels it offers. When assessing the risk associated with their products, services or transactions, FSPs must consider the level of transparency, or opaqueness, the product, service or transaction affords; the complexity of the product, service or transaction; and the value or size of the

product, service or transaction. 12. When identifying the risk associated with delivery channels, FSPs should consider the risk factors related to the business relationship and/or occasional transaction conducted on a non-face to face basis; and any introducers or intermediaries it utilises and the nature of those relationships. Risk Assessment of Technology Solutions 13. FSPs should consider the basic components of the technology solution including digital ID/e-KYC 12 systems and take an informed risk-based approach to relying on these when conducting remote non-face to face onboarding or ongoing monitoring of business relationships. This includes understanding a chosen system s assurance levels 13 and ensuring that those levels are appropriate to 12 A digital ID a system that covers the process of identity proofing/enrolment and authentication. Identity proofing and enrolment can be either digital or physical (documentary), or a combination, but binding, credentialing, authentication, and portability/federation must be digital.- FATF Guidance on Digital ID, 2020 E-KYC refers to the processes whereby a customer s identity is verified via electronic means. 13 Assurance levels measure the level of confidence and accuracy in the reliability and independence of a digital ID system and its components. Guidance Notes ML/TF/PF Page 35 of 245 the assessed ML/TF risks of the scenarios/cases to which the system is being used. FSPs must ensure the level of assurance is adequate for the jurisdiction, product, customer and other relevant risk factors. 14. FSPs should carry out formal risk assessments of the new technology solution, including e-KYC/digital ID systems which include documented consideration of how the proposed system works, the level of assurance that it provides, and any particular risks associated with it,inter alia,accuracy of the underlying information and/or technology, appropriateness of the application for the licensee's client base (i.e. some applications are aligned to verify identification within a specific region),timeliness of the applications' updates (i.e. sanctions lists),evaluation of the resilience and cyber security measures of the application ,storage of personal information etc. 15. The use of video-conferencing 14 , as with other forms of non-face-to-face measures must be in accordance with a risk-based approach. FSPs should put in place appropriate controls during the video-conferencing process to verify the identity and authenticity of the ID documents presented. If an eligible introducer or suitable certifier has met the customer, they must confirm to the FSP that they have met the customer via video-conferencing, including a photograph of the customer or scanned copy of the certified documents. 16. Customer identification and verification that rely on reliable independent e- KYC/digital ID systems with appropriate risk mitigation measures in place that meet ISO/IEC technical global standards for digital ID systems may present a standard level of risk, and may even be lower-risk where higher assurance levels are implemented and/or appropriate ML/TF risk control measures, such as product functionality limits, are present. 17. FSPs shall adopt appropriate anti-fraud and cybersecurity measures to support e-KYC/digital ID technology systems, such as authentication systems for CDD purposes 15 . High-risk Classification Factors (Products, services and delivery channels) 18. When assigning high risk ratings relating to products, services and delivery channels, FSPs should consider: (1) the level of transparency, or otherwise of the product, service or transaction (e.g., the extent to which the products or services facilitate or allow anonymity or opaqueness of the customer, ownership or beneficiary structures that could be used for illicit purposes); 14 Video-conferencing is live, visual and audio method of communication connection between two or more remote parties over the internet that simulates a face-to-face meeting. Video-conferencing is an e-KYC mechanism and is not considered face-to-face. 15 For

example, FSPs could utilise safeguards built into digital ID systems to; prevent fraud to feed into systems, conduct ongoing due diligence on clients and business relationship, and monitor, detect and report suspicious transactions to relevant authorities. Guidance Notes ML/TF/PF Page 36 of 245 (2) non-face-to-face business relationships 16 and/or occasional transactions when other high-risk factors have been identified. (3) payments received from unknown or un-associated third parties; (4) the value or size of the product, service or transaction (e.g. the extent that the products or services may be cash intensive, or the extent that the products or services facilitate or encourage high value transactions); (5) the complexity of the product, service or transaction, including the use of new technologies or payment methods; (6) whether, in the case of insurance products/services, there is a surrender of single premium life product or other investment-linked insurance products with a surrender value; (7) enhanced scrutiny of other activities, products or services such as 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 (Products, services and delivery channels) 19. In assigning lower risk classifications relating to products, services and delivery channels, FSPs may consider: (1) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion 17 purposes; (2) products and services that do not encourage early surrender options (e.g. in the case of insurance policies for pension schemes); (3) products that cannot be used as collateral; and (4) products that with strict rules that do not permit the assignment of a member s interest (e.g. a pension, superannuation or similar scheme, where contributions are made by way of deduction from wages). 20. The examples of risk factors/indicators outlined are not intended to be comprehensive, and although they are considered to be helpful indicators, they may not be relevant in all circumstances. 16 Non-face-to-face business relationship at the establishment of a business relationship or the carrying out of transaction where the customer is not physically present at the place where the relationship is being established or transaction is conducted. 17 In general terms, financial inclusion involves providing access to an adequate range of safe, convenient and affordable financial services to disadvantaged and other vulnerable groups, including low income, rural and undocumented persons, who have been underserved or excluded from the formal financial sector. Financial inclusion also involves making a broader range of financial products and services available to individuals who currently only have access to basic financial products. Financial inclusion can also be defined as ensuring access to appropriate financial products and services at an affordable cost in a fair and transparent manner. For AML/CFT/PF purposes, it is essential that these financial products and services are provided through financial institutions subject to adequate regulation in line with the FATF Recommendations. Examples of such products/services can include basic/low amount savings accounts, school children savings accounts. For additional information see the FATF s Guidance Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion. Guidance Notes ML/TF/PF Page 37 of 245 E. 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 applicant/customer exceed its risk tolerance, it may decide not to accept or

maintain that particular type of applicant/customer(s). Conversely, if the risks associated with a particular type of applicant/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 applicant/customer(s). 2. FSPs should establish their risk tolerance. Such establishment should be done by senior management and the Board. In establishing the risk tolerance, the FSP must identify the risks that it is willing to accept and the risks that it is not willing to accept. It must consider whether it has sufficient capacity and expertise to effectively manage the risks that it decides to accept. 3. When establishing the risk tolerance, an FSP should consider consequences such as legal, regulatory, financial and reputational consequences of an AML/CFT/PF 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 at the national level. Sources for this information may include NRA Reports or other similar reports including risk assessments conducted by the relevant Supervisory Authority such as the Monetary Authority s Combined 2019 Sectoral Risk Ratings. They should monitor the implementation of those controls and enhance them, if necessary. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with legal and regulatory requirements. 18 6. The policies and procedures designed to mitigate assessed ML/TF/PF risks should be appropriate and proportionate to these risks and should be designed to provide an effective level of mitigation. 18 FATF R.1 and IO- 1 Guidance Notes ML/TF/PF Page 38 of 245 7. The nature and extent of AML/CFT/PF controls will depend on a number of aspects, which include: (1) the nature, scale and complexity of the FSP s business; (2) diversity, including geographical diversity of the FSP s operations; (3) FSP s applicant/customer, product and activity profile; (4) volume and size of transactions; (5) extent of reliance or dealing through third parties or intermediaries. 8. Some of the risk mitigation measures that FSPs may consider include: (1) determining the scope of the identification and verification requirements or ongoing monitoring based on the risks posed by particular customers, products or a combination of both; (2) setting transaction limits for higher-risk customers or products; (3) determining the circumstances under which they may refuse to take on or terminate/cease high risk customers/products or services; (4) determining the circumstances requiring senior management approval (e.g. high risk or large transactions, when establishing relationship with high risk applicants/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. Residual risk is the risk remaining after taking into consideration the risk mitigation measures and controls. Residual risks must be in line with the FSP s overall risk tolerance. Where the FSP finds that the level of residual risk exceeds its risk tolerance, or that its risk mitigation measures do not adequately mitigate high risks, the FSP should enhance the risk mitigation measures that are in place. F. MONITORING AML/CFT SYSTEMS AND CONTROLS 1. FSPs should have systems in place to monitor the risks identified and assessed as they may change or evolve over time due to certain changes in risk factors, which may include changes in customer conduct, development of new technologies, new embargoes and new sanctions. FSPs should update their systems as appropriate to suit the change in

risks. 2. Additionally, FSPs should assess the effectiveness of their risk mitigation policies, procedures and controls, and identify areas for improvement, where needed. For that purpose, the FSP will need to consider monitoring certain aspects which include: (1) the ability to identify changes in a customer profile or transaction activity/behaviour, which come to light in the normal course of business; (2) the potential for abuse of products and services by reviewing ways in which they may be used to facilitate ML/TF/PF purposes, and how these ways may change, supported by typologies/law enforcement feedback, etc.; Guidance Notes ML/TF/PF Page 39 of 245 (3) the adequacy of staff training and awareness; (4) the adequacy of internal coordination mechanisms, that is, between AML/CFT compliance and other functions/areas; (5) the compliance arrangements (such as internal audit or external review); (6) the performance of third parties who were relied on for CDD purposes; (7) changes in relevant Acts or regulatory requirements; and (8) changes in the risk profile of countries to which the FSPs or its customers are exposed to. G. NEW PRODUCTS AND TECHNOLOGIES 1. FSPs should have systems in place to identify and assess ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products such as: (1) digital information storage including cloud computing; (2) digital or electronic documentation storage; (3) electronic verification of documentation; (4) digital ID system/technology solutions; (5) data and transaction screening systems; or (6) the use of virtual or digital currencies. 2. FSPs should have robust documented policies and procedures in place to ensure a consistent and adequate approach to relying on new digital ID system/technology solutions for CDD purposes. These may include (but are not limited to): a. A tiered CDD approach that leverages the new technology solutions with various assurance levels; b. Policies for the secure electronic collection and retention of records by the new technology solutions; c. A process for enabling authorities to obtain from the new technology solutions the underlying identity information and evidence needed for identification and verification of individuals; d. Anti-fraud and cybersecurity processes to support e- KYC/digital ID proofing and/or authentication for AML/CFT efforts resulting from the new technology solutions; e. Back-up plans for possible instances where the new technology solution fails; f. A description of risk indicators that would prompt a FSP to refrain from utilising new digital ID system/technology solutions; and g. Procedures for the regular, ongoing and independent review 19 of the effectiveness of the new systems and processes used. 19 Carried out by internal audit or any other control function as defined within Rule: Corporate Governance for Regulated Entities Guidance Notes ML/TF/PF Page 40 of 245 3. 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/PF measures because of the remote access by customers of the systems. 4. Systems utilising new technologies that are involved with the collection, monitoring or maintenance of customer information for example, may not be as reliable or work as expected or may not be fully understood by staff. Such systems could therefore be vulnerable and result in FSPs not complying with the AMLRs. 5. FSPs should also: (1) undertake a risk assessment prior to the launch or use of such products, practices and technologies; and (2) take appropriate measures to manage and mitigate the risks.20 6. 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/PF schemes, particularly those technologies that favour anonymity. Banking and investment business on the Internet, for example, add a new dimension to FSPs' activities. The unregulated nature of the Internet is attractive to criminals, opening up alternative possibilities for ML/TF/PF, and fraud. 7. It is recognised 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 that account in a way which would dispense with or bypass normal identification procedures. 8. 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. 9. 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/PF schemes. This may involve reviewing papers from international bodies such as the FATF on AML/CFT/PF typologies, warnings and information issued by regulators and law enforcement, as well as information issued by industry bodies or trade associations. 20 FATF- R. 15 and Methodology 15.1 and 15.2 Guidance Notes ML/TF/PF Page 41 of 245 10. To maintain adequate systems, FSPs should ensure that their systems and procedures can be and are kept up to date with such developments and the potential new risks and impact they may have on the products and services offered by the FSPs. Risks identified must be fed into the FSPs business risk assessment. H. EMERGING RISKS 1. FSPs should ensure that they have systems and controls in place which identify and assess emerging ML/TF/PF risks and incorporate them into their assessments in a timely manner. Where an FSP is aware that a new risk has emerged, or an existing risk has increased or otherwise changed, the changes should be reflected in the risk assessment as soon as possible. I. DOCUMENTATION 1. FSPs must document their RBA. Documentation of relevant policies, procedures, review results and responses should enable the FSP to demonstrate to the relevant Supervisory Authority, competent authorities and/or to a court: (1) risk assessment systems including how the FSP assesses ML/TF/PF risks; (2) details of the implementation of appropriate systems and procedures, including due diligence requirements, in light of its risk assessment; (3) how it monitors and, as necessary, improves the effectiveness of its systems and procedures; and (4) the arrangements for reporting to senior management and the Board on the results of ML/TF/PF risk assessments and the implementation of its ML/TF/PF risk management systems and control processes. J. REVIEW OF THE RISK ASSESSMENT 1. The AML/CFT risk assessment should be subjected to regular reviews to ensure that it adequately reflects the ML/TF risks pertaining to the FSP. FSPs should also assess information obtained as part of their ongoing monitoring business relationships and consider whether this affects the risk assessment. It is the expectation of the Monetary Authority that these reviews are approved by senior management and by the Board of the FSP. Guidance Notes ML/TF/PF Page 42 of 245 SECTION 4 CUSTOMER DUE DILIGENCE 21 A. CUSTOMER DUE DILIGENCE 22 1. FSPs shall take steps to know who their customers are. FSPs should not keep anonymous accounts 23 or accounts in fictitious names. FSPs are not allowed to open or maintain numbered accounts. A numbered

account is an account that is not in the name of a customer and is managed with a number assigned to the underlying customer. 2. FSPs shall take steps to ensure that their customers are who they purport themselves to be. FSPs shall conduct CDD which comprises of identification and verification of customers including beneficial owners, understanding the intended nature and purpose of the relationship, and ownership and control structure of the customer. 3. CDD measures involve: (1) Identifying the applicant or customer and verifying that identity using reliable, independent source documents, data or information. (2) Identifying the beneficial owner(s) (of the applicant/customer and beneficiaries, where appropriate), and taking reasonable measures to verify the identity of the beneficial owner, such that it is satisfied that it knows who the beneficial owner is. 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; (3) Carrying out one-off transactions that are wire transfers; (4) There is a suspicion of ML/TF; or (5) There are doubts as to the veracity or adequacy of the previously obtained customer identification information. 21 Part IV of the AMLRs (2020 Revision) 22 FATF-R.10 and IN 1 to 3 23 Example - Bearer shares Guidance Notes ML/TF/PF Page 43 of 245 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 Act and the AMLRs. 6. FSPs shall monitor transactions to determine whether they are linked. One-off transactions could be deliberately restructured into two or more transactions of smaller values to circumvent the applicable threshold (KYD 15,000). As such, FSPs should be vigilant and pay special attention to one-off transactions to ascertain if they are linked and exceed the set threshold. Guidance on one-off transactions is provided under Section 5 of these Guidance Notes. 7. FSPs shall verify the identification of an applicant/customer using reliable independent source documents, data or information. For verification purposes, FSPs may use independent sources such as company registries, World Check (or similar internationally accepted screening databases), Regulatory Data Corp (RDC), and Google. 8. Similarly, FSPs shall identify and verify the applicant s beneficial owner(s) to ensure that the FSP understands who the ultimate beneficial owner is. 9. FSPs shall ensure that they understand the purpose and intended nature of the proposed business relationship or transaction. FSPs shall assess and ensure that the nature and purpose are in line with its expectation and use the information as a basis for ongoing monitoring. 10. The AMLRs require FSPs to identify and verify the identity of any person that is purporting to act on behalf of the applicant/customer (authorised person). The FSP should also verify whether that authorised person is properly authorised to act on behalf of the applicant/customer. 11. FSPs shall conduct CDD on the authorised person(s) using the

same standards that are applicable to an applicant/customer. 12. Additionally, FSPs shall ascertain the reason for such authorisation and obtain a copy of the authorisation document. 13. FSPs shall conduct ongoing monitoring of their business relationship with their customers. Ongoing monitoring helps FSPs to keep the due diligence information up-to-date, and review and adjust the risk profiles of the customers, where necessary. Guidance Notes ML/TF/PF Page 44 of 245 CDD- For Legal Persons and Arrangements 24 14. When performing CDD measures in relation to applicants that are legal persons 25 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 (guidance on the identification and verification procedures are provided in the latter part of this section). 15. The purpose of the requirements set out regarding the identification and verification of the applicant and the beneficial owner is twofold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the applicant to be able to properly assess the potential ML/TF risks associated with the business relationship; and second, to take appropriate steps to mitigate the risks. 16. As two aspects of one process, these requirements are likely to interact and complement each other naturally. In this context, FSPs should: (1) Identify the applicant and verify its identity. The type of information that would normally be needed to perform this function would be: (a) Name, legal form and proof of existence verification could be obtained, for example, through a certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust, or other documentation from a reliable independent source proving the name, form and current existence of the customer. (b) The constitutional documents that regulate and bind the legal person or arrangement (e.g. the memorandum and articles of association of a company), as well as the names of the relevant persons holding a senior management position in the legal person or arrangement (e.g. directors, senior managing directors in a company, trustee(s) of a trust). (c) The address of the registered office, and, if different, a principal place of business. (d) When verifying customers that are corporate legal persons, regulated entities may use publicly available sources, including company registries. 17. The use of video-conferencing to onboard customers who are corporate legal persons or legal arrangements (trusts, foundations) may be used to identify natural persons such as directors and officers, ultimate beneficial owners, settlors or grantors, trustees, protectors, enforcers or those appointed to act on behalf of the customer. 24 FATF- R.10 and IN 5 25 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 organisations, that can take a variety of forms which vary between jurisdictions, such as foundations, associations, or cooperative societies. Guidance Notes ML/TF/PF Page 45 of 245 18. FSPs who are unable to verify official constitutive or formation documents such as certificates of incorporation, constitution or memorandum and articles of association and trust deeds presented during video-conferencing or via other electronic methods due to unavailability of public sources must seek alternative measures to verify the documentation. This may include obtaining an original certified true copy or accepting soft copies digitally signed by a suitable certifier attesting to the authenticity of the documents. 19. 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 26 20. 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. 21. The information collected should be recorded and maintained in accordance with the requirements for record-keeping under Part VIII of the AMLRs. 22. For both cases referred to above, the verification of the identity of the beneficiary(ies) should occur at least at the time of the pay-out. 23. The beneficiary of a long-term insurance policy should be included as a relevant risk factor by the FSP in determining whether EDD 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 EDD measures should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of pay-out. B. IDENTIFICATION INFORMATION AND VERIFICATION PROCEDURES 1. When considering entering into a business relationship, certain principles should be followed when ascertaining the level of identification and verification checks to be completed. 26 FATF- R.10 and IN 6 Guidance Notes ML/TF/PF Page 46 of 245 2. It is also recognised that the guidance relating to corporate customers (other than those regulated or listed) is principally directed at relatively small, closely controlled private companies without substantial physical activities. There is a distinguishable category of large private enterprise where it may be possible to obtain satisfactory evidence of identity from public sources, in which case the process by which the identity of the customer is verified should be approved in writing by senior management of the FSP. Copies of the identification evidence should be retained and maintained and made available to the relevant Supervisory Authority upon request or during the course of on-site inspections. 3. Reasonable measures should be taken to obtain sufficient information to distinguish those cases in which a business relationship is commenced, or relevant financial business is conducted with a person acting on behalf of another. This also includes where the FSP is providing to his own customer, fiduciary or nominee services or holds funds on customer accounts which are omnibus accounts. 4. There may be cases where the intermediary applicant 27 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 which the FSP assesses as having a low degree of risk of money laundering and terrorist financing. 5. 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. 6. 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. 7. 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. 27 In this context an intermediary applicant includes a person or applicant for business who is or appears to be acting as an agent or nominee for a principal. Guidance Notes ML/TF/PF Page 47 of 245 8. 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 applicant s/customer s identity and whether or not a report to the FRA ought to be made. 9. In circumstances in which the relationship is discontinued, funds held to the order of the applicant should be returned only to the source from which they came and not to a third party save for some exceptional instances such as to comply with a court order in case of controllership. 10. 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 11. 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.) 12. In the case of non-resident applicants, original, certified or electronic identification documents of the same sort set out in 12 above which bear a photograph and are pre-signed by the applicant should normally be obtained. On a risk-based approach, this evidence should, where necessary, be supplemented by additional information such as a reference from a respected professional (e.g. attorney) with which the customer maintains a current relationship or other appropriate reference. FSPs should be aware that other identifying information when practicable, for example, a government issued Guidance Notes ML/TF/PF Page 48 of 245 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. 13. 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 UN 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. 14. 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 15. Information and documentation should be obtained and retained to support or confirm the details provided by the applicant. 16. Identification documents, either originals or certified copies, or, subject to paragraph B 27 below, legitimate electronic documentation should be pre-signed and bear a photograph of the applicant, e.g.: (1) Current valid passport(s); (2) A Cayman Islands employer ID card bearing the photograph and signature of the applicant; (3) Government issued photo bearing ID card; (4) Provisional or full drivers licence bearing the photograph and signature of the applicant; or (5) Armed Forces ID card 17. 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. 18. Any photocopies of documents showing photographs and signatures should be plainly legible. Where applicants put forward documents with which an FSP is unfamiliar, either because of origin, format or language, the FSP must take reasonable steps to verify that the document is indeed genuine, which may include contacting the relevant authorities or obtaining a notarised translation. FSP should also be aware of the authenticity of passports. 19. Verification of documents through selfie documents, photographs or videos: Photographs should be in colour and clearly show the person s face, holding the identity document in the same photograph to demonstrate it actually Guidance Notes ML/TF/PF Page 49 of 245 belongs to the customer. A clear scanned copy in colour or photograph of the identity document itself should also be provided 28 . 20. CDD documents, including government issued identification, received in electronic form are acceptable provided that the FSP takes a RBA and has suitable documented policies and procedures in place to ensure the authenticity of the electronic document(s). For further guidance, FSPs may refer to the Statement of Guidance on the Nature, accessibility and retention of records issued by the Monetary Authority, where applicable. Persons Without Standard Identification Documentation 21. 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. 22. If information and documentation set above cannot be obtained to enable verification to be completed and the account to be opened, a request may be made to another institution or institutions (for example, entities that qualify under Regulation 22(d) of the AMLRs) for confirmation of identity (as opposed to a banker s reference). Failure of that institution to respond positively and within a reasonable time should put the requesting institution on its guard. Verification of Name and Address 23. FSPs should also take appropriate steps to verify the name and address of applicants by one or more methods, for example: (1) obtaining a reference from a "respected professional" who knows the applicant; (2) checking the register of electors; (3) making a credit reference agency search; (4) checking a current local telephone directory; (5) requesting sight of a recent rates or utility bill. Care must be taken that the document is an original and

not a copy. If a document is presented in an electronic form, it may be regarded as an original if it is evident that it was issued or created in such an electronic form; or (6) personal visit to the home of the applicant where possible. 28 This refers to e-KYC measures outside of digital ID systems, as opposed to ID systems which test the authenticity of ID documents. Guidance Notes ML/TF/PF Page 50 of 245 24. The term respected professional could be applied to for instance, lawyers, accountants, directors or managers of a regulated institution, priests, ministers or teachers. 25. 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. 26. In circumstances where an applicant/customer appoints another person as an account signatory e.g. appointing a member of his/her family, full identification procedures should also be carried out on the additional account signatory. 27. The form in Appendix B may be used for verification of identity to supplement the identification documentation already held. 28. 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 29. A certifier must be a suitable person, such as for instance a lawyer, accountant, director or manager of a regulated entity/ FSP, a notary public, a member of the judiciary or a senior civil servant. Such persons are expected to adhere to ethical and/ or professional standards and exercise his or her profession or vocation in a jurisdiction that has an effective AML/CFT regime. The certifier should sign the copy document (printing his/her name clearly underneath) and clearly indicate his/her position or capacity on it together with a contact address and number. 30. 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. 31. Where certified copies of documents are accepted, it is the FSP's responsibility to satisfy itself that the certifier is appropriate. An FSP may for instance, include in its policies and procedures a list of suitable certifiers approved by senior management. In all cases, the FSP should also ensure that the customer's signature on the identification document matches the signature on the application form, mandate, or other document. Guidance Notes ML/TF/PF Page 51 of 245 Face-to-Face 32. Where possible, face-to-face customers must show FSP s staff original documents. Copies should be taken immediately, retained and certified by a senior staff member at the managerial level or a member of staff that is suitably trained. Non-Face-to-Face 33. 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 any specific risks posed by non-face-to- face 29 contact for customers at the opening of the business relationship and throughout the operation of that relationship. 34. Examples of financial business conducted on a non-face-to-face basis include internet and telephone banking, and online share dealing. 35. Where there are doubts around the

veracity of identity 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 36. 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 Direct Corporate Customers 37. With respect to legal persons, FSPs should identify the beneficial owners of the applicant and take reasonable measures to verify the identity of such persons, through the following information: (1) The identity of the natural person (if any) as ownership interests can be so diversified that there are no natural persons (whether acting alone or together) who are the beneficial owners; 29 Non-face to face business relationships the establishment of business relationships and carrying out of transactions where the customer is not physically present at the place where the relationship is being established or transaction is conducted. Guidance Notes ML/TF/PF Page 52 of 245 (2) To the extent that there is doubt under (1) as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural persons (if any) exercising control of the legal person through other means; and (3) Where no natural person is identified under (1) or (2) above, FSPs should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of the general partner, president, chief executive officer, director(s), manager(s), or such other person who is in an equal senior management position exercising control over the management of the legal person. 38. The following paragraphs provide detailed guidance as to the various acceptable documents concerning corporate (legal persons) customers. FSPs shall take a risk-based approach in determining the scope of the identification and verification documentation that is required to be collected. FSPs may need to collect several or all types of documentation and information as listed below depending on the specifics/type of the corporate applicant and risks posed: (1) Certificate of Incorporation or equivalent, details of the registered office, and, if different, a principal place of business; - (2) Explanation of the nature of the applicant's business, the reason for the relationship being established, an indication of the expected turnover, the source of funds, and a copy of the last available financial statements where appropriate; (3) Satisfactory evidence of the identity of each of the legal owners, beneficial owners and a Register of Members; (4) In the case of a bank account, satisfactory evidence of the identity of the account signatories, details of their relationship with the company and if they are not employees an explanation of the relationship. Subsequent changes to signatories must be verified; (5) Evidence of the authority to enter into the business relationship (for example, a copy of the Board Resolution authorising the account signatories in the case of a bank account); (6) Copies of Powers of Attorney, or any other authority, affecting the operation of the account given by the directors in relation to the company; (7) Obtain and verify the names and addresses of any natural persons having Powers of Attorney or the authority in (6) (8) Copies of the list/register of directors or their equivalent; (9) Satisfactory evidence of identity must be established for directors, one of whom should, if applicable, be an executive director, if where different from account signatories. FSPs shall take a risk-based

approach in determining the number of directors on whom due diligence should be conducted and document the rationale for such determination; (10) Certificate of good standing or a similar document confirming that the applicant/customer is listed in the company registry of its place of formation and has not been dissolved, struck-off, wound up or terminated; Guidance Notes ML/TF/PF Page 53 of 245 (11) A copy of the constitutional documents i.e., memorandum and articles of association, by-laws of the applicant/ customer. 39. 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. 40. Where it is impractical or impossible to obtain sight of the original Certificate of Incorporation or equivalent, an FSP may accept a suitably certified copy in accordance with the Procedures stated in paragraphs under Certification of Identification Documents of this document. 41. It is recognised that on some occasions companies may be used as a disguise for their beneficial owner. FSPs shall take reasonable measures to ensure that they are not engaged in business relationship with such entities. 42. In addition to the documents and information to be obtained in respect of corporate customers, FSPs providing a registered office for a private trust company (PTC) (as defined in the Private Trust Companies Regulations, [2020 Revision] [PTCR]), 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 PTC itself. Identification Information and Verification Procedures for Partnerships/Unincorporated Businesses 43. In the case of Cayman Islands limited partnerships and other unincorporated businesses or partnerships FSPs should obtain, where relevant: (1) Identification evidence for at least two partners/controllers, the general partner and/or authorised signatories, in line with the requirements for direct personal customers. When authorised signatories change, care should be taken to ensure that the identity of the current signatories has been verified. (2) Evidence of the trading address of the business or partnership and a copy of the latest financial report and accounts (audited where applicable). (3) An explanation of the nature of the business or partnership should be ascertained (but not necessarily verified from a partnership deed) to ensure that it has a legitimate purpose. In cases where a formal partnership arrangement exists, a mandate from the partnership authorising the opening of an account or undertaking the transaction and conferring authority on those who will undertake transactions should be obtained. Guidance Notes ML/TF/PF Page 54 of 245 Identification Information and Verification Procedures for Trust And Fiduciary Customers 44. Trusts and other fiduciary relationships can be useful to criminals wishing to disguise the origin of funds. 45. 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 30 : (1) Trusts the identity of the settlor, the trustee(s), the protector (if any), the enforcer (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership). (2) Other types of legal arrangements the identity of persons in equivalent or similar positions. 46. In cases where an applicant settlor is a trustee, in its capacity as trustee, the FSP should take the necessary steps to verify the identity of that trustee and the identity and source of funds of the settlor of the trust from which the assets originated. 47. FSPs should normally, in addition to obtaining

identification evidence for the trustee(s) and any other person who has signatory powers on the account: (1) make appropriate enquiry as to the general nature of the trust (e.g. family trust, pension trust, charitable trust etc.) and the source of funds; (2) obtain identification evidence for the settlor(s), i.e. the person(s) whose property was settled on the trust; and (3) in the case of a nominee relationship, obtain identification evidence for the beneficial owner(s) if different to the settlor(s). (4) in the case of a PTC, consider whether some or all of the documented information recommended to be obtained in respect of a corporate customer, should be obtained in respect of the PTC, save to the extent not already obtained in respect of the settlor(s). 48. In some cases, it may be impractical for the FSP to obtain all of the above (e.g. if the settlor has died) or the FSP may need some additional information depending on the risks identified. As such, FSPs shall take a risk-based approach in determining what identification and verification documentation should be obtained. 49. FSPs providing trustee services should refer to Part IV of these Guidance Notes for sector specific guidance. 30 FATF- R.10 and IN 5 Guidance Notes ML/TF/PF Page 55 of 245 Identification Information and Verification Procedures for NPOs (Including Charities) 50. 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. 51. 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. 52. 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. 53. 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, provides a list of all IRS recognized NPOs including charities; and provides a list of registered charities. For various reasons, exhaustive lists of all legitimate NPOs in those jurisdictions are not available from these bodies. 54. Whilst it is not practical to obtain documentary evidence of identity of all donors, FSPs should undertake a basic vetting of foreign NPOs and NPOs established overseas, in relation to known ML and terrorist activities. This includes a reasonable search of public information; verifying that the NPO does not appear on any terrorist lists nor has any association with ML or a high risk country and that identification information on representatives / signatories is obtained. FSPs are advised to consult the databases related to applicable sanctions. Particular care should be taken where the purposes to which the associations funds are applied are located in a high-risk country. Provision of Safe Custody and Safety Deposit Boxes 55. 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. 31 FATF- R.10 and IN 11 and 12 Guidance Notes ML/TF/PF Page 56 of 242 Managed Financial Services Providers 56. 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. 57. It is recognised, however, that a managed FSP may have to delegate AML compliance functions in accordance with the principles set out in these

Guidance Notes. There is no objection to such delegation provided that: (1) Details thereof and written evidence of the suitability of any such person or institution to perform the relevant functions on behalf of the FSP are made available to the Monetary Authority on request; (2) There is a clear understanding between the FSP and the delegate as to the functions to be performed; (3) The relevant applicant/customer information is readily available to the Monetary Authority on request and to the FRA and law enforcement authorities in accordance with the relevant procedures; and (4) The FSP satisfies itself on a regular basis as to the reliability of the delegate s systems and procedures. 65. Delegation or sub-delegation of the performance of the compliance or any other function to a person(s) should be in accordance with the principles set out in Section 10 C (Outsourcing) of the Guidance Notes. 66. Where a (managed) FSP is relying on a person for the performance of any function, the (managed) FSP should adopt the principles set out in Section 2C (under the sub-heading Reliance/Delegation AML/CFT Functions) of Part II of the Guidance Notes. But, if a (managed) FSP is relying on an EI as allowed under Regulation 25 of the AMLRs, then the (managed) FSPs should adopt the principles set out under Section 5E. (Procedure for Introduced Business) of the Guidance Notes. C. TIMING OF VERIFICATION 31 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. 32 FATF- R.10 and IN 11 and 13 Guidance Notes ML/TF/PF Page 57 of 242 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, in accordance with a risk-based approach. (2) Securities transactions. In the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed. (3) In cases of telephone or electronic business where payment is or is expected to be made from a bank or other account, the person verifying identity should: (a) satisfy himself/herself that such account is held in the name of the applicant at or before the time of payment; and (b) not remit the proceeds of any transaction to the applicant or his/her order until verification of identity has been completed. 3. The above are only examples and FSPs should adopt risk management procedures with respect to the conditions under which an applicant may utilise the business relationship prior to verification. For the avoidance of doubt, FSPs should not postpone the verification where the ML/TF risks are high and enhanced due diligence measures are required to be performed. 4. Such conditions may include restricting the funds received from being passed to third parties, imposing a limitation on the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship. 5. Alternatively, a senior member of staff at the managerial level may be given authority to allow (sign-off) for a transaction to be conducted prior to the verification. Save in exceptional

circumstances, this authority should not be delegated. Any such decision should be recorded in writing. 6. Verification, once begun, should normally be pursued either to a satisfactory conclusion or to the point of refusal. If an applicant does not pursue an application, the FSP s staff could consider that this in itself is suspicious, and they should evaluate whether a report is required. D. EXISTING CUSTOMERS 32 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 Guidance Notes ML/TF/PF Page 58 of 245 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. 3. An FSP is entitled to rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer s account is operated, which is not consistent with the customer s business profile. E. OBLIGATIONS WHERE UNABLE TO COMPLETE CDD 1. Where an FSP is unable to complete and comply with CDD requirements as specified in the AMLRs, it shall not open the account, commence a business relationship, or perform the transaction. If the business relationship has already been established, the FSP must terminate the relationship. Additionally, the FSP shall consider submitting a SAR to the FRA. F. TIPPING-OFF AND REPORTING 1. As mentioned in Part I of these Guidance Notes, the Act prohibits tipping-off. However, a risk exists that applicants/customers could be unintentionally tipped off when the FSP is seeking to complete its CDD obligations or obtain additional information in case of suspicion of ML/TF. The applicant/customer s awareness of a possible SAR or investigation could compromise future efforts to investigate the suspected ML/TF operation. 2. Therefore, if FSPs form a suspicion of ML/TF while conducting CDD or ongoing CDD, they should take into account the risk of tipping-off when performing the CDD process. If the FSP reasonably believes that performing the CDD or on- going process will tip-off the applicant/customer, it may choose not to pursue that process, and should file a SAR. FSPs should ensure that their employees are aware of, and sensitive to, these issues when conducting CDD or ongoing CDD. G. NO SIMPLIFIED DUE DILIGENCE FOR HIGHER-RISK SCENARIOS 1. FSPs should not adopt simplified due diligence measures where the ML/TF risks are high. FSPs shall identify risks and have regard to the risk analysis in determining the level of due diligence. High-risk scenarios may include, but are not limited to the following: (1) the relevant person proposes to have a business relationship or carry Guidance Notes ML/TF/PF Page 59 of 245 out a one-off transaction with a PEP; or (2) the prospective customer holds a deposit-taking licence and proposes to establish a correspondent banking relationship with the FSP; or (3) the nature of the situation is such, or a risk assessment reveals, that a higher risk of ML/TF is likely. Guidance Notes ML/TF/PF Page 60 of 245 SECTION 5 SIMPLIFIED DUE DILIGENCE MEASURES 33 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 34 or the relevant

Supervisory Authority. 35 2. While determining whether to apply SDD, FSPs should pay particular attention to the level of risk assigned to the relevant sector, type of customer or activity by the NRA or relevant Supervisory Authority. 3. The simplified measures should be commensurate with the low risk factors. Examples of possible SDD measures are: (1) Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship. (2) Reducing the frequency of customer identification updates. (3) Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold, which in any event should be based on the customer profile. (4) Relying on a third party to conduct verification of identity of applicant/customer/beneficial owner(s). 4. SDD is not acceptable in higher-risk scenarios where there is an increased risk, or suspicion that the applicant is engaged in ML/TF, or the applicant is acting on behalf of a person that is engaged in ML/TF. 5. Where the risks are low and where there is no suspicion of ML/TF, the AMLRs allow the FSPs to rely on third parties for verifying the identity of the applicants and beneficial owners. Instances where an FSP can take SDD measures and rely on third parties are discussed below. 6. FSPs may consider digital ID systems/e-KYC processes with lower levels of assurance to be sufficient for simplified due diligence in cases of low ML/TF risk. 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. 33 Part V of the AMLRs 34 In the NRA or any similar assessments conducted by the Cayman Islands 35 For example, the Monetary Authority s Combined 2019 Sectoral Risk Ratings published March 2020. Guidance Notes ML/TF/PF Page 61 of 245 B. SCHEDULE 3 OF THE MONEY LAUNDERING REGULATIONS (MLRs) 1. Schedule 3 of the MLRs (2015 Revision 36) no longer exists in the AMLRs. Subsequent to the removal of the Schedule, countries previously listed in the Schedule 3 that were considered to have equivalent AML/CFT frameworks were reflected in a list maintained and published by the AMLSG. That list was called the List of Countries and Territories Deemed to have Equivalent Legislation (the AMLSG List). 2. Subsequently, the 2020 amendments to the AMLRs removed references to the AMLSG List in Regulations 22(1) and 23(1) 37 . 3. In the absence of the AMLSG List, FSPs are expected to complete the required assessments and based on these, determine whether there is a low degree of risk of ML /TF. FSPs should take a RBA and consider other risk factors in assigning the appropriate overall risk rating. 4. FSPs may rely on particular third parties from these countries when conducting SDD as provided in the below paragraphs. C. ACCEPTABLE APPLICANTS (Applicants for whom it may be appropriate to apply SDD) 1. FSPs are required to conduct verification of identity of applicants at the time of establishing the business relationship. However, Regulation 22 of the AMLRs allows FSPs not to conduct verification where: (1) The FSP knows the identity of the applicant/customer; (2) The FSP knows the nature and intended purpose of the business relationship or one-off transaction; (3) There is no suspicious activity; and (4) The applicant/customer is a person who: (a) is required to comply with the Regulation 5 or is a majority- owned subsidiary of the relevant financial business; (b) is a central or local government organisation, statutory body or agency of government in a country assessed by the FSP as having a low degree of risk of ML/TF; (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 assessed by the FSP as having a low degree of risk of ML/TF; (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 36 The MLRs are repealed and replaced by the AMLRs 37 The amendment will apply six months after the 4 th February 2020. Guidance Notes ML/TF/PF Page 62 of 245 (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, where a person carrying out relevant financial business- (1) has assessed a low level of risk; (2) has identified a customer/applicant, and the beneficial owner (where applicable); and (3) has no reason to doubt those identities, and (1) the circumstances are such that payment is to be made by the customer/applicant; and (2) it is reasonable in all the circumstances (i) for payment to be delivered by post, in person, or by electronic means to transfer funds; or (ii) for the details of such payment to be confirmed via telephone or other electronic means; then, verification of the identity of a customer/applicant is not required at the time of receipt of payment, if the payment is debited from an account held (whether solely or jointly) in the name of the customer/applicant at a licensee under the BTCA or at a bank that is regulated in and- (i) either based or incorporated in, or (ii) formed under the laws of a country assessed by the FSP as having a low degree of risk of money laundering and terrorist financing. 2. As such, in the circumstances outlined in 1 above, the FSP may defer the verification of the applicant s/customer s identity at that time. The FSP should however, have evidence- (1) identifying the branch or office of the Bank; and (2) verifying that the account is in the name of the applicant/customer. 3. When a payment meets the criteria for the simplified measures set out in 1 above, in addition to the details of the relevant branch or office of the bank and the account name, a record should be retained indicating how the transaction arose. 4. However, such simplified measures are not allowed: (1) if the circumstances of the payment give rise to knowledge, suspicion, or reasonable grounds for knowing or suspecting that the applicant/customer is engaged in ML/TF, or that the transaction is carried out on behalf of another person engaged in ML/TF; (2) if the payment is made by a person for the purpose of opening a relevant account with a licensee under the BTCA in the Cayman Islands; and (3) in relation to the applicant/customer, when an onward payment is to be made to the applicant/customer or any other person (including the beneficial owner). 5. In the circumstances set out in paragraph 4, the verification of identity must be conducted in accordance with the CDD procedures as outlined in Section 4 of this part of the Guidance Notes before the payment of any proceeds, unless Guidance Notes ML/TF/PF Page 63 of 245 such payment of the proceeds are to be made to a person for whom a court is required to adjudicate payment (e.g. trustee in bankruptcy, a liquidator, a trustee for an insane person or a trustee of the estate of a deceased person). E. RELIANCE ON THIRD PARTIES FOR VERIFICATION OF IDENTIFICATION 1. FSPs are required under the AMLRs to maintain identification procedures that result in the production of satisfactory evidence of identity of applicants. According to the AMLRs, evidence of identity is satisfactory if it is reasonably capable of establishing that the applicant is the person he claims to be and the person who obtains the evidence is satisfied, in accordance with the procedures maintained under these regulations in relation to the FSP concerned, that it does establish that fact. 2. There are, however, circumstances in which obtaining and verifying such evidence may be unnecessary duplication, commercially onerous and of no

real assistance in the identification of or subsequent investigation into ML/TF. 3. Where the risks are low and where there is no suspicion of ML/TF, subject to certain conditions FSPs may rely on third parties for verification of identification of applicants and beneficial owners. Applicants Who Are Nominees or Agents for a Principal 38 4. FSPs may rely on applicants who are or appear to be acting as nominees or agents for their principals for the verification of identity of the principals (or beneficial owners). However, the applicant should be a person who falls within the categories listed under an acceptable applicant listed in paragraph C.1.(4) above 39 . 5. Furthermore, an FSP shall not rely on the applicant unless the applicant provides a written assurance confirming that: (1) The applicant has identified and verified the identity of the principal and, where applicable, the beneficial owner on whose behalf the applicant may act; (2) The nature and intended purpose of the business relationship; (3) The applicant has identified the source of funds of the principal; and (4) The applicant will upon request by the FSP provide the copies of the identification and verification data or information and relevant documentation without any delay after satisfying the CDD requirements in respect of the principal and the beneficial owner. 6. Furthermore, an FSP who is bound by Regulation 5 and who relies on the written assurance provided as specified above by the applicant is liable for any failure of the applicant to obtain and record the evidence of identity of the principal or 38 Regulation 24 of the AMLRs 39 Regulation 22 of the AMLRs specifies who could be acceptable applicants for whom FSPs may apply SDD and not conduct verification. Guidance Notes ML/TF/PF Page 64 of 245 beneficial owner, or to make the same available to the FSP on request without delay. Procedure For Introduced Business 40 7. FSPs may place reliance on the due diligence procedures of third party 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 E.5 above confirming that it has conducted customer verification procedures substantially in accordance with the AMLRs and the Guidance Notes. The AMLRs further specify and limit EIs to a person that is listed under acceptable applicants above in C. 1.(4). 8. The FSP is required to ensure that adequate due diligence procedures are followed and that the documentary evidence of the EI that is being relied upon is satisfactory for these purposes. Satisfactory evidence is such evidence as will satisfy the AML/CFT regime in the country from which the introduction is made subject to E.7 above. 9. Only senior management should take the decision that reliance may be placed on the EI. The basis for deciding that normal due diligence procedures need not be followed should be part of the FSP s risk-based assessment and should be recorded and the record retained in accordance with the AMLRs. (See Appendix C for Introduced Business Flow Chart). 10. The FSP should not enter into a relationship with or rely on an EI if the FSP: (1) knows or suspects that the EI, the applicant or any third party on whose behalf the applicant is acting is engaged in ML/TF; (2) has any reason to doubt the identity of the applicant, the EI or beneficial owner; and (3) is not satisfied that CDD information or documentation will be made available upon request without any delay. 11. Where a relationship presents higher ML/TF risk, FSPs must consider whether it is appropriate to rely solely upon the EI or the terms of business provided by the EI containing the necessary information. 12. The decision of senior management that reliance may be placed on the EI is not static and should be assessed regularly to determine whether there is a reason that the relationship should be discontinued. 13. FSPs that depend on EIs must take steps to satisfy themselves that: (1) each person that they have so identified meets the criteria of an EI as set out above; (2) the information provided clearly establishes that the identity of the

applicant (or any beneficial owner) has been verified; 40 Regulation 25 of the AMLRs Guidance Notes ML/TF/PF Page 65 of 245 (3) the level of CDD carried out is made known and that the CDD procedures of the EI are satisfactory; and (4) the EI will make available, on request without delay, copies of any identification and verification data and relevant documents on the identity of the applicants (and any beneficial owners) obtained when applying CDD measures. 14. In the case of 13 (1) above for instance, when the proposed EI is an overseas financial institution captured under C. 1. 4 (c) above, the FSP should obtain, evidence that it is regulated which may comprise corroboration from the EI's regulatory authority, or evidence from the EI itself. 15. When considering whether it is reasonable to rely on an EI, additional consideration that senior management may consider include the following: (1) whether there is a pre-existing customer relationship between the Cayman FSP and the EI and/or between the EI and the applicant and the length of that relationship; (2) whether the nature of the business of the EI and applicant are appropriate to the business being introduced; and 16. The information provided by the EI should be in written form. The EI s Form in Appendix A or its functional equivalent that satisfies the criteria in E. 5 above should be completed in these circumstances. 17. If an EI fails or is unable to provide a written confirmation or undertaking of the sort required in 16 above, the relationship must be reassessed and a judgment made as to what other steps to verify identity are appropriate or, where there is a pattern of non-compliance, whether the relationship should be discontinued. 18. FSPs should also test procedures on a random and periodic basis to ensure that CDD documentation and information is produced by the EI upon demand and without undue delay. FSPs must maintain a record of the periodic testing, which should clearly highlight any difficulties/delays in the EI s producing the CDD documentation and the remedial action(s) taken by the FSP. 19. It would also be prudent for an FSP placing reliance on an EI to agree with that EI that the CDD information and verification documentation will be maintained for the period specified under the AMLRs. It should also be established that the EI will notify the FSP if it is no longer able to comply with any aspect of the agreement (e.g. if the EI ceases to trade or there is a change in the law) and provide the FSP with the records or copies of records. 20. If FSPs are aware of any cases where EIs have incorrectly been treated as eligible, they must take steps to obtain suitable CDD information and verification documents in accordance with the AMLRs. 21. Following introduction by an EI, it will not usually be necessary to re-verify identity or duplicate records in respect of each transaction or piece of business. Guidance Notes ML/TF/PF Page 66 of 245 22. FSP and other persons that meet the criteria of EIs who are themselves subject to the AMLRs have no obligation to act as EIs. Should they choose to do so, however, they must be satisfied that the information provided has in fact been obtained appropriately and verified and will be made available to the person relying on it as soon as reasonably practicable. A Cayman Islands licensed bank branch for example should not provide confirmation to another party on any non-compliant account or in circumstances where it would be in breach of the act to provide customer information. F. VERIFICATION OBLIGATIONS FOR ONE-OFF TRANSACTIONS 1. Unless a transaction is a suspicious one, an FSP is not required to obtain documentary evidence of identity for one-off transactions valued less than KYD 15,000. One-off transaction valued less than KYD 15,000 means is a one-off transaction where the amount of the (single) transaction or the aggregate of a series of linked transactions is less than KYD15,000. In the event of any knowledge or suspicion that ML/TF has occurred or is occurring, the case should be treated the same as one requiring

verification and reporting. 2. As a matter of best practice, a time period of 12 months for the identification of linked transactions is normally acceptable. However, there is some difficulty in defining an absolute time scale that linked transactions may fall within. Therefore, the relevant procedures for linking will ultimately depend on the characteristics of the product rather than relating to any arbitrary time limit. For example, FSPs should be aware of any obvious connections between the sender of funds and the recipient. 3. Verification of identity will not normally be needed in the case of a one-off transaction referred to above. If, however, the circumstances surrounding the one-off transaction appear to the FSP to be unusual or questionable, it is likely to be necessary to make further enquiries. Depending on the result of such enquiries, it may then be necessary to take steps to verify the proposed customer s identity. If ML/TF is known or suspected, the FSP should not refrain from making a report to the FRA simply because of the size of the transaction. Guidance Notes ML/TF/PF Page 67 of 245 SECTION 6 ENHANCED CDD MEASURES (EDD) 41 A. EDD MEASURES 1. FSPs should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, that have no apparent economic or lawful purpose. 2. Where the risks of ML/TF are higher, or in cases of unusual or suspicious activity, FSPs should conduct EDD measures, consistent with the risks identified. In particular, FSPs should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. 3. Examples of EDD measures that could be applied for high-risk business relationships include: (1) Obtaining additional information on the applicant/customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.). (2) Updating more regularly the identification data of applicant/customer and beneficial owner. (3) Obtaining additional information on the intended nature of the business relationship. (4) Obtaining additional information on the source of funds or source of wealth of the applicant/customer. (5) Obtaining additional information on the reasons for intended or performed transactions. (6) Obtaining the approval of senior management to commence or continue the business relationship. (7) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination. (8) Requiring the first payment to be carried out through an account in the customer s name with a bank subject to similar CDD standards. 4. Where the FSP is unable to conduct EDD, it shall follow the procedures as specified in the section on CDD under Obligations where unable to complete CDD of this document. B. HOLD MAIL ACCOUNTS 1. "Hold Mail" accounts are accounts where the accountholder has instructed the FSP not to issue any correspondence to the accountholder's address. Although this is not necessarily a suspicious act in itself, such accounts do carry additional risk to FSPs, and they should exercise due caution as a result. 41 Part VI of the AMLRs Guidance Notes ML/TF/PF Page 68 of 245 2. Regardless of the source of "Hold Mail" business, it is recommended on a best practice basis that evidence of identity of the accountholder should be obtained by the FSP, even where the customer was introduced by an EI. "Hold Mail" accounts should be regularly monitored and reviewed. 3. It is recommended that FSP have controls in place for when existing accounts change status to "Hold Mail", and that the necessary steps to obtain the identity of the account holder are taken where such evidence is not already in the FSP file. 4. Accounts with a "c/o" address should not be treated as "Hold Mail" accounts, as mail is being issued, albeit not necessarily to the accountholder's address.

There are of course many genuine innocent circumstances where a "c/o" address is used, but an FSP should monitor such accounts more closely as they represent a higher risk. 5. FSPs should incorporate procedures to check the current permanent address of hold mail customers when the opportunity arises. C. HIGH-RISK COUNTRIES 42 1. Certain countries are associated with crimes such as drug trafficking, fraud and corruption, and consequently pose a higher potential risk to an FSP. Conducting a business relationship with an applicant/customer from such a country exposes the FSP to reputational and legal risks. 2. FSPs should exercise additional caution and conduct EDD 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 country, FSPs are encouraged to consider among the other sources, sanctions issued by the UN and UK, the FATF high risk and non-cooperative jurisdictions, the FATF and its regional style bodies (FSRBs) such as MoneyVal mutual evaluation reports, and Transparency international corruption perception index. 5. Useful websites include: FATF website at the Financial Crimes Enforcement Network (FinCEN) at for country advisories; the Office of Foreign Assets Control (OFAC) for information pertaining to US foreign policy and national security; and Transparency International, for information on countries vulnerable to corruption. 42 FATF R.19 and IN- 19.1 Guidance Notes ML/TF/PF Page 69 of 245 6. FSPs should be aware that with respect to high-risk countries, the relevant Supervisory Authority may apply countermeasures proportionate to the risks, which may include: (1) Requiring FSPs to apply specific elements of EDD measures. (2) Introducing relevant enhanced reporting mechanisms or systematic reporting of financial transactions. (3) Refusing the establishment of subsidiaries or branches or representative offices of FSPs from the country concerned, or otherwise taking into account the fact that the FSP is from a country that does not have adequate AML/CFT systems. (4) Prohibiting FSPs from establishing branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant branch or representative office would be in a country that does not have adequate AML/CFT systems. (5) Limiting business relationships or financial transactions with the identified country or persons in that country. (6) Prohibiting FSPs from relying on third parties located in the country concerned to conduct elements of the CDD process. (7) Requiring FSPs to review and amend, or if necessary, terminate, correspondent relationships with FSPs in the country concerned. (8) Increasing examinations/inspections and/or external audit requirements for branches and subsidiaries of FSPs based in the country concerned. (9) Requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned. Guidance Notes ML/TF/PF Page 70 of 245 SECTION 7 POLITICALLY EXPOSED PERSONS 43 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 44 . 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. 45 5. Provision of financial services to corrupt PEPs exposes an FSP to reputational risk and costly information requests and seizure orders from law enforcement or judicial authorities. In addition, public confidence in the ethical standards of the whole financial system can be undermined. 6. FSPs are encouraged to be vigilant in relation to PEPs from all jurisdictions, who are seeking to establish business relationships. FSPs should, in relation to PEPs, in addition to performing normal due diligence measures: (1) have appropriate risk management systems to determine whether the customer is a PEP; (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. 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. 46 43 Part VII of the AMLRs 44 Please refer to the definitions of PEP, family member and close associate provided in the AMLRs 45 Definitions of family members and close associates from Part II of the FATF June 2013 Guidance on Politically Exposed Persons (Recommendations 12 and 22) 46 FATF R.12 and IN- 12 Guidance Notes ML/TF/PF Page 71 of 245 8. FSPs shall take a risk-based approach to determine the nature and extent of EDD where the ML/TF risks are high. In assessing the ML/TF risks of a PEP, the FSP shall consider factors such as whether the customer who is a PEP: (1) Is from a high risk country (see section on high risk countries); (2) Has prominent public functions in sectors known to be exposed to corruption; and (3) Has business interests that can cause conflict of interests (with the position held). 9. The other red flags that the FSPs shall consider include (in addition to the above and the red flags that they consider for other applicants): (1) The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries; (2) Funds are repeatedly moved to and from countries to which the PEP does not seem to have ties; (3) A PEP uses multiple bank accounts for no apparent commercial or other reason; (4) The PEP is from a country that prohibits or restricts certain citizens from holding accounts or owning certain property in a foreign country. B. PEP STATUS 1. FSPs shall take a risk-based approach in determining whether to continue to consider a customer as a PEP who is no longer a PEP. The factors that they should consider include: (1) the level of (informal) influence that the individual could still exercise; and (2) whether the individual s previous and current function are linked in any way (e.g., formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters). 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 must be done at least at the time of pay-out. 2. Where high risks are identified in the above cases, FSPs should inform the senior management before the pay-out of the policy and conduct EDD on the whole business relationship. Additionally, where appropriate, FSPs should consider filing a SAR. Page 72 of 245 SECTION 8 RECORD-KEEPING PROCEDURES 47 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 must 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 CDD 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. FSPs must also ensure that records of identification data obtained through digital ID systems and e-KYC procedures are easily accessible, maintained and can be made available to competent authorities upon request. 4. 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. 5. 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. 6. Records relating to verification of identity will generally comprise: (1) a description of the nature of all the evidence received relating to the identity of the verification subject; and (2) the evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy. 7. 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 counterparty. (2) details of securities and investments transacted including: (a) the nature of such securities/investments; (b) valuation(s) and price(s); (c) memoranda of purchase and sale; 47 Part VIII of the AMLRs Page 73 of 245 (d) source(s) and volume of funds and bearer securities; (e) destination(s) of funds and bearer securities; (f) memoranda of instruction(s) and authority(ies); (g) book entries; (h) custody of title documentation; (i) the nature of the transaction; (j) the date of the transaction; (k) the form (e.g. cash, cheque) in which funds are offered and paid out. B. GROUP RECORDS 1. There may be circumstances in which group records are stored centrally outside the Cayman Islands. In the case of records that are maintained outside the Cayman Islands, the records shall be maintained in accordance with the AMLRs and should be able to be retrieved and provided to the competent authorities promptly on request without delay. For further guidance, FSPs may refer to the Statement of Guidance on Nature, Accessibility and Retention of Records issued by the Monetary Authority. C. TRAINING RECORDS 1. FSPs should demonstrate that they have complied with the provisions of Section 5 of the AMLRs concerning staff training. 2. They may do so by maintaining records which include: (1) details of the content of the training programmes provided; (2) the names and designations/titles of staff who have received the training; (3) the date on which the training was delivered; (4) the results of any testing carried out to measure staff understanding of the ML requirements; and (5) an on-going training plan. D. ESTABLISHMENT OF REGISTERS 1. An FSP should maintain a register of all enquiries made to it by the FRA and all disclosures to the FRA. 2. The register should be kept separate from other records and contain as a minimum the following details: (1) the date and nature of the enquiry; (2) details of the account(s) involved; and (3) be maintained for a period of at least 5 years after termination of the

relationship. E. EQUIVALENCY 1. Where, in order to satisfy the requirements of the AMLRs, the FSP- (a) has delegated the performance of any function to a person or institution in a country assessed by the FSP as having a low degree of risk of ML/TF; or (b) relies on a person or institution in such a country to perform any function required to be Page 74 of 245 performed, then the FSP must be satisfied that the relevant records will be maintained in accordance with the relevant requirements of the AMLRs. FSPs may refer to Section 10 of this part of the Guidance Notes and to the Statement of Guidance on Nature, Accessibility and Retention of Records issued by the Monetary Authority. 2. The FSP shall ensure that those records will be available to the relevant Supervisory Authority on request and to the FRA or law enforcement authorities in accordance with the relevant provisions. Page 75 of 245 SECTION 9 MONEY LAUNDERING REPORTING OFFICER 48 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 are aware of the reporting chain and the procedures to be followed. 2. Such procedures should be periodically updated to reflect any legislative changes. B. APPOINTING AN MLRO TO WHOM ALL REPORTS OF KNOWLEDGE OR SUSPICION OF ML/TF ARE MADE. 1. Each FSP should designate a suitably qualified and experienced person as MLRO at management level, to whom SARs must be made by staff. 2. The FSP should ensure that the person acting as MLRO/DMLRO: (1) is a natural person; (2) is autonomous (meaning the MLRO is the final decision maker as to whether to file a SAR); (3) is independent (meaning no vested interest in the underlying activity); (4) 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; and (5) can dedicate sufficient time for the efficient discharge of the MLRO function, particularly where the MLRO/DMLRO 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 in Parts III to IX of these Guidance Notes gives examples of such transactions, which are not intended to be exhaustive. 6. It is recognised that it is possible that an FSP may not have employees in the Cayman Islands and it may not be possible for a senior member of staff (or a sole trader him/herself) to be the MLRO/DMLRO. In these circumstances, the FSP should identify a person that meets the criteria set out in B 2 above and designate that person as an MLRO/DMLRO. (1) After designating an MLRO/DMLRO, the FSP may choose to delegate the performance of the MLRO function to a person or rely on a person to perform the MLRO function in accordance with Regulation 3(2) of the 48 Part IX of the AMLRs Page 76 of 245 AMLRs. See Part II, Section 10. C. (Outsourcing) for the guidance on delegation; and Part II, Section 2. C.8 for the guidance on placing reliance on third parties. 7. Where the FSP is a mutual fund regulated in the Cayman Islands, the FSP should utilise the further options set out in the relevant sector specific guidance. 8. Where it is not possible to nominate a staff member (or a sole trader, him/herself) as a DMLRO, the FSP may delegate/outsource the DMLRO function in a similar manner to the MLRO as specified above. 9. Where the relevant Supervisory Authority requires FSPs to provide notification or

obtain prior approval for the appointment of an AMLRO/DMLRO, FSPs should comply with such requirements in the manner prescribed, if any, by the relevant Supervisory Authority. 10. Where an FSP has no staff, the provisions under the AMLRs regarding awareness and training will not apply. However, the FSP shall ensure that the person assuming the role of the MLRO is receiving adequate AML/CFT related training (that is appropriate and useful to perform the MLRO function diligently) on a regular basis. 11. The FSP is responsible for ensuring that any staff member involved in the relevant activities of the FSP is aware of the identity of the MLRO (and DMLRO) and that all internal SARs are submitted to the MLRO or in his/her absence to the DMLRO. 12. Where the MLRO that is located outside of the Islands files a SAR 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 SAR. All relevant staff must be aware of the chain through which SARs 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, Page 77 of 245 the line/relationship manager can be permitted to add his comments to the SAR 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. Page 78 of 245 8. Activities which should put staff on enquiry may be recognisable 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 D1. to D8. above should also be extended to attempted transactions or instructions. E. QUESTIONS TO ASK YOURSELF 1. The following factors should be considered when seeking to identify a suspicious transaction. This list is not meant to be exhaustive. (1) Is the applicant/customer known personally? (2) Is the transaction in keeping with the customer's normal activity known to the FSP, the markets in which the customer is active and the customer's own business? (i.e. does it make sense?) (3) Is the transaction in keeping with normal practice in the market to which it relates i.e. with reference to market, size and frequency? (4) Is the role of the agent involved in the transaction unusual? (5) Is the transaction to be settled in the normal manner? (6) Are there any other transactions linked to the transaction in question which could be designed to disguise money and divert it into other forms or to other destinations or beneficiaries? (7) Are the reasons for the transaction(s) comprehensible (i.e. might there be an easier, cheaper or more convenient method available?) F. CASH TRANSACTIONS 1. Given the international nature of the business conducted by many FSPs, cash transactions may be relatively uncommon, whereas for banks, building societies or money services businesses offering services to local customers, cash transactions may be a normal every-day service to many customers. 2. Where cash transactions are being proposed by customers, and such requests are not in accordance with the customer's known reasonable practice, many FSPs will need to approach such situations with caution and make further relevant enquiries. 3. Depending on the type of business each FSP conducts and the nature of its customer portfolio, each FSP may wish to set its own parameters for the identification and further investigation of cash transactions. Where the staff member of the FSP has been unable to satisfy him/herself that any cash Page 79 of 245 transaction is reasonable, and therefore she/he considers it suspicious, he/she should make a disclosure as appropriate. 4. Whilst certain

cash transactions may lead the FSP to make further enquiries to establish or dispel suspicion, it goes without saying that equal vigilance must be applied to transactions which do not involve cash. G. ROLE OF STAFF MEMBERS 1. Staff should be required to report any suspicion of ML/TF either directly to their MLRO or, if the FSP so decides, to their line manager for preliminary investigation in case there are any known facts which may negate the suspicion subject to C(2) of this section. 2. Employees should comply at all times with the vigilance systems of their institution and will be treated as having met appropriate standards of vigilance if they disclose their suspicions to their MLRO or other appropriate senior colleague according to the vigilance systems in operation in their institution. H. THE ROLE OF THE MLRO 1. On receipt of a report concerning a suspicious applicant/customer or suspicious activity, the MLRO/DMLRO should determine whether the information contained in such report supports the suspicion. The MLRO/DMLRO should investigate the details in order to determine whether in all the circumstances he/she in turn should submit a report to the FRA. 2. If the MLRO decides that the information does substantiate a suspicion of ML/TF, he/she must disclose this information promptly to the FRA. If the MLRO decides that the information does not substantiate a suspicion, he/she would nevertheless be well advised to record fully the reasons for his decision not to report to the FRA. 3. It is for each FSP (or group) to consider whether its vigilance systems should require the MLRO to report suspicions within the FSP (or group) to the inspection or compliance department at head office. 4. Failure by the MLRO to diligently consider all relevant material may lead to vital information being overlooked and the suspicious activity not being disclosed to the FRA in accordance with the requirements of the legislation. Alternatively, it may also lead to vital information being overlooked which may have made it clear that a disclosure would have been unnecessary. 5. MLROs should establish and maintain a register of ML/TF referrals made to him/her by staff. 6. Staff members should note that in the event of suspicion of ML/TF, a disclosure must 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. Page 80 of 245 I. REPORTING SUSPICIONS TO THE FRA 1. If the MLRO decides that a disclosure should be made, a report, in standard form as prescribed by the FRA, should be sent to the FRA without delay. The FRA s prescribed reporting form can be found on its website through the link below: 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 must 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. Page 81 of 245 SECTION 10 OTHER INTERNAL CONTROLS (RELATING TO AUDIT FUNCTION, OUTSOURCING, EMPLOYEE SCREENING AND TRAINING) A. INTRODUCTION 1. FSPs are expected to have systems and controls that are comprehensive and proportionate to the nature, scale and complexity of their activities and the ML/TF risks they identified. FSPs obligation to establish and maintain AML/CFT policies and procedures are discussed in different sections of this document. This section specifically discusses the internal controls in relation to: (1) an audit function to test the AML/CFT systems, policies and procedures; (2) outsourcing arrangements; (3) employee screening procedures to ensure high standards when hiring employees; and (4) an appropriate employee training programme. 2. The type and extent of measures to be taken should be appropriate to the ML/TF risks, and to the size of the FSP. B. AUDIT FUNCTION 1. An FSP should, on a regular basis, conduct an AML/CFT audit. The frequency of the audit must be commensurate with the FSP s nature, size, complexity, and risks identified during the risk assessments. The AML/CFT audits should be conducted to assess the AML/CFT systems which include: (1) test the overall integrity and effectiveness of the AML/CFT systems and controls; (2) assess the adequacy of internal policies and procedures including; (a) CDD measures; (b) Record keeping and retention; (c) Third party relationships (e.g. EIs) and supporting documentation; and (d) Transaction monitoring; (3) assess compliance with the relevant Acts 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 Acts, regulations, rules, guidance, and policies and procedures; (6) assess the adequacy, accuracy and completeness of training programmes; and (7) assess the adequacy of the FSP s process of identifying suspicious activity including screening lists. C. OUTSOURCING 1. FSPs should maintain policies and procedures in relation to outsourcing where they intend to outsource some of their functions. The guidance provided here particularly addresses the required controls for outsourcing AMLCO and MLRO functions. Page 82 of 245 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 outsourcing service provider (OSP) is fit and proper to perform the activity that is being outsourced. 4. Where the FSP decides to enter into an outsourcing arrangement, the FSP shall ensure that the outsourcing agreement clearly sets out the obligations of both parties. 5. FSPs entering into an outsourcing arrangement should develop a contingency plan and a strategy to exit the arrangement in the

event that the OSP fails to perform the outsourced activity as agreed. 6. The OSP should report regularly to the FSP within the timeframes as agreed upon with the FSP. The FSP should have access to all the information or documents relevant to the outsourced activity maintained by the OSP. 7. FSPs must not enter into outsourcing arrangements where access to data without delay is likely to be impeded by confidentiality, secrecy, privacy, or data protection restrictions. 8. FSPs shall ensure that the outsourcing agreement requires OSPs to file a SAR with the FRA in case of suspicions arising in the course of performing the outsourced activity. 9. Where the outsourcing arrangement allows for sub-contracting, the OSP may sub- contract any of the outsourced activities that are allowed for sub-contracting. The FSP shall ensure that while sub-contracting, the OSP follows the outsourcing standards equivalent to that of the FSP. 10. Where the OSP operates from a country outside of the Cayman Islands in which the standards are lower when compared to the Cayman Islands, then the OSP should adopt the Cayman Islands standards. The same approach should be adopted in case of sub-contracting. Where the sub-contractor is from a country whose standards are lower when compared to the Cayman Islands, the sub- contractor should adopt the standards of the Cayman Islands. 11. For further guidance on outsourcing, FSPs may refer to the Statement of Guidance on Outsourcing issued by the Monetary Authority, where applicable. D. EMPLOYEE SCREENING 1. The AMLRs (5 (a) (iii)) require FSPs to maintain procedures to screen employees to ensure high standards when hiring. 2. The extent of employee screening should be proportionate to the potential risk associated with ML/TF in relation to the business in general, and to the particular risks associated with the individual positions. Employee screening should be Page 83 of 245 conducted at the time of recruitment, periodically thereafter, i.e., at least annually and where a suspicion has arisen as to the conduct of the employee. 3. FSPs shall ensure that their employees are competent and proper for the discharge of the responsibilities allocated to them. While determining whether an employee is fit and proper, the FSP may: (1) Verify the references provided by the prospective employee at the time of recruitment (2) Verify the employee s employment history, professional membership and qualifications (3) Verify details of any regulatory actions or actions taken by a professional body (4) Verify details of any criminal convictions; and (5) Verify whether the employee has any connections with the sanctioned countries or parties which may include doing checks against screening databases (e.g. world check). E. EMPLOYEE TRAINING 1. Where FSPs have staff, they should ensure that all appropriate staff, in accordance with Section 5 of the AMLRs, receive training on ML/TF prevention on a regular basis, ensure all staff fully understand the procedures and their importance, and ensure that they fully understand that they will be committing criminal offences if they contravene the provisions of the legislation. The Timing and Content of Training Programmes 1. Training to staff should be provided at least annually, or more frequently where there are changes to the applicable legal or regulatory requirements or where there are significant changes to the FSP s business operations or customer base. 2. FSPs should provide their staff training in the recognition and treatment of suspicious activities. Training should also be provided on the results of the FSP s risk assessments. Each FSP can tailor its training programmes to suit its own needs, depending on size, resources and the type of business they undertake. 3. Smaller organisations with no in-house training function may wish to approach third parties such as specialist training agencies, firms of attorneys or legal practitioners, or the major firms of accountants or management consultants. Training should be

structured to ensure compliance with all of the requirements of the applicable legislation. 4. Where the FSP has delegated the performance of relevant functions to a person or an institution in a country assessed by the FSP as having a low degree of risk of ML/TF, it must be satisfied that equivalent training and education procedures are in place in relation to the applicable laws and regulations of such country. In cases where the delegated party is an affiliate or subsidiary of the FSP, the FSP is typically responsible for ensuring that the respective staff is appropriately trained on a regular and ongoing basis. Page 84 of 245 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 staff aware of the relevant AML/CFT legislation and regulatory requirements. New Employees 7. Irrespective of seniority, all new employees should be given a general introduction to the background of ML/TF and the procedures for reporting suspicious activities to the MLRO, prior to them becoming actively involved in day to day operations. New employees should also receive a clear indication of the importance placed on ML/TF issues by the organisation, of the legal requirement to report, and of their personal legal obligations in this regard. 8. FSPs shall consider obtaining an undertaking from their staff members (both new and existing) confirming that they have attended the training on AML/CFT matters, read the FSP s AML/CFT manuals, policies and procedures, and understand the AML/CFT obligations under the relevant legislation. Operations Staff 9. Staff members who deal with the public such as cashiers, salespersons 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. Page 85 of 245 Training for Supervisors, Managers and Senior Management 12. Although Directors and Senior Managers may not be involved in the day-to-day procedures for handling transactions that may relate to ML/TF, it is important that they understand the statutory duties placed upon them, their staff and the firm itself given that these individuals are involved in approving

AML/CFT policies and procedures. 13. Supervisors, managers and senior management (including Board of Directors) should receive a higher level of training covering all aspects of AML/CFT procedures, including the offences and penalties arising from the relevant primary legislation for non-reporting or for assisting money launderers, the procedures relating to dealing with production and restraint orders and the requirements for verification of identity and retention of records. Training for Money Laundering Reporting Personnel (MLRO) 14. MLROs and DMLROs should receive in-depth training on all aspects of the primary legislation, the AMLRs, supervisory or regulatory rules and guidance and relevant internal policies. They should also receive appropriate initial and ongoing training on the investigation, determination and reporting of suspicious activities, on the feedback arrangements and on new trends of criminal activity. Continuing Vigilance and 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. Page 86 of 245 SECTION 11 IDENTIFICATION AND RECORD-KEEPING REQUIREMENTS RELATING TO WIRE TRANSFERS 49 A. GENERAL 50 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 51 1. These Guidance Notes apply to transfer of funds i.e., cross-border wire transfers and domestic wire transfers, including serial payments, and cover payments in any currency. 2. Recognising, and in keeping with international standards that certain transfers of funds represent a low risk of ML/TF, the AMLRs do not require FSPs to comply with the identification and record keeping obligations provided in this section in case of the following types of funds transfers 52 : (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; 49 Part X of the AMLRs 50 FATF R. 16 and IN. 16.1 51 FATF R. 16 and IN. 16.3 to 16.5 52 Regulation 25 of the AMLRs Page 87 of 245 (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 - IDENTIFICATION INFORMATION AND RECORD KEEPING REQUIREMENTS 53 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 BTCA licensee or where the payer is bound by regulation 5 of the AMLRs. 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). 53 FATF R. 16 and IN. 16.6 to 16.8 Page 88 of 245 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 AND 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 affect 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 Page 89 of 245 (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 AND 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) 54 1. More detailed sector specific guidance are provided in Part VII of these Guidance Notes in respect of MSBs. However, these Guidance Notes which pertain to them in the execution of their wire transfer functions should also be observed by MVTS or MSB. 2. An MSB should comply with all of the relevant requirements of these Guidance Notes relating to wire transfers in the countries in which they operate, directly or through their agents. 3. In the case of an MSB that controls both the ordering and the beneficiary side of a wire transfer, the MSB: 54 FATF R. 16 and IN. 16.22 Page 90 of 245 (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 (2) should file a SAR in any country affected by the suspicious wire transfer, and without delay make relevant transaction information available to the FRA and the relevant authorities in the Cayman Islands. Page 91 of 245 SECTION 12 CORRESPONDENT BANKS 55 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. 7. With respect to payable-through accounts (PTA) 56 , FSP shall be satisfied that the respondent institution has verified the identity of and performs on-going due diligence on the customers having direct access to accounts of the correspondent institution and that the respondent institution is able to provide relevant customer identification data upon request to the correspondent bank. 55 Part XI of the AMLRs 56 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. Page 92 of 245 8. FSPs should not enter into, or continue, a correspondent relationship with a shell bank 57 ; and should take appropriate measures to ensure that they do not enter into, or continue a corresponding banking relationship with a bank which is known to permit its accounts to be used by a shell bank. Neither should FSPs set up anonymous accounts or anonymous passbooks for new or existing customers. 9. FSPs should satisfy themselves that the respondents in foreign countries do not permit their accounts to be used by shell banks. 10. The similar relationships to which FSPs should apply criteria under 6 above include, for example, those established for securities transactions or funds transfers, whether for the cross-border financial institution as principal or for its customers. 58

57 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. 58 FATF R.13 and IN- 13 Page 93 of 245 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 TA and the PFPA. 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 weapons of mass destruction 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. Page 94 of 245 2. Official sanction 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 However, it is the responsibility of the FSPs to check from time-to-time for updates. 3. When conducting risk assessments, FSPs shall, as noted in Section 3.C, take into account any sanctions that may apply (to applicants/customers or countries). 4. FSPs shall screen applicants, customers, beneficial owners, transactions, service providers and other relevant parties to determine whether they are conducting or may conduct business involving any sanctioned person or person associated with a sanctioned person/country. In the event of updates to the relevant sanctions lists, FSPs may discover that certain sanctions are applicable to one or more of their customers, existing or new. 5. Where there is a true match or suspicion, FSPs shall take steps that are required to comply with the sanctions obligations including reporting pursuant to the Act, AMLRs and TA. FSPs are required to file a Compliance Reporting Form (CRF) when making a report to the FRA. The CRF should be used when reporting suspected designated persons, frozen assets, and suspected breaches of financial sanctions. Additionally, FSPs must file a SAR with the FRA, if they discover a relationship that contravenes a sanctions order or a direction under the PFPA. 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, ensure that existing customers are not listed. 7. Generally, the sanctions lists in force in the UK (HM Treasury) are extended to the Cayman Islands. These sanctions apply to all individuals and entities in

the Cayman Islands. The lists issued in the United Kingdom (HM Treasury) might be different from lists issued by other countries, such as the United States (OFAC). While the OFAC sanctions may have no legal effect in the Cayman Islands, because of the extra-territorial effect of the US measures, and their implications for international banking transactions in US dollars, FSPs should take note of them. It is important that FSPs carefully select the sanctions lists as lists that do not include at least all the sanctions applicable in the Cayman Islands may cause an FSP s sanctions compliance programme and monitoring to be deficient. Page 95 of 245 SECTION 14 COUNTER PROLIFERATION FINANCING A. APPLICABILITY 1. This section of the Guidance Notes applies to all financial services providers in the Cayman Islands. Moreover, this section applies to any entity conducting insurance business, regardless of whether the entity carries on long-term or general insurance business. This section also applies to trust and corporate services providers and Designated Non-Financial Businesses and Professionals that provide services to shipping and freight forwarding business, import/export business activity, and clients in jurisdictions near sanctioned countries. B. PROLIFERATION AND PROLIFERATION FINANCING 1. Proliferation is the manufacture, acquisition, possession, developing, export, transhipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations. It includes technology, goods, software, services and expertise. 2. Proliferation financing is the act of providing funds or financial services which are used, in whole or in part, to make proliferation possible. In other words, it is the financing of the proliferation activities described above. 3. Proliferation financing refers to more than simply the payment for goods and includes any financial service provided in support of any part of the procurement process (even if it is not directly connected to the physical flow of goods). Financing can include financial transfers, mortgages, credit lines, insurance services, middlemen services, trust and corporate services and company formation. 4. Proliferation financing facilitates the movement and development of proliferation- sensitive goods. The movement and development of such items poses a risk to global security and stability and may ultimately result in loss of life. 5. While the Cayman Islands has not encountered any direct acts of terrorism or proliferation to date, the risk of proliferation still exists given the size and breadth of the Cayman Islands financial system as well as the increasingly novel and sophisticated methods, vehicles and jurisdictions used by proliferators in an attempt to escape sanctions imposed against them. 6. This section of the Guidance Notes seeks to assist financial services providers in identifying the proliferation financing risks and vulnerabilities to which they are exposed and also in the development of their systems and controls to prevent, detect and report proliferation financing. C. INTERNATIONAL FRAMEWORK 1. The UN has passed three resolutions relating to anti-proliferation. Two resolutions are country specific, relating to North Korea (DPRK) and to Iran. These UN resolutions are in force in the Cayman Islands via Orders passed in the Page 96 of 245 United Kingdom, namely The Iran (Restrictive Measures) (Overseas Territories) Order 2012 and the North Korea (UN Measures) (Overseas Territories) Order 2006. 2. The third resolution is global in nature (non-country specific). UN Security Council Resolution 1540 seeks to prevent non-State actors from obtaining weapons of mass destruction. It establishes binding obligation on member states to: (1) Prohibit support to non-state actors seeking weapons of mass

destruction, their means of delivery and related materials (2) Adopt and enforce effective laws prohibiting the proliferation of such items to non-state actors, and prohibiting assisting or financing such proliferation; and (3) to take and enforce effective measures to control these items, in order to prevent their proliferation, as well as to control the provision of funds and services that contribute to proliferation. 3. The United Kingdom (UK) extends these resolutions to the Cayman Islands via overseas territories Orders. D. DOMESTIC LEGISLATION 1. The Proliferation Financing (Prohibition) Act, 2017 makes it an offence for any person to provide funds and economic resources to fund unauthorised proliferation activities, or to enter into or become concerned in an arrangement which that person knows or suspects facilitates the acquisition, retention, use or control of funds and economic resources to fund unauthorised proliferation activities. 2. A person who acts in the course of a business in the financial sector may be committing an offence, even if the offence takes place wholly or partly outside the Islands. E. HOW PROLIFERATION FINANCING DIFFERS FROM MONEY LAUNDERING 1. Proliferators operate globally, try to mask their activities as legitimate trade and exploit global commerce by trading in countries with weak export controls or free trade zones. 2. The stages of proliferation financing differ from the placement-layering- integration cycle associated with ML. Rather, the pattern used by proliferators is a linear Raise Obscure Procure & Ship. 3. During the Raise stage funds are raised from overseas criminal activities, state budgets and overseas commercial enterprises. 4. During the second stage of proliferation financing, proliferators rely on extensive networks of businesses (including front companies) and middlemen to obscure any connection on paper to sanctioned countries. Countries use opaque ownership structures for evading sanctions lists. Often proliferation financing involves companies in or near a sanctioned country and accounts under the control of a foreign national (i.e. not Iranian or a North Korean national) with sympathies to the sanctioned country. This, combined with the use of false documentation, allows proliferators to avoid detection. However, studying previous proliferation financing cases and typologies can allow FSPs to gain a better understanding of these networks. 5. The Procure & Ship stage involves expenses associated with brokers, shippers, freight forwarders, insurance coverage, for goods and technology that is intended to be delivered to conduit countries for final entry into a sanctioned country. It is important to note that proliferation involves not only the purchase of weapons but also of individual goods and component parts that can be used to develop weapons or missiles. This makes proliferation activities more difficult to detect. 6. Also, unlike ML, which is concerned about funds raised by illegitimate means, the source of funds used to finance proliferation can be both legal and illegal. The destination or use of those funds is for advancing the ambitions of sanctioned states. In many cases the financing source is from a state or a person acting as an indirect agent of the state. 7. As such, while some risk indicators and control elements might overlap for ML and proliferation financing, proliferation financing also has its own unique risk indicators and associated controls that financial institutions should implement. Table - Comparison of Proliferation Financing to Money Laundering and Terrorist Financing Money Laundering Terrorist Financing Proliferation Financing Flow of Funds Circular money eventually ends up with the person that generated it Linear money generated is to propagate terrorist groups and activities Linear money is used to purchase goods and parts, technology from brokers and manufacturers. Shipping and insurance also part of money trail Conduits Favours formal financial system Favours cash couriers or informal systems such as

hawala and currency exchange firms Favours formal financial system Detection Focus Suspicious transactions deposits uncharacteristic of customer s or the expected activity Suspicious relationships, such as wire transfers to seemingly unrelated parties Goods and materials, activities, countries, individuals Transaction Amounts Large, but often structured to avoid reporting requirements Small usually below reporting thresholds Moderate amounts transactions appear legitimate with transaction profile Financial Activity Complex web of transactions often involving shell or Varied methods, including formal banking system, Transactions look like normal commercial Page 98 of 245 front companies, bearer shares and countries with lax financial services regulation informal value transfer systems, smuggling of cash and valuables activity, structured to hide origin of funding F. DUAL USE GOODS AND EXPORT CONTROLS 1. Proliferation financing is often associated with trade in dual use goods. Dual-use goods are items that have both commercial and military or proliferation applications. These goods could be components of a weapon or machines to manufacture a weapon that also have civilian applications (for example, certain tools that can be used to repair vehicles). Even if some goods do not appear on export control lists, they are still subject to restrictions if their end use is for illicit proliferation purposes. Dual-use goods can be identified from lists produced by the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual- Use Goods and Technologies. G. CHALLENGES OF IDENTIFYING PROLIFERATION FINANCING 1. While the UN and several national governments have issued lists of designated persons and entities known to be associated with proliferation, sole reliance on screening against those lists might not always be effective, as they do not cover the full extent of proliferation networks and proliferation activity. Proliferators try to engage new persons or form new entities with different managers and directors to carry out transactions on their behalf. Proliferators also use several transhipment points before goods reach their target destination. 2. Proliferation financing tends to be directed by state actors, who develop their own networks and distinct ways of accessing the financial system. FSPs should be aware that proliferation networks and methods will vary from country to country. Conversely, proliferation networks from the same country tend to behave similarly. 3. Finally, illicit proliferation can include procurement of illicit materials by a sanctioned country as well as a sanctioned country that provides sensitive goods to other countries. H. OBLIGATIONS OF FINANCIAL SERVICES PROVIDERS 1. FSPs must carry out appropriate CDD on their clients, which includes screening names of clients and clients counterparties, including shipping companies, beneficiaries of letters of credit and freight companies, against sanctions lists. However, that is not enough, as the names of entities or individuals on sanctions lists rarely appear in financial transactions. In addition, on paper, a transaction is rarely directly connected to a sanctioned country. 2. Therefore, in addition to screening, FSPs must also implement risk-based systems and controls to detect proliferation financing. FSPs should carry out a risk assessment to determine their exposure to proliferation financing risk. The risk assessment should consider risks relating to geography, customers and products and services. Page 99 of 245 Customers 3. FSPs should determine the exposure of their clients to the manufacture, trade or provision of expertise or consulting services relating to sensitive or dual use goods or technology. Conversely, given the potential difficulties of identifying clients that are involved with sensitive goods and technology, FSPs should identify the clients that pose a smaller risk of proliferation financing and concentrate on gathering more information from the customers that remain. 4. FSPs and DNFBPs should also be aware of the

transactions of their clients, particularly paying attention to payments being made to importers /exporters, shipping agents, brokers and freight forwarders, especially where controlled and dual use goods are being shipped to conduit countries (those near sanctioned countries). Geography 5. The FSP should determine its level of business (including customers and beneficial owners) with sanctioned countries as well as with countries that are known to have ties with sanctioned countries (e.g. China, Hong Kong, Singapore and Malaysia). The FSP should remain informed about the countries that present a higher risk for proliferation financing. 6. The FSP should identify its business relationships, including correspondent banking relationships, with partners and financial services providers located in the above noted jurisdictions. 7. The FSP should identify clients with payments to importers/exporters, shipping agents, brokers, and freight forwarders that export to countries and ports near the border of sanctioned countries. For example, shipments of prohibited goods to the Democratic People s Republic of Korea (North Korea) are often marked as destined to Dandong, China, and other nearby ports. 8. Shipments and freight forwarding destined to Iran could be labelled as being shipped to bordering countries such as Turkey, Turkmenistan, Afghanistan, Pakistan, United Arab Emirates, Oman, Qatar, Bahrain, Saudi Arabia, Kuwait, Iraq, Syria and Lebanon, and Syria. Products and Services 9. Shipping insurance and insurance against certain risks in the trading process is a financial product that is highly sought by proliferators. FSPs that offer this type of insurance should be particularly aware of their exposures to proliferation. 10. Proliferators use trade finance to assist with the procurement and movement of goods. FSPs should determine the amount of business they conduct in loans or credit facilities to facilitate export transactions, purchasing promissory notes or bills of exchange from foreign banks to exporters, purchase of discounted foreign accounts receivable and provisions of guarantees to or on behalf of exporters. 11. FSPs should consider whether they provide loans, project financing or credit to clients in sensitive industries or to entities in higher risk jurisdictions. FSPs should note that loan repayments for these facilities may be made from corporate Page 100 of 245 structures associated or linked to jurisdictions near, but not necessarily in, Iran and North Korea. Controls and Ongoing Monitoring 12. Each FSP should implement risk-based anti-proliferation and proliferation financing policies and procedures, comparable to international standards. This should include detailed internal escalation and external reporting procedures. 13. FSPs procedures should include the use of software to screen all incoming and outgoing transactions against lists of entities and persons designated under international sanctions regimes. 14. In addition to sanctions lists, UN Panel of Experts reports contain names of entities and individuals involved in proliferation activities, as well as other identifying information, including addresses, names of directors, addresses and telephone numbers. FSPs can check whether any of their clients share any of these contact details. 15. FSPs KYD and CDD frameworks should include factors relevant to proliferation financing activity. FSPs must understand the nature of their clients business, and the clients and jurisdictions with which they trade or where they operate. FSPs should be aware of clients who are either sellers or manufacturers of proliferation sensitive goods and technology. FSPs should understand their clients trade patterns and suppliers and buyers. FSPs should conduct ongoing monitoring of client accounts to ensure the account remains used for the originally stated purpose and to detect unusual activities. 16. Each FSP should conduct training on countering proliferation financing for relevant staff. The training should be commensurate with the staff members role in the FSP in the identification

or processing of suspicious transactions. 17. FSPs should familiarise themselves with export control lists. When applicable and possible, FSPs, particularly those facilitating trade finance, must screen for any clients involvement with dual-use goods and technology. FSPs might need to request specific information from clients about certain transactions that involve goods being shipped. Many goods that are considered controlled or sensitive are listed in international export control regimes. 18. In higher risk scenarios, where a customer is importing or exporting goods, FSPs should be alert to proliferation financing. FSPs should ask the customer to provide valid export licenses or letter from official sources stating that a license is not required, or other proof that a license is not required (e.g. legislation). I. FREEZING AND REPORTING OBLIGATION 1. The Proliferation Financing (Prohibition) Act requires that any person that has in its possession, custody or control, any funds or economic resources that relate to a designated person to immediately freeze such funds and resources and ensure that no funds or resources are made available for the benefit of the designated person. Page 101 of 245 2. In addition, any person must, as soon as reasonably practicable, disclose to the Financial Reporting Authority, using the form issued for that purpose 59, details of any frozen funds or economic resources or actions taken in compliance with the with the prohibition requirements of the relevant Security Council measures. This includes attempted transactions. 3. Any person who fails to comply with the freezing and reporting requirement faces civil penalties and criminal prosecution. J. RED FLAGS 1. The presence of a single red flag by itself may not automatically make a transaction suspicious. However, a combination of a red flags with other indicators might warrant the FSP to conduct a deeper investigation. Geographical Factors 2. Transactions involve foreign country of proliferation concern (i.e. Iran and North Korea) or country of diversion concern (e.g. China, particularly Liaoning and Jilin provinces, Hong Kong, Singapore and Malaysia). 3. Transactions include countries that are known to trade with North Korea (including Syria, Egypt, the United Arab Emirates, Yemen and Iran). 4. Trade finance transaction shipment route through jurisdiction with weak export control laws or enforcement or involves entities located in jurisdiction with weak export control laws or enforcement. 5. Transaction involves shipment of goods inconsistent with normal geographic trade patterns (e.g. goods are shipped through several countries for no apparent reason). 6. Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped (e.g. improbably goods, origins, quantities, destinations). 7. Transaction involves financial institutions with known deficiencies in AML/CFT controls or located in weak export control and enforcement jurisdiction. For example, it is known that North Korea has used correspondent accounts held with Chinese banks to facilitate its international financial transfers. Documentation Supporting the Transaction 8. Based on the documentation obtained in the transaction, the declared value of shipment was obviously under-valued vis- -vis shipment cost (e.g. the transaction makes little financial sense for the seller or the buyer). 9. Inconsistencies between information contained in trade documents and financial flows (e.g. names, addresses, destinations, descriptions of goods), or changes in shipment location or goods shipped. 10. Freight forwarding company listed as final destination. 59 The CRF. Page 102 of 245 11. Obvious alterations to third party documents or the documentation appears illogical, altered, fraudulent or is absent. Customers 12. Customer is involved in the supply, sale, delivery or purchase of dual use goods, or is a military or research body connected with a high risk jurisdiction. 13. Customer activity does not match business profile or end-user information does not match end-user profile. A customer engages in

a transaction that lacks business sense or strategy, or that is inconsistent with historical pattern of trade activity. 14. Order for goods placed by person in foreign country other than the country of the stated end-user. 15. New customer requests letter of credit while awaiting opening of account. 16. Customer vague or inconsistent in information it provides, resistant to providing additional information when queried. 17. The customer or counterparty or its address is similar to one of the parties found on publicly available lists of denied persons or has a history of export control contraventions. Transaction Structure 18. Transaction concerns dual-use goods or military goods. 19. Transaction demonstrates links between representatives of companies exchanging goods (e.g. same owner or management or same address, or providing a residential address or address of registered agent). 20. Transaction involves possible shell companies. 21. Wire transfer or payment from or due to parties not identified on the original letter of credit or other information, or the transaction involves an unusual intermediary, or payment to be made to a beneficiary in a country other than the beneficiary s stated location. 22. Pattern of wire transfers or payment activity that shows unusual patterns or has no apparent purpose, or payment instructions are illogical or contain last minute changes. 23. Circuitous route of shipment and/or circuitous route of financial transactions. Transaction structure (whether shipping route, financing arrangement or documentation) appears unnecessarily complex. Page 103 of 245 SECTION 15 TARGETED FINANCIAL SANCTIONS A. INTRODUCTION 1. This section of the Guidance Notes is to be read and applied in conjunction with Part II, Section 13 Sanctions Compliance and the relevant sector specific guidance that are provided in Part III to Part IX hereof. FSPs should also read the FRA's issued Industry Guidance on Targeted Financial Sanctions 60 . Sanctions queries should usually be directed to the FRA. B. OVERVIEW 1. Financial sanctions are restrictive measures put in place to limit the provision of certain financial services and/ or restrict access to financial markets, funds and other assets 61 to persons or entities. They are generally imposed to: (1) Coerce a regime, or individuals within a regime, into changing their behaviour (or aspects of it) by increasing the cost on them to such an extent that they decide to cease the offending behaviour; and (2) Constrain a target by denying them access to key resources needed to continue their offending behaviour, including the financing of terrorism or nuclear proliferation; (3) Signal disapproval, stigmatising and potentially isolating a regime or individual, or as a way of sending broader political messages nationally or internationally; and/or (4) Protect the value of assets that have been misappropriated from a country until these assets can be repatriated. 2. Targeted financial sanctions (TFS) are a specific type of financial sanction with stated objectives, one of which is the prevention of terrorist financing and proliferation financing. 3. The term TFS means both asset freezing and restrictions and directions to prevent funds or other assets, including virtual assets, from being made available, directly or indirectly, for the benefit of designated persons and entities. In establishing an effective counterterrorist and proliferation financing regime, consideration is also given to respecting human rights, respecting the rule of law, and recognising the rights of innocent third parties.

60 61 According to FATF, the term funds or other assets means any assets, including, but not limited to, financial assets, economic resources (including oil and other natural resources), property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders,

shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets, and any other assets which potentially may be used to obtain funds, goods or services. Page 104 of 245 4. TFS entail the use of financial instruments and institutions to apply coercive pressure on specific parties 62 in an effort to change or restrict their behaviour. Sanctions are targeted in the sense that they apply only to a subset of the population usually the leadership, responsible elites, or operationally responsible persons. The sanctions are financial in that they involve the use of financial instruments, such as asset freezes, blocking of financial transactions or financial services. They are sanctions in that they are coercive measures applied to effect change. 5. Where the financial sanction takes the form of an asset freeze, it is generally prohibited to: (1) Deal with the funds or other assets, belonging to or owned, held or controlled by a designated person or entity; (2) Make funds or other assets available, directly or indirectly, to, or for the benefit of a designated person or entity; or (3) Engage in actions that, directly or indirectly, circumvent the financial sanctions prohibitions. C. RELEVANT SANCTIONS 1. Two key international bodies that impose international sanctions measures are the United Nations (UN) through resolutions passed by the UN Security Council (UNSCRs) and the European Union (EU) through EU regulations 63 . 2. His Excellency the Governor (the Governor), through local designations, can impose domestic financial sanctions in the Cayman Islands. 3. The UK imposes its own financial sanctions and restrictions under the following legislation: (1) Terrorist Asset-Freezing etc. Act 2010 (TAFA 2010); (2) Counter Terrorism Act 2008 (CTA 2008); and (3) Anti-Terrorism, Crime and Security Act 2001 (ATCSA 2001). 4. The UK s Office of Financial Sanctions Implementation (OFSI) publishes a consolidated list of sanctions that provides information to help FSPs decide whether they are dealing with a person or entity that is subject to financial sanctions. It lists full name; any known aliases; honorary, professional or religious titles; date of birth, place of birth; nationality; passport details; national identification numbers; address; any additional information that may be useful; title of the financial sanctions regime under which the designated person or entity is listed; the date when the designated person or entity was added to the list by HM Treasury; when the information regarding the designated person or entity was last updated by HM Treasury and a unique reference number relating to the designated person or entity. 62 Usually, government officials, elites who support them, or members of non-government entities, but this is not exhaustive. 63 The FRA s Industry Guidance provides some detail on how sanctions are imposed. 15%20FRA%20Guidance%20Targeted%20Financial%20Sanctions(1).pdf Page 105 of 245 5. Additionally, the UK Government passes Orders in Council implementing UN, EU and UK sanctions and extending such sanctions to its Overseas Territories through Overseas Orders in Council (OOICs), namely: (1) The Isil (Da esh) and Al-Qaida (Sanctions) (Overseas Territories) Order 2016, and successors; (2) The Afghanistan (UN Measures) (Overseas Territories) Order 2012, and successors; (3) The Democratic People s Republic of Korea (Sanctions) (Overseas Territories) Order 2012, and successors; and (4) The Iran (Sanctions) (Overseas Territories) Order 2016, and successors. 6. It is important for FSPs to note that OOICs have the force of law in the Cayman Islands. 7. It is the responsibility of every FSP to keep itself updated on and comply with the TFS in force in the Cayman Islands. Official sanctions orders applicable in the Cayman Islands are published in the Cayman Islands Gazette. 8. The FRA s website provides a link to the consolidated list of financial sanctions targets, issued by the UK s OFSI, applicable to the Cayman Islands.

[64][65] Additionally, the FRA maintains a Cayman Islands domestic consolidated list of designated persons by the Governor. The Monetary Authority, however, does not guarantee that these lists are accurate, complete and up to date, therefore FSPs need to ensure that they are kept up to date with all applicable sanctions. D. RELEVANT AUTHORITIES 1. His Excellency the Governor (the Governor) is the competent authority for the implementation of TFS in the Cayman Islands. All reports relating to TFS should be made to the Governor through the FRA. 66 2. Effective November 15, 2017, the Governor of the Cayman Islands, delegated the function of receiving reports to the FRA pursuant to: (1) Articles 7(2) 7(4) of The Isil (Da'esh) and Al-Qaida (Sanctions) (Overseas Territories) Order 2016; Articles 22(1) 22(3) of The Afghanistan (UN Measures) (Overseas Territories) Order 2012; (2) Articles 6(2) 6(4) of The Democratic People s Republic of Korea (Sanctions) (Overseas Territories) Order 2012; (3) Articles 8(2) 8(4) of The Iran (Sanctions) (Overseas Territories) Order 2016; and (4) Paragraph 20 of Schedule 4A of the Terrorism Act (2018 Revision). 3. The FRA is the Cayman Islands Financial Intelligence Unit (FIU) with responsibility for receiving, requesting, analysing and disseminating disclosures of information concerning the proceeds of criminal conduct, money laundering and the financing of terrorism. 64 65 The direct link to the OFSI website is consolidated-list-of-targets/consolidated-list-of-targets 66 CRF must be completed when making a report to the FRA. The CRF should be used when reporting suspected designated persons, frozen assets, and suspected breaches of financial sanctions 4. The Sanctions Coordinator (SC) of the FRA is responsible for coordinating the implementation of TFS with respect to terrorism, terrorism financing, proliferation and proliferation financing. The SC will take a holistic approach to ensuring compliance with the sanctions regime to cover the whole lifecycle of compliance. For example: promote compliance by publishing financial sanctions and engaging with the private sector and enable compliance by providing guidance and alerts to help them discharge their own compliance responsibilities. The SC will also perform a central and proactive role in the making of recommendations for designation to the Governor. 5. The Financial Crimes Unit (FCU) is the unit within the Royal Cayman Islands Police Service (RCIPS) with responsibility for investigating all financial crimes within the Cayman Islands. This includes ML investigations, with the exception of ML related to corruption as a predicate offence, which is dealt with by the Anti-Corruption Commission (ACC), and TF investigations. 6. The Monetary Authority, in its role as regulator for FSPs, assesses whether persons or entities under its regulatory Acts are aware of applicable international TFS and any local designations or directions that are in force; and their compliance obligations including, but not limited to, responsibilities for screening and reporting, ongoing monitoring and staff training. The Monetary Authority also reviews regulated entities reports and returns, paying special attention to persons, entities or countries listed on any autonomous list of designations and applicable international TFS. During an inspection, the Monetary Authority will test the effectiveness of systems established by the licensee to observe and comply with TFS in effect. E. COMPLIANCE FUNCTION 1. FSPs should develop a comprehensive compliance programme to comply with the relevant and applicable Acts and obligations and prevent and report ML/TF/PF. Senior management of an FSP should establish a culture of compliance throughout the organisation. 2. During the course of ongoing monitoring of relevant sanctions lists, FSPs may discover that certain TFS are applicable to one or more of their clients, existing or new. Pursuant to the Terrorism Act and the Proliferation Financing (Prohibition) Act, FSPs have certain reporting

obligations to the FRA. It is a criminal offence not to freeze funds or other assets belonging to, owned, held or controlled by a designated person or entity, if an FSP discovers a relationship that contravenes an Order or a direction under the Terrorism Act or Proliferation Financing (Prohibition) Act. 3. FSPs are required to have in place procedures for ongoing monitoring of business relationships or one-off transactions for the purposes of preventing, countering and reporting terrorist and proliferation financing; and extend to allowing for the identification of assets subject to applicable TFS. F. DESIGNATED PERSONS AND ENTITIES 1. Designated persons or entities are established through the designation of sanctions. Financial Sanctions Notices advise of the addition or removal of a designated person or entity from, or amendments to the consolidated list or local Page 107 of 245 designations made in the Cayman Islands by the Governor and are published on the FRA website. 2. The definition of designated person is as prescribed in: (1) Schedule 4A, paragraph 2 of the Terrorism Act (as amended); (2) Part I, Section 2 of the Proliferation Financing (Prohibition) Act (as amended); and (3) The relevant OOICs. G. OBLIGATIONS OF FSPS 1. FSPs must ensure that they comply with their legal obligations to: (1) regularly monitor the sanctions in place including local designations 67 made by the Governor; (2) review their clients against the lists of designated persons or entities and the consolidated list, maintained by the OFSI; (3) freeze any accounts, other funds or economic resources belonging to, owned, held or controlled by designated persons or entities; (4) refrain from dealing with funds or assets or making them available to designated persons or entities, unless licensed by the Governor; (5) report to the Governor, through the FRA, as soon as practicable, if they know or have reasonable cause to suspect that a person is a designated person or has committed an offence under the legislation; and (6) disclose to the Governor, through the FRA, via the CRF 68 , details of any frozen funds or other assets or actions taken in compliance with the prohibition requirements of all applicable sanctions, including attempted transactions 69 . 2. FSPs should ensure that they have adequate resources, policies and procedures to comply with TFS obligations. Regular reviews and updates of TFS policies and procedures must take place to ensure they remain fit for purpose and are enforced. 3. FSPs are required to foster a culture of compliance and ensure that clear, comprehensive policies and procedures are in place to guide employees in ensuring that their legal obligations and these Guidance Notes relating to TFS are being adhered to. 4. FSPs should maintain records of any potential matches to names on sanctions lists and related actions, whether the match turns out to be a true match or a false positive. 5. At a minimum, FSPs should keep the following information about any match: (1) the basis or other grounds which triggered the match (e.g. a hit provided by screening software); (2) any further checks or enquiries undertaken; 67 These designations, when made, are published on the FRA s website. 68 This form can be found on the FRA s website. Page 108 of 245 (3) the associated sanctions regime; (4) the person(s) involved, including any members of compliance or senior management who authorised treatment of the match as a false positive; (5) the nature of the relationship with the person or entity involved, including attempted or refused transactions; and (6) subsequent action taken (e.g. freezing of funds). 6. FSPs should always refer to the up-to-date version of the legislation imposing the specific financial sanctions which apply in each case to understand exactly what is prohibited. 7. FSPs should familiarise themselves with their legal and other obligations and where necessary, seek independent legal advice. 8. If an FSP is unsure whether it is dealing with a designated person or entity, then it should consider requesting more information from the client.

Sanctions/Orders Monitoring 9. FSPs are required to have in place and effectively implement internal controls and procedures to, without delay, ensure compliance with the obligations arising from the designation or delisting of a person or entity. This includes putting systems in place to review the financial sanctions notices and consolidated list of designations; and to screen their client databases against those lists immediately after a change to any of these lists occurs. 10. Screening should also take place at the commencement of any business relationship. This includes screening existing customers when data changes, e.g. change of director or signatory on account; when new financial sanctions notices are issued; and when there are updates to the consolidated list. 11. FSPs should ensure that payments are not indirectly made to or for the benefit of, a targeted person or entity. Thus, screening of directors, beneficial owners, trustees, settlors, beneficiaries and third-party payees against financial sanctions notices and the consolidated list is important. 12. FSPs are required to put systems and controls in place to allow for ongoing monitoring of transactions and to ensure that proper records are kept of these transactions. Asset Freezing/Freezing Mechanisms 13. Once a person or entity has been designated, there is a legal obligation not to transfer funds or make funds or other assets available, directly or indirectly, to that person or entity. FSPs are required to freeze, without delay 70 and without prior notice, the funds or other assets of designated persons and entities. 14. The freezing of assets extends to all funds or other assets, including virtual assets, that are owned, held or controlled by the designated person or entity, and not just those that can be tied to a particular terrorist act, plot or threat; those funds or other assets that are wholly or jointly owned, held or controlled, directly or 70 Without delay should be interpreted in the context of the need to prevent the flight or dissipation of funds or other assets which are linked to terrorist organisations, and those who finance terrorism, and the need for global, concerted action to interdict and disrupt their flow swiftly. Page 109 of 245 indirectly, by designated persons or entities; and the funds or other assets derived or generated from funds or other assets owned, held or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities. 15. Funds generally means financial assets and benefits of every kind 71 , including but not limited to: (1) Cash, cheques, claims on money, drafts, money orders and other payment instruments; (2) Deposits with financial institutions or other entities, balances on accounts, debts and debt obligations; (3) Publicly and privately traded securities and debt instruments, including stocks and shares, certificates representing securities, bonds, notes, warrants, debentures and derivatives contracts; (4) Interest, dividends or other income on or value accruing from or generated by assets; (5) Credit, right of set-off, guarantees, performance bonds or other financial commitments; (6) Letters of credit, bills of lading, bills of sale; and (7) Documents showing evidence of an interest in funds or financial resources. 16. FSPs are prohibited from making any funds, economic resources, other assets or financial or other related services, available, directly or indirectly, wholly or jointly, for the benefit of designated persons and/or entities; entities owned, held or controlled, directly or indirectly, by designated persons or entities; and persons and/or entities acting on behalf of, or at the direction of, designated persons or entities, unless licensed, authorised or otherwise notified in accordance with the relevant Security Council resolutions. False Positives 17. False positives are potential matches to listed persons or entities, either due to the common nature of the name or due to ambiguous identifying data, which on examination prove not to be matches. 18. FSPs must take reasonable steps to ensure that a person or entity identified

as designated is the same person or entity as that on the consolidated list or the local designation made in the Cayman Islands by the Governor, by verifying the name with other identifying information. 19. Distinguishing between designated and non-designated persons or entities may be difficult even with additional identifiers. In some cases, the funds or other assets of a person or entity that was not the intended target of the restrictive measures will be frozen due to identifiers that match with those of a designated person or entity. As a precautionary measure, FSPs should refrain from entering into a business relationship or conduct transactions with any person or entity that the available identifiers match, unless it is clear that it is not the same as the designated person or entity. 71 Including economic resources and virtual assets. Page 110 of 245 20. An FSP should be aware that if a person or entity whose funds or other assets are frozen, claims that they are not the intended target of the restrictive measures, that person or entity should first contact the relevant FSP that froze the funds or other assets, requesting an explanation, including why the relevant FSP believes they are a target match on the consolidated list or to the local designations made in the Cayman Islands by the Governor . The burden of proof concerning determination of a question of a false positive rests with the person or entity, who should submit documentary evidence to the relevant FSP of their identity and a detailed statement as to why they are not the listed person or entity. If the relevant FSP or the person or entity, after using all the available sources cannot resolve the issue as to whether a customer is in fact the designated person or entity, then either should inform the FRA. Training and Internal Controls 21. FSPs should have systems in place to ensure compliance with legal and regulatory obligations in relation to TFS. FSPs should develop and maintain adequate internal controls (including due diligence procedures and training programmes as appropriate) to be able to identify any existing accounts, transactions, funds or other assets of designated persons and/or entities and file any applicable reports with the competent authority. It is essential that FSPs maintain documentation in relation to their sanctions practices. 22. Regular employee training is required in the identification of persons or entities and assets subject to TFS; as well as the processes to be followed where such persons or entities are identified. FSPs should also provide training to employees to ensure proper and efficient recognition and treatment of transactions carried out by, or on behalf of, any person or entity who is or appears to be engaged in terrorist and/or proliferation financing, or whose funds or other assets are subject to TFS. 23. Ongoing training and assessments of employees should be conducted to ensure that they obtain and maintain adequate knowledge of matters related to TFS, sanctions obligations and compliance standards. Reporting Obligations to the Competent Authority 24. FSPs are obligated to report to the relevant competent authority, including the FRA through the Governor, any assets frozen or actions taken in compliance with the prohibition requirements of the applicable TFS, including attempted transactions, as soon as practicable. Reports of frozen funds and economic resources should be submitted to the FRA using the CRF. 25. FSPs must report to the Governor, through the FRA, as soon as practicable, all matches identified on the local designations made in the Cayman Islands by the Governor or on the consolidated list. The report should contain the nature and value of any funds or other assets held. 26. FSPs are obligated to report to the Governor, through the FRA, as soon as practicable, if it is aware of have a reasonable cause to suspect that a person is a designated person or has committed an offence under the legislation. The information reported should include the information or other matter on which the knowledge of suspicion is based; any identifying information that is held about

of 245 the person or entity; the nature and amount of funds or economic resources held by that person or entity. 27. Additionally, FSPs should report, as soon as practicable: (1) the results of searches and/ or examinations of past financial activity by designated persons and/or entities; (2) the details of any other involvement with a listed person or entity, directly or indirectly, or of any attempted transactions involving those persons or entities; (3) the details of incoming transfers or other transaction resulting in the crediting of a frozen account in accordance with the specific arrangements for FSPs; (4) attempts by clients or other persons to make funds or assets available to a designated person or entity without authorisation; and (5) information that suggests the freezing measures are being circumvented. 28. Once a person or entity is delisted, FSPs are also required to advise the Governor, through the FRA, of any actions taken in relation to that de-listed person or entity, as soon as practicable. 29. In addition to their reporting obligations under the sanctions regime, FSPs must file a SAR if they suspect or have grounds to suspect criminal conduct separate from the person or entity being the target of TFS. 30. If an FSP files a SAR about a sanctioned person or entity, a disclosure that a SAR has been filed may constitute tipping-off under the PoCA. 31. The filing of a SAR does not provide protection in respect of offences that may have been committed under sanctions legislation. Unfreezing Assets 32. Upon becoming aware or receiving notification advising that a person or entity is no longer designated under a sanctions regime, an FSP must, without delay, confirm whether they have frozen funds or other assets of any such person or entity; verify that the person or entity is no longer subject to the asset freeze; remove the person or entity from the FSP s list of persons or entities subject to financial sanctions; and unfreeze the funds or other assets of the person or entity and reactivate the relevant accounts. 33. The FSP is required to submit notification to the person or entity that the assets are no longer subject to an asset freeze and notify the Governor through the FRA of the actions taken. H. EXEMPTIONS AND LICENSING Exemptions 1. In certain circumstances, an individual can make a transfer to a sanctioned person or entity. Freezing obligations are subject to certain exemptions in limited circumstances. Page 112 of 245 2. An exemption to a prohibition applies automatically in certain defined circumstances and does not require an FSP to obtain a licence from Governor. 3. Asset freezing legislation generally permits the following payments into a frozen account without the need for a licence from the Governor, provided those funds are frozen after being paid in: (1) any interest or earnings on the account; and/ or (2) any payments due to a designated person or entity under contracts, agreement or obligations that were concluded or arose before the date the person or entity became sanctioned. 4. The legislation also generally permits the crediting of a frozen account with payments from a third party without the need for a licence, provided that the incoming funds are also frozen, and that the Governor is informed of the transaction without delay. Licensing 5. A licence is a written authorization from the Governor permitting an act otherwise prohibited under the sanctions. The licence can include additional reporting requirements or have a time limitation. 6. The overall objective of the licensing system in terrorist asset freezing cases is to minimise the risk of diversion of funds to terrorism, while respecting including those of bona fide third parties. To this end, the Governor may grant licences to allow exceptions to the freeze. If a licence is being granted under an OOIC, the Governor must obtain the consent of the UK Secretary of State; whereas a licence issued pursuant to the Terrorism Act requires the Governor to consult with the UK Secretary of State. 7. Some common licensing grounds found in the OOICs are for basic needs, legal fees and disbursements, fees or service charges for routine

holding or maintenance of frozen funds or other assets, satisfaction of prior contractual obligations of the designated person or entity, and extraordinary expenses. 8. Any person seeking a licence for the release of funds or other assets, which are subject to an asset freeze , must submit an application to the Governor using the prescribed form72 which is available on the FRA s website. The application must be supported by evidence to demonstrate that all the licensing criteria are met. 9. An FSP must provide evidence to support an application. As such, applicants are required to provide: (1) the licensing ground(s) being relied upon in the application including supporting arguments; (2) full information on the parties involved in the proposed transaction including, inter alia, the designated person(s) or entities and any financial institution(s) involved; (3) ultimate beneficiary of the transaction; (4) the complete payment route, including account details; and (5) the amount (or estimated amount) of the proposed transaction. 72 The relevant form can be obtained from the FRA s website. Page 113 of 245 10. In cases where the application for a licence is considered urgent, this needs to be clearly stated. The basis of the urgency and supporting evidence establishing a basis for the urgency should be included in the application. It is important to note that there is no guarantee that the application will be treated urgently. It is at the discretion of the competent authority that an application be treated as urgent. 11. Employees and clients of FSPs need to be clear about the specific permissions contained in the licence, as they must be strictly complied with. It is important to note that licences are not issued retrospectively. Additionally, FSPs must be mindful that engaging in transactions or attempting to transact with a designated person or entity without obtaining a licence is a breach of financial sanctions legislation and therefore, a criminal offence. I. ADDITIONAL SCREENING GUIDANCE 1. Screen for full name, date of birth, address and aliases. 2. Sanctioned parties are known to use false personal information to try and evade detection. Additionally, information held by an institution may not exactly correlate to information recorded on the consolidated list or the local designation made in the Cayman Islands by the Governor. 3. To maximise screening, seek to incorporate variables such as: (1) Different spellings of names (e.g. Abdul instead of Abdel); (2) Name reversal (first/middle names written as surnames and vice versa); (3) Shortened names (e.g. Bill instead of William); (4) Maiden names; (5) Removing numbers from entities; and (6) Insertion/removal of full stops and spaces. 4. If using automated screening, the following actions may assist to improve screening quality: (1) Understanding the capabilities and limits of the particular automated screening system. (2) Ensuring the system is calibrated to the FSP s needs. (3) Checking the matching criteria is relevant and appropriate for the nature and the size of business to ensure less false positives are produced. (4) Ensuring screening rules are appropriately defined e.g. allow for the use of alternative identifiers. (5) The calibration of systems to include the use of fuzzy matching. Fuzzy matching searches for words or names likely to be relevant, even if words or spelling do not match exactly. It can assist to identify possible matches where data is misspelled, incomplete or missing. (6) Ensuring prominent flagging of matches so that they are clearly identifiable. (7) Keeping calibration and automated systems under regular review to ensure they are fit for purpose. Page 114 of 245 SECTION 16 ONGOING MONITORING A. APPLICABILITY 1. This section of the Guidance Notes applies to all persons conducting relevant financial business in the Cayman Islands. B. OVERVIEW OF ONGOING MONITORING 1. FSPs are required to understand the purpose and intended nature of the business relationship which it has with a customer. FSPs shall assess and ensure that the nature and purpose of the business relationship is in line with its

expectation of the customer, and this information should form the basis for ongoing monitoring. Conducting ongoing monitoring is essential for FSPs to maintain understanding of a customer and the business relationship, keep the CDD documents up-to-date, review and revise risk assessments as appropriate, and identify unusual transactions and activities and report. 2. Pursuant to its obligations under the AMLRs, an FSP is required to conduct ongoing monitoring on a business relationship to the extent reasonably warranted by the risk of ML/TF/PF and sanctions-related risks. Ongoing monitoring includes: (1) Ensuring that documents, data or information collected under the customer due diligence process remains current and relevant to the customer. This is done by reviewing existing customer s records based on their assigned level of risk, and/or based on a change in their profile; and (2) Reviewing of transactions conducted to ensure that they are consistent with the FSP s knowledge of the customer, which may include the customer s source of funds and source of wealth, along with the customer s occupation and/or business. 3. Ongoing monitoring is not a customer-driven rule, but rather a transaction-driven rule. Failure to adequately monitor for activity occurring within FSPs because such monitoring is done solely on account or direct customer basis may put FSPs at risk for AML/CFT deficiencies. 4. The figure below summarises the cycle for ongoing monitoring, which forms part of the Monetary Authority s expectations for the AML/CFT compliance programmes of FSPs. Page 115 of 245 Figure:Process for Ongoing Monitoring C. INTERNATIONAL FRAMEWORK 1. Recommendation 10 of the FATF s 40 Recommendations highlights that financial institutions should be required to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of customers 73 . 2. 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. Where the risks of ML or TF are higher, financial institutions should be required to conduct EDD 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 1 . D. DOMESTIC LEGISLATION 1. The AMLRs outline the requirements of a person carrying out relevant financial business to implement procedures and systems to scrutinise transactions and 73 Financial Action Task Force. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. (June 2019) ONGOING MONITORING CYCLE Page 116 of 245 review customer documentation with the aim to prevent money laundering, terrorist financing, proliferation financing and sanctions-related breaches. 2. These requirements are set out in Regulations 5 and 12 of the AMLRs. E. OBLIGATIONS OF FSPS 1. FSPs must develop and apply written policies and procedures relating to ongoing monitoring as part of their AML/CFT compliance programme. 2. The risks associated with ML, TF and PF are different, therefore FSPs are expected to put in place measures tailored to each of these risks. As an example, ML risk may be increased with unusual large transactions, while TF or PF risks are increased with unusual small transactions in targeted jurisdictions. Reviewing Customer Information 3. FSPs policies and procedures must document appropriate risk-based measures for ensuring that data or information collected during the customer s onboarding process are kept up-to-date and relevant by undertaking routine reviews of existing records. 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 intentions of the customer, nature and risk of the transactions and business relationships should determine the documentation maintained as part of the FSP s records. Particular attention should be paid to higher risk categories of customers and their business relationships. 5. FSPs must assess the information received as a part of ongoing monitoring to determine whether it affects the risk associated with the business relationship. Where the basis of a relationship has changed, FSPs must re-evaluate the risk rating of the customer. Also, FSPs must carry out further CDD procedures to ensure that the revised risk rating and basis of the relationship is fully understood. Ongoing monitoring procedures must take into account changes in the customer s risk. If the risk changes significantly, then EDD or SDD should be applied 74 . 6. As part of its periodic reviews, an FSP is required to update the CDD records as determined by the customer s assigned level of risk or on the occurrence of a triggering event (see paragraph 16 of this subsection), whichever is earlier. 7. If an FSP has a suspicion of ML, TF, PF or sanction-related breaches, then the FSP is required to make the relevant disclosures to the competent authority. 8. FSPs must ensure that its customers are periodically screened against required sanctions lists (see the section on Targeted Financial Sanctions) as a part of their ongoing monitoring and periodic review processes, in order to identify and freeze assets of and report designated persons to the relevant authorities without delay. 9. Policies and procedures must clearly outline the remedial action required when the required CDD documentation or information is not held on file, including the 74 FSPs may conduct SDD in case of lower risks identified, while EDD must be applied where higher risks are identified. various steps that should be taken to locate or obtain such documentation or information. Transactions Monitoring 10. FSPs must be able to identify the transactions/activities of customers during the course of the business relationship, that is, the anticipated type, volume and value of transactions/activities. The aim is to ensure that transactions/activities are consistent with the FSPs knowledge of the customer, the customer risk assessment, and the purpose and intended nature of the business relationship. 11. Ongoing monitoring of transactions is an essential component, which aids in identifying transactions/activities that are unusual or potentially suspicious, therefore FSPs are to ensure that they have a robust process in place to monitor transaction activities. The intention is to reduce the possibility of the occurrence of ML/TF/PF or sanctions breach without detection and to meet the obligations set out in the AMLRs. 12. It is expected that transactions monitoring and transactions processing are carried out by separate functions, to minimise any possible conflicts of interest. 13. It is recognised that the most effective method of monitoring of accounts is achieved through a combination of automated and manual solutions. It is important to note that a culture of compliance coupled with well-trained, vigilant staff aid in forming an effective monitoring system overall. 14. An FSP s transactions monitoring process should be well-documented and subjected to regular reviews including assurance testing, to ensure their process is functioning adequately in identifying any potential suspicious ML/TF/PF activities or sanctions-related breaches. 15. FSPs must be able to identify changes in the nature of the relationship with the customer over time. Trigger Events 16. The transactions monitoring programme for FSPs should provide for the identification of possible trigger events and how they should be interpreted. Potential trigger events which FSPs could consider include the following: (1) A material change in ownership and/or management structure; (2) Reclassification of the jurisdiction, where the customer or

respondent institution is based; (3) The identification or entry of a PEP in the business relationship; (4) Inconsistencies between customer information and supporting verification evidence; (5) Identification of adverse information from sources such as media reports or other relevant sources; or (6) Customer requesting a new or higher risk product. 17. Based on their own assessment, FSPs should conduct a review of all trigger events associated with its customers. While examples of trigger events should be provided to staff, training should also be delivered in order to inform staff how to identify new and emerging trigger events. FSPs should beware that compiling a Page 118 of 245 definitive list of trigger events is a non-risk-based mechanism which could result in an inadequate transaction monitoring process. Unusual Transactions (refer also to Section 9 of Part II of the Guidance Notes) 18. FSPs should have adequate policies and procedures to identify unusual transactions. These transactions may include: (1) Transactions that are inconsistent with customer profile; (2) Transactions that do not follow the same pattern compared with the customer s normal activity or that of a similar customer, products or services; (3) Transactions where the FSP is not aware of a reason or lawful purpose or doubts the validity of the information submitted. 19. FSPs should be able to identify unusual transactions and regularly review the information they hold to ensure that any new or emerging information that could affect the risk assessment is identified in a timely manner. 20. Where an FSP s customer base is homogenous, and where the products and services provided to customers result in uniform patterns of transactions or activities, e.g. deposit-taking activity, it will be more straightforward to establish parameters to identify unusual transactions/activities. However, where each customer is unique, and where the product or service provided is bespoke, e.g. acting as trustee of an express trust, an FSP will need to tailor their monitoring to the nature of its business and facilitate the application of additional judgement and experience to the recognition of unusual transactions/activities. 21. Where an alert has been generated, either by an automated system or a manual review of the customer file, FSPs should attempt to establish the reason for changes in behaviour and take appropriate measures, such as conducting additional CDD and if warranted, submitting the relevant disclosures to the FRA, such as a SAR or a CRF. Monitoring Systems 22. FSPs should consider implementing risk-based transactions monitoring systems commensurate with the size, nature and complexity of their business, whether automated or otherwise. If an FSP implements a system that is partially or fully automated, then they should understand its operating rules, they should perform integrity verification on a regular basis and ensure that it addresses the identified ML/TF/PF or sanctions-related breaches. FSPs are responsible for the quality of all outputs from any automated system, including those from third-party vendors. 23. Transactions monitoring systems should be reviewed regularly to ensure that that the systems are operating appropriately and effectively. Furthermore, they should be reviewed to accommodate changes for emerging risks, new trends and regulations. 24. Examples of the types of monitoring systems FSPs should put in place may include: Page 119 of 245 (1) Transaction monitoring systems that detect anomalies or suspicious patterns of behaviour, including the unexpected use of a product in a way for which it was not designed; (2) Systems that identify discrepancies between submitted and detected information, for example, between submitted country of origin information and the electronically detected IP address; (3) Systems that compare data submitted with data held on other business relationships and that can identify patterns such as the same funding instrument or the same contact details; (4) Systems that identify whether the product is used with merchants

dealing in goods and services that are associated with a high risk of financial crime and/or sanctioned entity. Frequency of Review 25. The frequency of ongoing monitoring for any customer should be determined by the level of risk associated with the business relationship. The application of SDD to low risk customers does not exempt FSPs from the obligation to conduct ongoing monitoring or from their duty to report suspicious activities to the FRA. Where FSPs have applied SDD in case of low risk scenarios, FSPs may choose to adjust the extent of ongoing monitoring of the business relationship commensurate with the low risks. Where ML, TF and PF risks are high, FSPs should apply enhanced monitoring, increasing the frequency and intensity. For more details on the identification and assessment of risks, FSPs should refer to Section 3 of Part II of these Guidance Notes. 26. When assessing CDD obligations in relation to the ongoing monitoring of customers, FSPs should ensure that they have effective and relevant ongoing monitoring policies and procedures in place, which are adhered to by all staff. 27. FSPs should have a well-documented and efficient ongoing monitoring programme in place, which demonstrates a risk-based approach where higher risk customers are reviewed on a more frequent basis. 28. FSPs should demonstrate a periodic review of all customers, the frequency of which is decided by the FSP and based on the level of ML/TF/PF or sanctions- related risks associated with the customer. Therefore, FSPs are expected to adjust the level of ongoing monitoring in line with their institutional risk assessment and individual customer risk profiles. Staff with responsibility for this function should be provided with training on how to carry out such a review.

PART III SECTOR SPECIFIC GUIDANCE: BANKS AND OTHER DEPOSIT TAKING FINANCIAL INSTITUTIONS The purpose of this part of the Guidance Notes is to establish the obligations and provide some guidance specifically for the Banks and Other Deposit Taking Financial Institutions sector. The types of FSPs covered in Part III are: (1) Retail and Non-Retail Banks; (2) Credit Unions; and (3) Building Societies. This sector specific guidance addresses specialised areas of relevant financial business that require more and / or different guidance or explanation than dealt with in the general body of these Guidance Notes. Part III should be read in conjunction with Part I and Part II of the Guidance Notes and the Appendices. SECTION 1 RETAIL BANKS AND NON-RETAIL BANKS A. OVERVIEW 1. Section 2 of the Banks and Trust Companies Act defines banking business as: the business of receiving (other than from a bank or trust company) and holding on current, savings, deposit or other similar account money which is repayable by cheque or order and may be invested by way of advances to customers or otherwise . 2. Banking encompasses a wide range of financial products and services, which include, but are not limited to: (1) Retail banking, where banks offer products and services directly to personal and business customers (including legal arrangements), such as current accounts, loans (including mortgages) and savings products; (2) Corporate and investment banking, where banks provide corporate finance and corporate banking products and investment services to corporations, governments and institutions; (3) Investment services (or wealth management), where banks provide products and services to manage their customers wealth (sometimes referred to as private banking); and (4) Correspondent services, where banking services are provided by one bank (the correspondent bank) to another bank (the respondent bank). 75 The guidance on correspondent banking are provided in Part II of these Guidance Notes. B. SCOPE 1.

This sector specific guidance seeks to provide practical assistance to Retail Banks and Non-Retail Banks (collectively, Banks) in complying with the AMLRs, interpreting and applying the general provisions of these Guidance Notes, and for Banks to adopt sound risk management and internal controls for their operations. 2. The AMLRs apply to Banks as indicated in the list of activities falling within the definition of Relevant Financial Business in the Sixth Schedule of the Act. 3. It is the responsibility of each Bank to have systems and training in place to prevent ML/TF. This means that each Bank must maintain AML/CFT policies and procedures appropriate for the purposes of forestalling and preventing ML/TF. C. ML/TF RISKS 1. Certain products and services offered by Banks may pose a higher risk of ML or TF depending on the nature of the specific product or service offered. 2. Such products and services may facilitate a higher degree of anonymity, or involve the handling of high volumes of currency or currency equivalents. Some of these products and services are listed below, but the list is not all inclusive: 75 FATF Guidance for a Risk-Based Approach The Banking Sector (October 2014) Page 122 of 245 Retail Banking (1) The provision of services to cash-intensive businesses is a particular area of risk associated with retail banking. Some businesses are legitimately cash based and so there will often be a high level of cash deposits associated with some accounts. The risk is in failing to identify such businesses where the level of cash activity is higher than the underlying business would justify. 76 Wealth Management (2) Wealthy and powerful customers may be reluctant or unwilling to provide adequate documents, details and explanations. The situation with regards to these types of customers can be exacerbated where the customer occupies a high public profile, and may fall into the category of a PEP indicating that they wield or have recently wielded political or economic power or influence. Additionally, wealthy customers often have many accounts in more than one jurisdiction, either within the same firm or group, or within different firms, which may be more difficult for wealth managers to accurately assess the true purpose and business rationale for individual transactions. 77 Correspondent Banking (3) The correspondent bank often has no direct relationship with the underlying customers of the respondent bank and therefore may have limited information on a transaction and may not be in a position to verify their identities. Correspondent banks often have limited information regarding the nature or purpose of the underlying transactions, particularly when processing electronic payments. Correspondent banking relationships, if poorly controlled, can allow other financial services firms with inadequate AML/CFT systems and controls, and customers of those firms 78 , direct access to international banking systems. Lending (4) The main ML/TF risk arises through the acceleration of an agreed repayment schedule, either by means of lump sum payments, or early termination. Additionally, the involvement of multiple parties may increase the risk of ML/TF when the source and use of the funds are not transparent. This lack of transparency can create opportunities in any of the three stages of ML/TF financing schemes. Payable Through Accounts (5) PTA may be prone to higher risk because banks may not implement the same due diligence requirements for PTAs that they require of other customers who want to open checking and other accounts. These banks 76 - 77 The Joint Money Laundering Steering Group Prevention of money laundering/combating terrorist financing Guidance for the UK Financial Sector Part II Sectoral Guidance (Amended November 2014) 78 Financial institutions with poor AML/CFT systems are vulnerable to ML/TF risks and could be misused by the money launderers. Page 123 of 245 then process thousands of sub-accountholder cheques and other transactions, including currency deposits,

through the foreign financial institution s PTA. In most cases, little or no independent effort is expended to obtain or confirm information about the individual and business sub-accountholders that use the PTAs. The potential for facilitating ML or TF and other serious crimes increases when a bank is unable to identify and adequately understand the transactions of the ultimate users of its account with a foreign correspondent. 79 Trade Financing (6) The international trade system is subject to a wide range of risks and vulnerabilities that provide criminal organizations with the opportunity to launder the proceeds of crime and move funds to terrorist organizations with a relatively low risk of detection. The involvement of multiple parties on both sides of any international trade transaction can make the process of due diligence more difficult. Also, due to the fact that trade finance can be more document-based than other banking activities, it can be susceptible to documentary fraud, which can be linked to ML/TF. While banks should be alert to transactions involving high-risk goods (e.g., trade in weapons or nuclear equipment), they need to be aware that any good may be over or under-valued in an effort to evade AML/CFT or customs regulations, or to move funds or value across national borders. 80 D. RISK BASED APPROACH 1. Banks must adopt a risk-based approach to managing ML/TF risks. The risk-based approach to AML/CFT aims to support the development of prevention and mitigation measures that are commensurate to the ML/TF risks identified. This applies to the way banks allocate their compliance resources, organize their internal controls and internal structures, and implement policies and procedures to deter and detect ML/TF. 2. The bank s risk assessment forms the basis of a bank s RBA. In identifying and assessing the ML/TF risk to which they are exposed, Banks should consider a range of factors which may include 81 : (1) The nature, scale, diversity and complexity of their business; (2) Target markets; (3) The number of customers already identified as high risk; (4) The jurisdictions the bank is exposed to, either through its own activities or the activities of customers, especially jurisdictions with relatively higher levels of corruption or organised crime; (5) The distribution channels, including the extent to which the bank deals directly with the customer or the extent to which it relies (or is allowed to rely on) third parties to conduct CDD and the use of technology; The internal audit and regulatory findings; and (6) The volume and size of its transactions, considering the usual activity of the bank and the profile of its customers. 79 Bank Secrecy Act Anti-Money Laundering Examination Manual Payable Through Accounts - Overview 80 Bank Secrecy Act Anti-Money Laundering Examination Manual Trade Finance Activities - Overview 81 FATF - Risk-based approach guidance for the banking sector Page 124 of 245 E. CUSTOMER DUE DILIGENCE Who is the Customer/Applicant for Business? 1. The applicant may be any one of the following: (1) Natural persons; (2) Corporate persons (including MSBs, other deposit taking financial institutions, trust and fiduciary customers, companies); and (3) Partnerships / Unincorporated Businesses. 2. The following are the applicants whose identity must be verified by Banks and the evidence of identity required in each case: Applicant for Business CDD Requirements (Highlights and supplementary only please refer to Section 4 of Part II of the Guidance Notes for the full (normal) CDD requirements). Natural Persons (1) CDD documentation to identify and verify that identity should be obtained for the customer and, where appropriate, beneficial owner(s) of accounts. (2) Satisfactory evidence of identity, name and address confirmed by using one or more of the verification methods outlined in section 4 of Part II of the Guidance Notes. (3) Information, including necessary documentation required to understand the purpose and intended nature of the business relationship as outlined in section 4 of Part II

of the Guidance Notes. Note: As stated in paragraph 16, Section 4, Part II of these Guidance Notes, it is usually not sufficient to rely on one document or data source and the extent of documentation and data that an FSP needs to collect depends on the risk assessment of the customer. FSPs must also be aware that some documents are more easily forged than others. Additionally, under the RBA, where there are higher risks, FSPs are required to take enhanced measures to manage and mitigate those risks. In such cases, Banks should supplement their verification documentation with references from other FSPs that are banks as in (4) below or with references from a respected professional (e.g. Attorney) or other appropriate reference with whom the customer maintains a current relationship. (4) Current, satisfactory bank reference from at least one bank with whom the prospective customer has had a relationship for not less than 3 years. If one is not forthcoming, satisfactory reference from a person or entity who has personal knowledge of the prospective customer and which establish his bona fides and integrity. References confirmed for genuineness. Genuineness may be confirmed by directly contacting the referee either via or telephone. Page 125 of 245 (5) For non-face-to-face verification, suitably certified or authenticated documents. Note: Given the international nature of banking business in and from the Cayman Islands, Bank FSPs should also be particularly vigilant in ensuring that CDD documentation collected that are in a foreign language are appropriately translated and verified and the copy of the translation kept with the original document. (6) Evidence of identity required for assets bought, sold or managed through the relationship. Corporate customers (including MSBs, other deposit taking financial institutions, trust and fiduciary customers, companies) (1) CDD as set out in Part II Section 4. N.B. Paragraphs 14 to 17 and 42 to 49 (of Part II Section 4). (2) Consistent with that required for natural persons, documentary evidence of identity for all directors that are natural persons; all those with signing powers, including third parties; and beneficial owners. (See Section 4 of Part II in the Guidance Notes). (3) Documentary evidence of identity of the new owner/controller where there is a change in ownership or control, in accordance with that required of natural persons. Partnerships / Unincorporated Businesses (1) Identification information and satisfactory evidence of its existence, confirmed by at least one of the following independent checks, of existence of partnership / unincorporated business: (a) Partnership agreement or excerpt if relevant (b) Certificate of Registration (if applicable) (2) Consistent with that required for direct personal customers, documentary evidence of identity required for partners/managers; all those with signing powers; all relevant parties, including third parties; and controlling partners / shareholders/beneficial owners as defined in the Guidance Notes, Section 4 (e.g., excerpt from partnership document. (3) Documentary evidence of identity of the new owner/controller where there is a change in ownership or control, in accordance with that required of direct personal relationships. When must identify be verified? 3. Customer verification information must be obtained and verification should be conducted prior to opening the account or establishing the business relationship. 4. Where the verification information is not forthcoming at the outset or within a reasonable time after initial contact, the relationship must be re-evaluated and transactions must not proceed. Page 126 of 245 When might it be possible to rely on third-parties to verify identity? 5. Banks should use their judgment in determining whether or not in the context of banking they should place reliance on third parties for conducting the due diligence procedures (verification). However, such reliance should only be considered in situations where the ML/TF risks have been

assessed as low and where there is no suspicion of ML/TF. 6. Refer to Section 5 of the Part II of the Guidance Notes, for details on SDD and Procedure for Introduced Business . F. ENHANCED DUE DILIGENCE (EDD) 1. In the case of high-risk situations/customers, the bank has to conduct EDD. Customers that pose high ML or TF risks present increased exposure to banks; in such cases, banks should apply EDD. EDD for high-risk customers is especially critical in understanding their anticipated transactions and implementing a suspicious activity monitoring system that reduces the bank s reputation, compliance, and transaction risks. High-risk customers and their transactions should be reviewed more closely and more frequently throughout the term of their relationship with the bank. 2. NPOs (including Charities), PEPs, Correspondent Banking, Trade Financing and customers in High-Risk Countries are some factors to consider which may result in EDD. Additional examples would include cases whereby a customer is confidentiality-driven or presents a multi-layered structure of beneficial ownership. 3. In applying EDD, banks may for example collect sufficient information regarding intra-group relationships, if any; types of customers; service providers; and trading partners to establish a trading profile which can be monitored against transactions. More examples of EDD measures are provided in Section 6, Part II of the Guidance Notes. G. ON-GOING MONITORING 1. Banks should conduct on-going monitoring of the business relationship. On-going monitoring includes the scrutiny of transactions to determine whether those transactions are consistent with the Bank s knowledge of the customer and the nature and purpose of the business relationship. Monitoring also involves identifying changes to the customer profile and keeping it up to date, which may require the application of new, or additional CDD measures. Monitoring transactions is an essential component in identifying transactions/activities that are potentially suspicious. 2. Monitoring should be carried out on a continuous basis or triggered by specific transactions. It could also be used to compare a customer s activity with that of a peer group. For some types of banking activity where large volumes of transactions occur on a regular basis, automated systems may be the only realistic method of monitoring transactions. However, where automated systems are used, banks should understand their operating rules, verify their integrity on a regular basis and check that they address the identified ML/TF risks. Page 127 of 245 3. Banks should adjust the level of monitoring in line with their institutional risk assessment and individual customer risk profiles. Enhanced monitoring should be required for high risk situations. The adequacy of monitoring systems and the factors leading banks to adjust the level of monitoring should be reviewed regularly for continued relevance to the bank s AML/CFT risk programme. 82 4. Refer to Section 16 of Part II of the Guidance Notes, On-Going Monitoring , for additional details. H. ML/TF WARNING SIGNS OR RED FLAGS 1. The following are examples of potentially suspicious activities or red flags for ML/TF. Although these lists are not all-inclusive, they may help banks recognize possible ML/TF schemes. The below red flags, when encountered, may warrant additional scrutiny. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny will assist in determining whether the activity is unusual or suspicious or one for which there does not appear to be a reasonable business or legal purpose. Transactions Involving Large Amounts of Cash 2. The following are some of the warning signs and red flags that Banks should be alert to in respect of transactions. The list is not exhaustive, but includes: (1) Frequent withdrawal of large cash amounts that do not appear to be justified by the customer s business activity. (2) Frequent withdrawal of large amounts by means of cheques, including traveller s cheques. (3)

Customers making large and frequent cash deposits but cheques drawn on the accounts are mostly to individuals and firms not normally associated with their business. (4) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad. (5) A large amount of cash is withdrawn and immediately deposited into another account. (6) Exchanging an unusually large number of small-denominated notes for those of higher denomination. (7) Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank. (8) Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash, rather than by way of debits and credits normally associated with the normal commercial operations of the company (e.g. cheques, letters of credit, bills of exchange). (9) Depositing cash by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the cumulative total of which is substantial. (10) The deposit of unusually large amounts of cash by a customer to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments. 82 FATF Guidance for a Risk-Based Approach The Banking Sector (October 2014) Page 128 of 245 (11) Aberrant customer transactions of large cash deposits using cash deposit machines or similar facilities, thereby avoiding direct contact with the bank. (12) Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions. (13) Customers whose deposits contain counterfeit notes or forged instruments. (14) Customers who use cash advances from a credit card or charge card account to purchase money orders or bank drafts to transfer funds to foreign destinations. (15) Customers who take cash advances from a credit card or charge card account to deposit into another account. (16) Large cash payments for outstanding credit card or charge card balances. (17) Customers who maintain positive balances on their credit card or charge card and then request cash advances or other type of refunds. Transactions Involving Transfers Abroad 3. The following are some of the warning signs and red flags that Banks should be alert to in respect of transactions involving cross-border transfers. The list is not exhaustive, but includes: (1) Large and regular payments that cannot be clearly identified as bona fide transactions, from and to countries or jurisdictions that are high-risk, which include jurisdictions that are associated with (a) the production, processing or marketing of narcotics or other illegal drugs or (b) terrorism or related criminal conduct. (2) Substantial increase in cash deposits by a customer without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account or to a destination not normally associated with the customer. (3) Repeated transfers of large amounts of money abroad accompanied by the instruction to pay the beneficiary in cash. (4) Building up large balances, not consistent with the known turnover of the customer s business, and subsequent transfer to account(s) held overseas. (5) Cash payments remitted to a single account by a large number of different persons without an adequate explanation. (6) U-turn transactions, i.e. where funds received from a person or company in a foreign country or jurisdiction are immediately remitted to another person or company in the same country or foreign jurisdiction, or to the sender s account in another country or jurisdiction. Electronic Payments 4. The following are some of the warning signs and red flags that Banks should be alert to in respect of electronic payments. The list is not exhaustive, but includes: (1) Multiple electronic payments ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements. (2)

Electronic payments to or for an individual where information on the originator, or the person on whose behalf the transaction is conducted, is not provided with the wire transfer, when the inclusion of such information would be expected. Page 129 of 245 (3) Use of multiple personal and business accounts or the accounts of NPOs to collect and then funnel funds immediately or after a short time to a small number of foreign beneficiaries. (4) Foreign exchange transactions that are performed on behalf of a customer by a third party followed by electronic payments of the funds to locations having no apparent business connection with the customer or to countries of ML/TF concern. Lending 5. The following are some of the warning signs and red flags that Banks should be alert to in respect of lending. The list is not exhaustive, but includes: (1) Loans secured by pledged assets held by third parties unrelated to the borrower. (2) Loans secured by deposits or other readily marketable assets, such as securities, particularly when owned by apparently unrelated third parties. (3) Borrower defaults on cash-secured loan or any loan that is secured by assets that are readily convertible into currency. (4) Loans are made for, or are paid on behalf of, a third party with no reasonable explanation. (5) To secure a loan, the customer purchases a certificate of deposit using an unknown source of funds, particularly when funds are provided via a currency or multiple monetary instruments. (6) Loans that lack a legitimate business purpose, provide the bank with significant fees or assuming little or no risk, or tend to obscure the movement of funds (e.g., loans made to a borrower and immediately sold to an entity related to the borrower or back to back loans without any identifiable and legally admissible purpose). Trade Finance 6. The following are some of the warning signs and red flags that Banks should be alert to in respect of trade finance. The list is not exhaustive, but includes: (1) Items shipped that are inconsistent with the nature of the customer s business (e.g., a steel company that starts dealing in paper products, or an information technology company that starts dealing in paper products). (2) Customers conducting business in high-risk jurisdictions. (3) Customers shipping items through high-risk jurisdictions. (4) Customers involved in potentially high-risk activities, including activities that may be subject to export/import restrictions. (5) Obvious over or under pricing of goods and services. (6) Obvious misrepresentation of quantity or type of goods imported or exported. (7) Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction. (8) Customer requests payment of proceeds to an unrelated third party. (9) Shipment locations or description of goods not consistent with letter of credit. (10) Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment. Page 130 of 245 Employee Activity 7. The following are some of the warning signs and red flags that Banks should be alert to activities of their own employees. The list is not exhaustive, but includes: (1) Employee lives a lavish lifestyle that cannot be supported by his salary. (2) Employee fails to adhere to bank s internal policies, procedures, and processes and frequently overrides internal controls. (3) Employee is reluctant to take a vacation. Page 131 of 245 SECTION 2 CREDIT UNIONS A. CREDIT UNIONS 1. Section 2 of the Cooperative Societies Act defines credit union business , in relation to a registered society (i.e., a society that, among other criteria, has as its object the promotion of the economic interest of its members in accordance with cooperative principles), as: "The business of (1) promoting thrift among the members of the society by the accumulation of their savings; (2) creating sources of credit for the benefit of the members of the society at a fair and reasonable rate of interest; (3) using and controlling the members savings for their mutual benefit; and (4) training and educating the

members in the wise use of money and in the management of their financial affairs. B. SCOPE 1. This sector specific guidance seeks to provide practical assistance to credit unions in complying with the AMLRs, interpreting and applying the general provisions of these Guidance Notes, and for credit unions to adopt sound risk management and internal controls for their operations. 2. The AMLRs apply to credit unions as indicated in the list of activities falling within the definition of Relevant Financial Business in the Sixth Schedule of the Act. 3. It is the responsibility of each credit union to have systems and training in place to prevent ML/TF. This means that each credit union must maintain identification procedures, record-keeping procedures, and such other procedures and controls appropriate for the purposes of forestalling and preventing ML/TF. C. ML/TF RISKS 1. Credit unions should consider all relevant risk factors at the sectorial and business relationship levels in conducting risk assessments and determining the appropriate level of mitigating measures to be applied. 2. Risk factors related to credit union business activities include, but are not limited to: (1) Money transfers to third parties; (2) Third parties paying in cash on behalf of the member; (3) Unusual loan or savings patterns (including regular significant payments); (4) Reluctance to provide documentary evidence of identity when joining; (5) Large One-Off transactions e.g. sudden loan repayment; and (6) Regular requests for loans that are soon repaid. Page 132 of 245 D. RISK BASED APPROACH 1. Credit unions must adopt a risk-based approach to managing ML/TF risks. The risk-based approach to AML/CFT aims to support the development of prevention and mitigation measures that are commensurate to the ML/TF risks identified. 2. The credit union needs to take a number of steps, documented in a formal policy which assesses the most effectual and proportionate way to manage ML and TF risks. These steps are: (1) Identify the ML and TF risks that are relevant to the credit union; (2) Assess the risks presented by the credit unions : (a) Members (b) Products (c) Delivery channels (3) Design and implement controls to manage and mitigate these assessed risks; and (4) Monitor and improve the effective operation of these controls. E. CUSTOMER DUE DILIGENCE (CDD) Who is the Applicant for Business? 1. The applicant for business is a natural person. 2. The following are the applicants whose identity must be verified by credit unions and the evidence of identity required in each case: Applicant for Business Requirements Natural Persons (1) Identification documentation should be obtained for the customer and beneficial owners of accounts. (2) Evidence of identity required for assets bought, sold or managed through the relationship. (3) Satisfactory evidence confirmed by using one or more of the verification methods outlined in Section 4 Part II of the Guidance Notes. (4) Current, satisfactory bank reference from at least one bank with whom the prospective customer has had a relationship for not less than 3 years. If one is not forthcoming, satisfactory reference from a person or entity who has personal knowledge of the prospective customer and which establish his bona fides and integrity. (5) References confirmed for genuineness. This can be achieved by or telephone confirmations. (6) For non-face to face verification, suitably certified or authenticated documents. When must identity be verified? 3. A credit union must obtain identity information prior to accepting a person s application to become a member. Page 133 of 245 F. ENHANCED DUE DILIGENCE (EDD) 1. EDD is required in cases where a credit union is exposed to high ML/TF risks i.e., where the customer and product/service combination is considered to be a greater risk. (Refer to Part II, Section 6 of these Guidance Notes and Part VI of the AMLRs for additional information). EDD is required to mitigate the high ML/TF risks. 2. Example of high risk scenarios include 83 : (1) where the member is a PEP (2) when the member is involved in a business that is

considered to present a high ML/TF risk 3. The nature and extent of EDD to be applied will depend on the nature and severity of the ML/TF risks identified. Examples of EDD measures are provided in Part II Section 6 of these Guidance Notes. The credit union should satisfy itself the EDD measures undertaken have sufficiently mitigated the risks identified. G. ON-GOING MONITORING 1. Credit unions must establish a process for monitoring member transactions and activities, which will highlight unusual transactions and those which need further investigation. It is important to take into account the frequency, volume and size of transactions. The key elements to monitoring are having up-to-date member information on the basis of which it will be possible to recognize the unusual transaction, and to ask pertinent questions to elicit the reasons for unusual transactions. 2. Refer to Section 16 of Part II of these Guidance Notes, On-Going Monitoring . H. ML/TF WARNING SIGNS OR RED FLAGS 1. The following are examples of potentially suspicious activities or red flags for ML/TF. Although these lists are not all-inclusive, they may help credit unions recognize possible ML/TF schemes. The below red flags, when encountered, may warrant additional scrutiny. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny will assist in determining whether the activity is unusual or suspicious or one for which these does not appear to be a reasonable business or legal purpose. Customer Behaviour 2. The following are some of the warning signs and red flags that Credit Unions should be alert to in respect of customer behaviour. The list is not exhaustive, but includes: (1) Member uses unusual or suspicious identification documents or refuses to produce originals for verification. (2) Member refuses to provide personal background information when opening an account. 83 A high-risk customer does not mean that they will be involved in ML/TF or other criminal activity but that there is an increased possibility of such activity. Page 134 of 245 (3) Member s permanent address is outside of the credit union s service area. (4) Member indicates that he/she does not want a statement of account or any mail sent to his/her address. (5) A member is reluctant to provide information about the nature and purpose of the member s business or expected account activity. (6) Member asks about record-keeping or reporting requirements. (7) Member discourages employee from filing required reports or complying with recordkeeping requirements. (8) Member reluctant to proceed with cash transaction after being told it must be reported. Cash Transactions 3. The following are some of the warning signs and red flags that Credit Unions should be alert to in respect of cash transactions. The list is not exhaustive, but includes: (1) Member regularly uses ATMs to make several deposits below the reporting threshold. (2) Member comes in with another member and they go to different tellers to conduct currency transactions under the reporting threshold. (3) Member opens different accounts under different names, and then makes several cash deposits under the reporting threshold. (4) Member deposits cash into several accounts in amounts below the reporting threshold and subsequently transfers the funds into one account and wire transfers them overseas. (5) Member attempts to take back a portion of the proposed cash deposit after learning that the proposed cash deposit exceeds the reporting threshold. (6) Member makes numerous purchases of monetary instruments with cash in amounts less than the reporting threshold. (7) Member purchases a number of prepaid cards for large amounts, inconsistent with normal account activity. Credit Transactions 4. The following are some of the warning signs and red flags that Credit Unions should be alert to in respect of credit transactions. The list is not exhaustive, but includes: (1) Member suddenly pays down or pays off a large loan with no credible explanation as to where the funds came from. (2) Member purchases certificates of deposit

and uses them as loan collateral. (3) Loans are made for, or paid on behalf of, a third party with no plausible explanation. (4) Member s loan proceeds are unexpectedly transferred offshore or member requests that loan proceeds be wire transferred. Page 135 of 245 Employee Activity 5. The following are some of the warning signs and red flags that Credit Unions should be alert to in respect of employee activity. The list is not exhaustive, but includes: (1) Employee lives a lavish lifestyle that cannot be supported by his salary. (2) Employee fails to adhere to credit union s internal policies, procedures, and processes and frequently overrides internal controls. (3) Employee is reluctant to take a vacation. Page 136 of 245 SECTION 3 BUILDING SOCIETIES A. BUILDING SOCIETIES 1. A Building Society is a financial institution that provides banking and other financial services to its members (i.e. the people who invest in savings schemes and those who hold mortgages and other accounts with them). Building societies offer banking and related financial services, especially savings and mortgage lending. B. SCOPE 1. This sector specific guidance seeks to provide practical assistance to Building Societies in complying with the AMLRs, interpreting and applying the general provisions of these Guidance Notes, and for Building Societies to adopt sound risk management and internal controls for their operations. 2. The AMLRs apply to Societies as indicated in the list of activities falling within the definition of Relevant Financial Business in the Sixth Schedule of the Act. 3. It is the responsibility of each building society to have systems and training in place to prevent ML/TF. This means that each building society must maintain identification procedures, record-keeping procedures, and such other procedures and controls appropriate for the purposes of forestalling and preventing ML/TF. C. ML/TF RISKS 1. Building societies should consider all relevant risk factors at the sectorial and business relationship levels in order to assess the ML/TF risks and determine the appropriate level of mitigating measures to be applied. 2. Risk factors related to building society business activities include, but are not limited to: (1) Third parties paying in cash on behalf of the member; (2) Unusual loan or savings patterns (including regular significant payments); (3) Reluctance to provide documentary evidence of identity when joining; (4) Large One-Off transactions e.g. sudden loan repayment; and (5) Regular requests for loans that are soon repaid. Page 137 of 245 D. RISK BASED APPROACH 1. Building societies should adopt a risk-based approach to managing ML/TF risks. The risk-based approach to AML/CFT aims to support the development of prevention and mitigation measures that are commensurate to the ML/TF risks identified. 2. The building society needs to take a number of steps, documented in a formal policy which assesses the most effectual and proportionate way to manage ML and TF risks. These steps are: (1) Identify the ML and TF risks that are relevant to the building society; (2) Assess the risks presented by the building societies : (a) Members (b) Products (c) Delivery channels (d) Geographical areas of operation (3) Design and implement controls to manage and mitigate these assessed risks; and (4) Monitor and improve the effective operation of these controls. E. CUSTOMER DUE DILIGENCE Who is the applicant for business? 1. The applicant may be any one of the following: (1) Natural persons; (2) Corporate persons (including MSBs, companies); and (3) Partnerships / Unincorporated Businesses. 2. The following are the applicants for business whose identity must be verified by building societies and the evidence of identity required in each case: Applicant for Business Requirements Natural Persons (1) Identification documentation should be obtained for the customer and beneficial owners of accounts. (2) Evidence of identity required for assets bought, sold or managed through the relationship. (3) Satisfactory evidence confirmed by using one or more of the

verification methods outlined in Section 4 of the Guidance Notes. (4) Current, satisfactory bank reference from at least one bank with whom the prospective customer has had a relationship for not less than 3 years. If one is not forthcoming, satisfactory reference from a person or entity who has personal knowledge of the prospective customer and which establish his bona fides and integrity. Page 138 of 245 (5) References confirmed for genuineness. Genuineness may be confirmed by directly contacting the referee either via or telephone. (6) For non-face to face verification, suitably certified or authenticated documents. Corporate customers (including MSBs, companies) (1) CDD as set out in Part II Section 4. N.B. Paragraphs 14 to 17 and 37 to 42 (of Part II Section 4). (2) Consistent with that required for natural persons, documentary evidence of identity for all directors that are natural persons; all those with signing powers, including third parties; and beneficial owners. (See Section 4 of Part II in the Guidance Notes). (3) Documentary evidence of identity of the new owner/controller where there is a change in ownership or control, in accordance with that required of natural persons. Partnerships / Unincorporated Businesses (1) Identification information and satisfactory evidence of its existence, confirmed by at least one of the following independent checks, of existence of partnership / unincorporated business: (a) Partnership agreement or excerpt if relevant (b) Certificate of Registration (if applicable) (2) Consistent with that required for direct personal customers, documentary evidence of identity required for partners/managers; all those with signing powers; all relevant parties, including third parties; and controlling partners / shareholders/beneficial owners as defined in the Guidance Notes, Section 4 (e.g., excerpt from partnership document. (3) Documentary evidence of identity of the new owner/controller where there is a change in ownership or control, in accordance with that required of direct personal relationships. When must identity be verified? 3. A building society must obtain identity information prior to accepting a person s application to become a member. 4. Where the verification information is not forthcoming at the outset or within a reasonable time after initial contact, the relationship must be re-evaluated, and transactions must not proceed. When might it be possible for identity to be verified by a party not based in the Cayman Islands? 5. Where the building society is relying on another entity within its group to verify the identity of a member who may not be physically present in the jurisdiction, all documentation must be certified by a senior manager within the group entity and copies provided prior to any outward transaction. Page 139 of 245 F. ENHANCED DUE DILIGENCE (EDD) 1. EDD is required in cases where the credit union is exposed to high ML/TF risks i.e., where the customer and product/service combination is considered to be a greater risk. (Refer to Part II, Section 6 of these Guidance Notes and Part VI of the AMLRs for additional information). EDD is required to mitigate the high ML/TF risks. 2. Example of high-risk scenarios include 84 : (1) where the member is a PEP (2) when the member is involved in or is a business that is considered to present a high risk for ML/TF 3. In applying EDD the building society may for example, collect sufficient information regarding intra-group relationships, if any; types of customers; service providers; and trading partners to establish a trading profile which can be monitored against transactions. The nature and extent of EDD to be applied will depend on the nature and severity of the ML/TF risks identified. More examples of EDD measures are provided in Section 6, Part II of the Guidance Notes. The FSP should satisfy itself the EDD measures undertaken have sufficiently mitigated the risks identified. G. ON-GOING MONITORING 1. Building societies must conduct on-going monitoring of the business relationship with its members.

On-going monitoring of a business relationship includes: (1) Scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions are consistent with the building society s knowledge of the member, his/her business and risk profile; (2) Ensuring that the documents, data or information held by the building society are kept up to date and relevant. 2. Monitoring member activity is useful in identifying unusual/suspicious transactions/activities. On-going monitoring helps to adjust the mitigating measures proportionate to the risks and apply appropriate CDD measures. 3. Refer to Section 16 of Part II of these Guidance Notes, On-Going Monitoring , for additional details. H. ML/TF WARNING SIGNS OR RED FLAGS 1. The following are examples of potentially suspicious activities or red flags for ML/TF. Although these lists are not all-inclusive, they may help building societies to recognise possible ML/TF schemes. The below red flags, when encountered, may warrant additional scrutiny. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny will assist in determining whether the activity is suspicious or one for which these does not appear to be a reasonable business or legal purpose. 84 A high-risk customer does not mean that they will be involved in ML/TF or other criminal activity but that there is an increased possibility of such activity. Page 140 of 245 (1) A member provides minimal, vague or fictitious information that cannot be easily verified. (2) Frequent deposits or withdrawals of large amounts of cash with no apparent business source, or the business is of a type not known to generate substantial amounts of cash. (3) Accounts with a high volume of activity, which carry low balances or are frequently overdrawn. (4) A member makes large deposits and maintains large balances with little or no apparent justification. (5) A sudden, unexplained increase in account activity, both from cash and non-cash items. An account may be opened with a nominal balance that subsequently increases rapidly and significantly. (6) Reluctance to provide the purpose of the loan, or the stated purpose is ambiguous. (7) Inappropriate disbursement of loan proceeds, or disbursements for purposes other than the stated loan purpose. (8) A member suddenly pays down or pays off a large loan, with no evidence of refinancing or other explanation. (9) Loans are made for, or are paid on behalf of, a third party with no reasonable explanation. (10) Loans secured by pledged assets held by third parties unrelated to the borrower. (11) Loans that lack a legitimate business purpose. Employee Activity 2. The following are some of the warning signs and red flags that Building Societies should be alert to in respect of employee activity. The list is not exhaustive, but includes: (1) Employee lives a lavish lifestyle that cannot be supported by his salary. (2) Employee fails to adhere to the FSP s internal policies, procedures and processes and frequently overrides internal controls. (3) Employee is reluctant to take a vacation. Page 141 of 245 GUIDANCE NOTES ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING ,TERRORIST FINANCING AND PROLIFERATION FINANCING IN THE CAYMAN ISLANDS PART IV SECTOR SPECIFIC GUIDANCE: FIDUCIARY (COMPANY FORMATION AND TRUSTS) The purpose of this part of the Guidance Notes is to establish the obligations and provide some guidance specifically for the Fiduciary sector (Company Formation and Management and Trusts) on more complex AML / CFT matters or issues which require more explanation than provided for in the general body of these Guidance Notes. This sector specific guidance should be read in conjunction with Part I and Part II of the Guidance Notes. Page 142 of 245 SECTION 1 COMPANY FORMATION AND MANAGEMENT A. OVERVIEW 1. Company formation and management business carried out in and from the Cayman Islands is defined and regulated pursuant to the

Companies Management Act (2021 Revision) and the Directors Registration and Licensing Act, 2014. 2. There are a number of FSPs under other regulatory Acts that are allowed to engage in company formation and management activity without being required to hold a licence under the Companies Management Act. Those FSPs that operate within such circumstances are required to comply with the AML/CFT framework outlined in this Section and under the general guidance which are designed for company management and formation services professionals (CSPs). B. SCOPE 3. This guidance is specific to CSPs and is intended to provide support in complying with the AMLRs. 4. The AMLRs apply to CSPs as indicated in the list of activities falling within the definition of Relevant Financial Business in the Sixth Schedule of the PoCA. 5. CSPs must have systems and training in place to prevent ML/TF. This means that each CSP must maintain ML and TF policies and procedures appropriate for the purposes of preventing ML and TF. C. ML/TF RISKS 1. The company is an extremely versatile vehicle that is often used in various structures and for a broad range of activities, including financial structures, financial transactions, and the management and custody of wealth. 2. In spite of the many varied legitimate uses of companies, companies are vulnerable to being improperly utilised to perpetrate fraud, illegally hide the ownership of assets, hide the proceeds of corruption, perpetrate ML schemes, or to facilitate TF. 3. There is potential for companies to be misused to facilitate ML/TF activity at various stages by allowing the conversion of proceeds of crime or disguising financing for illicit and terrorist activity. D. CUSTOMER DUE DILIGENCE Who is the Applicant for Business? Company Formation 1. In the case of forming a company, the applicant for business is the ultimate customer upon whose instructions the company is formed. This may or may not be a proposed shareholder. In addition to obtaining identification evidence for the customer, as outlined in Part II, Section 4 of these Guidance Notes, the FSP Page 143 of 245 will normally be required to obtain: (1) an explanation of the nature of the proposed company s business, (2) the source of funds; (3) satisfactory evidence of the identity of each of the proposed beneficial owners; and (4) satisfactory evidence of the identity of each of the proposed directors (and in the event of corporate directors, evidence of the identity of the natural persons that will be acting on the corporate directors behalf). CSPs should understand the ownership and control structure. 2. In some circumstances, reliance may be placed on the due diligence of other persons. (Refer to the section on Introduced Business in Part II Section 5 E of the Guidance Notes). Company Management 3. Where a CSP provides corporate services to a company, the CSP must look behind the company for due diligence purposes and, depending upon the circumstances, investigate and obtain proof of identity of any or all of the following: (1) the shareholders (or beneficial owners if different from the registered shareholders); (2) the directors and officers; (3) anyone who is giving instructions to the CSP on behalf of the company; and (4) anyone who introduces any of the above persons to the CSP. 4. Where a CSP provides corporate services to a company, the CSP must understand the ownership and control structure. At the start of the arrangement, the CSP should establish the legal status of any legal persons or arrangements in the structure and monitor the same on an ongoing basis. Business Introduction 5. However, it is recognised that obtaining due diligence on all of the above in every case could be onerous and could lead to a duplication of procedures, unnecessary complication and eventual loss of legitimate business. The AMLRs and the Guidance Notes therefore, allow for reliance, in certain circumstances, on third party intermediaries. For guidance in this area see section on Introduced Business in Section 5 in Part II of the Guidance Notes. Where the CSP is

approached by a shareholder or beneficial owner, or directors or officers as the applicant for business, the CSP should carry out appropriate due diligence on: (1) the shareholders and beneficial owners; (2) the directors and officers; and (3) anyone who gives instructions to the company manager on behalf of: (a) the company; (b) the directors and officers of the company; or (c) the shareholders and beneficial owners of the company. 6. This must be done in accordance with the requirements pertaining to Corporate Customers outlined in Part II of the Guidance Notes. Page 144 of 245 7. Where the CSP is approached by a person who gives instructions to the CSP on behalf of the company, the CSP should carry out appropriate due diligence on that person (the applicant for business), the shareholders, and the directors and officers of the company in accordance with the requirements pertaining to Corporate Customers outlined in Part II of the Guidance Notes. 8. However, it may, in certain circumstances, be acceptable to rely solely on the due diligence of the person giving those instructions. (Refer to the section on Introduced Business in Part II Section 5 E of the Guidance Notes). 9. Where the CSP relies upon the due diligence of an introducer, such a decision must be made by senior management and the reasons for the decision must be documented. In addition, the CSP must carry out appropriate due diligence on the introducer or intermediary to ensure their eligibility and ensure that written undertakings are received from the introducer or intermediary in accordance with the Guidance Notes. Structured Finance Companies 10. Where a company is established to undertake one or more structured finance transactions, it may be established by a trustee (the applicant for business) or an Arranger for that transaction or generally. In such cases, the FSP must identify the parties and the commercial purpose and conduct enquiries on any or all of the following persons and entities as appropriate in the circumstances, with a view to ensuring that appropriate due diligence and anti-money laundering compliance is applied to the identity of the investors/note holders and persons that control the flow of the funds, in accordance with the AMLRs and Guidance Notes. 11. Such enquiry may extend to any or all of the following: (1) the arranger; or (2) the originator; or (3) where relevant, the promoter; (4) investors in the securities of the company; and (5) other relevant parties. Private Trust Companies 12. In the case of a PTC (as defined in the PTCR), the applicant for business will usually be the settlor(s) of the trusts of which the PTC will be trustee. 13. In addition to the due diligence required to be obtained in the company formation and company management sections above, it will be necessary to obtain the due diligence recommended in Part III Section 2 Trusts of these Guidance Notes, save to the extent not already obtained in respect of the PTC itself. Discontinued Relationships 14. Funds held to the order of a customer or prospective customer should only be returned to the source from which they came and not to a third party, save for some exceptional instances such as where there is need to comply with a court order in case of controllership. Page 145 of 245 Ongoing Monitoring 15. In order to be alert for instances of ML/TF, CSPs must continue monitoring the activities of their client companies for signs of unusual or suspicious activities. 16. Activities that warrant special attention include: (1) changes in transaction type, frequency, unusually large amounts, geographical origins and destinations attributes; (2) changes in account signatories; (3) changes in use of the company from the originally stated purpose; and (4) changes which involve money flows into dormant companies. 17. It is important that monitoring systems be implemented to detect and deter ML/TF activity and such systems should be tested for effectiveness on an ongoing basis. 18. This is an ongoing process which will require periodic refinement to the approach. However, the focus should

be to understand changing risks, while maintaining additional implementation of effective ML/TF controls. Additional effective ML/TF controls should be implemented as appropriate. Hold Mail and c/o Addresses 19. Sometimes the directors or beneficial owners of client companies request that mail not be forwarded but held at the registered office for storage or later collection. In such cases FSPS should follow the guidance set out in Part II Section 6 B (EDD Hold Mail Accounts) and extend its application to beneficial owners where necessary. 20. Customers who request c/o addresses should also receive additional attention. 21. CSPs should understand and document the customers rationale for requesting c/o and Hold Mail services. Bearer Shares 22. The Cayman Islands Companies Act (2023 Revision) does not allow the issue of bearer shares. 23. In circumstances where a CSP provides corporate services to a foreign company that has issued bearer shares, the CSP is directed to: (1) maintain proof of identity of all of the following: (a) the beneficial owners; (b) the directors and officers; (c) any person who gives instructions to the CSP on behalf of the company; and (2) maintain proof of identity of any custodian of the bearer shares, or person in like capacity, who can at all times verify the identity of the ultimate beneficial owner of the bearer shares. 24. In circumstances where a CSP provides corporate services to a company that is owned by a structure that has vehicles owned through bearer instruments, the Page 146 of 245 CSP must ensure that it can at all times verify the ultimate beneficial owners and natural persons that control the company. Changes in Service Provider 25. Customers have the right to choose which CSP should manage their affairs and to change to others if they so desire. 26. However, CSPs who are asked by a prospective customer to take over the management of a company which is being managed by another service provider should communicate with that service provider and make appropriate enquiries as to the reason for the transfer of business. E. RISK BASED APPROACH 1. CSPs must adopt a risk-based approach to managing ML and TF risks as set out in Part II Section 3 of these Guidance Notes. 2. In identifying and assessing the ML/TF risk to which they are exposed, CSPs should consider a range of factors, which may include: (1) the nature, scale, diversity and complexity of their business; (2) target markets; (3) the number of customers already identified as high risk; (4) the jurisdictions the CSP is exposed to, either through its own activities or the activities of customers, especially in jurisdictions with relatively higher levels of corruption or organised crime; and (5) the internal audit function and regulatory findings. F. ML/TF WARNING SIGNS 1. In taking on new business or in monitoring existing business relationships, CSPs should consider that particular structures, customers and activities may pose a higher ML/TF risk. However, just because a factor is listed below, does not automatically make the relationship high-risk provided that suitable controls are in place. 2. Some potentially higher risk services include: (1) ownership and management structures that consist of nominee arrangements, where the actual beneficial owner is unclear or undisclosed; (2) complex networks of legal persons and/or arrangements (e.g. multiple layers or tiers of intermediate persons or arrangements) where there is no clear rationale for the structure proposed and/ or result in a lack of transparency without an acceptable explanation; (3) complex structures that span a number of different jurisdictions, with no clear legitimate rationale; (4) Commercial, private, or real property transactions or services with no apparent legitimate business, economic, tax, family governance, or legal reasons; (5) trading entities for which CSPs provide management services, particularly where the customer retains some control, or where there is difficulty in monitoring movement of goods, services and financial flows; Page 147 of 245 (6) customers who

request third-party signatories on bank accounts (including themselves); (7) structures and customers that are involved with or connected to higher risk businesses or activities including cash and cash equivalent businesses such as casinos or money services businesses and businesses or industries that are more prone to higher levels of corruption such as oil, mining, pharmaceuticals or defence (arms); (8) structures and customers that are involved with or connected to high risk jurisdictions; and (9) Involvement of PEPs in the structures, including where the PEP may not be the CSP s customer. Page 148 of 245 SECTION 2 TRUSTS A. OVERVIEW 1. Corporate trust business carried out in and from the Cayman Islands is regulated pursuant to the BTCA, and the PTCR. The BTCA defines trust business as the business of acting as trustee, executor or administrator . 2. Trust business may be divided into three categories for the purposes of the AMLRs and these Guidance Notes: (1) unit trusts which are therefore covered by the sector specific guidelines relating to mutual funds, in relation to their creation and administration; (2) bare trusts or nomineeships where the trustee is acting both as a trustee and as an agent; and (3) all other express trusts, including trusts created under the Special Trust Alternative Regime (STAR), where the trust is not a mutual fund and the trustee is a principal as a matter of law. B. SCOPE 1. This guidance is intended for all providers of trusts, where the trust is not a mutual fund and the trustee is a principal as a matter of law. C. ML/TF RISKS 1. The Trust sector is particularly exposed to the risk of being utilised to perpetrate a fraud or a ML scheme, or to facilitate TF. 2. Some of the core risk areas include: (1) At the layering and integration stages of money laundering there is greater potential for the misuse of trusts. (2) Once the illegal proceeds have already entered the banking system, trusts could be exploited to further confuse the links between these proceeds and the illicit activity that generated them. D. RISK-BASED APROACH 1. There is no single approach that will detect and prevent all money laundering or terrorist financing. 2. However, a risk-based approach aims to balance the cost burden placed on individual businesses and on their customers with a realistic assessment of the threat of the business being used in connection with money laundering or terrorist financing. 3. FSPs must adopt a risk-based approach to managing ML and TF risks. The risk- based approach to AML/CFT aims to support the development of prevention and mitigation measures that are commensurate to the ML/TF risks identified. This applies to the way FSPs allocate their compliance resources, organize their internal controls and internal structures, and implement policies and procedures Page 149 of 245 to deter and detect ML/TF. 4. In identifying and assessing the ML/TF risk to which they are exposed, FSPs should consider a range of factors which may include: (1) the nature, scale, diversity and complexity of their business; (2) target markets; (3) the number of customers already identified as high risk; (4) the jurisdictions the FSP is exposed to, either through its own activities or the activities of customers (including settlors, protectors, beneficiaries), especially in jurisdictions with relatively higher levels of corruption or organised crime; and (5) the internal audit function and regulatory findings. 5. The FSP s risk-based approach will ensure that its strategies are focused on deterring, detecting and disclosing in the areas of greatest perceived vulnerability. 6. The FSP needs to take a number of steps, documented in a formal policy which assesses the most effectual and proportionate way, to manage ML and TF risks. These steps include: (1) identifying the ML and TF risks that are relevant to the FSP; (2) assessing the risks, including those presented by the FSP s: (a) ownership and Management; (b) products; (c) delivery channels; (d) geographical areas of operation; (3) designing and implementing controls to manage and

mitigate the assessed risks; and (4) monitoring and improving the effective operation of these controls. E. SYSTEMS, POLICIES AND PROCEDURES Who is a Customer/Applicant for Business? Settlor 1. Where a new trust is being created, the Applicant for Business will be the settlor (or all of the settlors if more than one). Settled Assets 2. FSPs should also make appropriate inquiry as to the source of the assets a settlor intends to settle. 3. Assets settled, and their source, will necessarily vary from case to case and depend on many factors, such as the type of trust intended to be created, the relative and absolute value of the assets intended to be settled, the objectives of the settlor in creating the trust and the timeframe within which the parties are working. Page 150 of 245 Transfer of an Existing Trust 4. Where an FSP is approached to become an additional or successor trustee, it is recognised that the concept of an Applicant for Business can be another trustee. Customer Due Diligence Ongoing Obligations 5. FSPs must recognise the need to adopt ongoing procedures for vetting any settlors to a trust and the source of the funds that are introduced to the trust. In particular, each time assets are added to the trust by a new or existing settlor the same procedures must be followed. Trust Companies and Private Trust Companies 6. In the case of PTCs, consider whether some or all of the due diligence recommended to be obtained in accordance with the Company Formation and Management section of these Guidance Notes should be obtained, save to the extent not already obtained in respect of the settlor(s). 7. A trust company acting as trustee of a trust should collect due diligence documentation on: (1) the settlor (including any person subsequently settling funds into the trust) and any person who directly or indirectly provides trust property or makes a testamentary disposition on trust or to the trust; (2) any co-trustee; (3) any protector; (4) any enforcer (in respect of trusts created under STAR); (5) any named beneficiary with a vested right; (6) any other beneficiary with a vested right; and (7) any other person exercising ultimate effective control over the trust. Previous Due Diligence 8. Trustees act as a body. Additional or successor trustees step into the shoes of the existing or predecessor trustees. 9. An FSP who is an additional or successor trustee should inquire of the existing or predecessor trustees whether appropriate inquiries were made of the settlor or settlors at the time of creating the trust and at the time of addition of any assets to the trust, and seek to obtain the originals or copies of the relevant due diligence documentation (e.g. verification of the settlor s identity and source of funds). Having done so, the FSP should consider whether it is adequate, according to the circumstances of the particular case. 10. However, in some cases, such documentation may not be available or upon review may not be adequate. In such cases the FSP should make reasonable inquiries of its own: (1) Where the Settlor is Alive: Where the settlor is still alive, the FSP should make the relevant inquiries of the settlor. Page 151 of 245 (2) Where the Settlor is dead: Where the settlor is dead, the FSP should make reasonable inquiries about the settlor of such persons as may be appropriate in the circumstances of the particular case e.g. the existing or predecessor trustees or the beneficiaries. In particular, if the beneficiaries are relatives of the deceased settlor, as will often be the case, appropriate inquiry of the oldest beneficiaries may be the most fruitful. Simplified/Enhanced Due Diligence Simplified Due Diligence 11. Section 21 of the AMLRs states that, a person carrying out relevant financial business may apply SDD measures where lower risks have been identified, and the SDD shall be commensurate with the lower risk factors . 12. The simplified measures shall be commensurate with the lower risk factors but are not acceptable whenever there is suspicion of money laundering or terrorist financing, or higher risk scenarios apply. Enhanced Due Diligence 13. Risk factors that

may indicate high risk, and should therefore be carefully assessed to determine if there is indeed high risk and need for EDD include circumstances where: (1) a customer is resident in another country or territory; (2) a customer is not physically present for identification purposed; or (3) a customer is a company with nominee shareholders. F. ML/TF WARNING SIGNS 1. FSPs are urged to be particularly vigilant in the following areas: (1) Links with high risk and non-cooperative jurisdictions. (2) Certain countries are associated with crimes such as drug trafficking, fraud and corruption and consequently pose a higher potential risk to FSPs. Conducting a business relationship with such a country exposes the FSP to reputational risk and legal risk. 2. FSPs are advised to consult publicly available information to ensure that they are aware of those countries/territories described in 1(1) above. A source of relevant information for FSPs is the FATF website at Other useful websites include: the Financial Crimes Enforcement Network (FinCEN) at for country advisories; the Office of Foreign Assets Control (OFAC) for information pertaining to US foreign policy and national security; and Transparency International, for information on countries vulnerable to corruption. 3. FSPs should exercise additional caution and conduct EDD on individuals and/or entities based in high-risk countries. Caution should also be exercised in respect of the acceptance of certified documentation from individuals/entities based in high-risk countries/territories and appropriate verification checks undertaken on such individuals/entities to ensure their legitimacy and reliability. Page 152 of 245 Total Changes of Beneficiaries 4. Where all of the existing beneficiaries are removed and different beneficiaries are added, or where this is intended, or where the trust is intentionally structured to permit this, heightened scrutiny is required by the FSP. The FSP should ensure that it documents a clear rationale for changes to the originally stated beneficiaries or classes of beneficiaries. 5. There may be perfectly legitimate reasons for this occurring or for this to be possible, but FSPs should endeavour to ascertain what these are. Unexplained Requests for Anonymity 6. Where the settlor s stated reason for establishing a trust is the need for anonymity or confidentiality in relation to himself or the beneficiaries, the FSP should ensure that it is clear on the legitimacy of settlor s purposes and rationale prior to taking on such business. 7. It should not be automatically inferred that this in itself is an illegitimate need. There are many instances where a settlor may desire that the extent or nature of his wealth is not known to third parties such as children, the media, business or industry colleagues, potential kidnappers, industry competitors etc. The legitimate need for privacy is acknowledged and supported in the Cayman Islands as in other countries and may be a reason for establishing a trust. 8. However, FSPs are encouraged to adopt a conservative and cautious approach in this area. In particular, where the reasons given by the settlor for the need for anonymity or confidentiality are not clear or are unconvincing, FSPs should take appropriate further action. Beneficiaries with no apparent connection to the settlor 9. Another red flag or warning sign is where there is no readily apparent connection or relationship of the settlor to the beneficiaries. 10. Since the economic nature of a trust is a mechanism for the settlor to benefit a beneficiary, typically not in return for any consideration (payment, transfer of assets or provision of services), FSPs should endeavour so far as possible to ascertain the settlor s reasons for wanting to benefit a beneficiary with whom he seemingly has no connection. 11. This can be a matter of great sensitivity (for example, where the beneficiary turns out to be an illegitimate child of the settlor) and FSPs are encouraged to take this into account while pursuing necessary or appropriate inquiries. Unexplained Urgency 12. FSPs are encouraged to inquire as to the reasons for any urgency,

especially where the settlor is indicating that some of the due diligence process can or will be completed after the trust has been established or a transaction has been entered into by the trustees or an underlying company owned by the trust. Page 153 of 245 Potentate Risk 13. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose FSPs to significant reputational and/or legal risk. The risk occurs when such persons abuse their public powers for either their own personal benefit and/or the benefit of others through illegal activities such as the receipt of bribes or fraud. Such persons commonly referred to as (PEPs) or potentates include heads of state, ministers, influential public officials, judges and military commanders. 14. Provision of financial services to corrupt PEPs exposes FSPs to reputational risk and costly information requests and seizure orders from law enforcement or judicial authorities. In addition, public confidence in the ethical standards of a whole financial system can be undermined. 15. FSPs are encouraged to be vigilant in relation to PEPs from all jurisdictions; in particular High Risk Countries who are seeking to establish business relationships. FSPs should, in relation to PEPs, in addition to performing normal due diligence measures: (1) have appropriate risk management systems to determine whether the customer is a PEP; (2) obtain senior management approval for establishing business relationships with such customers; (3) take reasonable measures to establish the source of wealth and source of funds; and (4) conduct enhanced ongoing monitoring of the business relationship. 16. FSPs should obtain senior management approval to continue a business relationship once a customer or beneficial owner is found to be, or subsequently becomes a PEP. 17. See Section 7 of Part II of these Guidance Notes Politically Exposed Persons. Private Trust Companies 18. In the case of FSPs that provide registered office services to PTCs, when a PTC is the applicant for business, including in respect of registered office services, the applicant for business will usually be the settlor(s) of the trusts of which the private trust company will be trustee. 19. The due diligence recommended for registered office service providers to PTCs is the same as recommended in the Company Formation and Company Management Sections of these Guidance Notes. 20. PTCs must have in place controls to comply with the ML/TF framework in the jurisdiction. 21. In the case that a PTC is managed by an FSP, the FSP must ensure that its ML/TF controls extend to the services that it provides to the PTC, including training and record retention controls. Page 154 of 245 Trusts established under STAR 22. Where any of the objects of a trust is a purpose, whether or not charitable, FSPs are encouraged to understand the rationale for establishing the trust. In such circumstances additional attention should be paid to the parties to the trust and the source of any funds settled in the trust. 23. In cases where any of the objects of a trust is a charity, FSPs should make best effort to determine the legitimate nature of the charity and make best efforts to satisfy themselves that the beneficiary charity is not being utilized to facilitate ML/TF activity. FSPs should document the results of any research or investigation of the legitimacy and goals of the charity in such situations. Other warning signs 24. Additional warning signs to which FSPs should be particularly alert include the following: (1) situations where there is no clear rationale for the structure proposed and/ or result in a lack of transparency without an acceptable explanation or where it is inordinately difficult to identify (where relevant) the beneficiaries; (2) complex structures that span a number of different jurisdictions, with no clear rationale; (3) structures involving legal persons and legal arrangements that involve high value goods and/or transactions; (4) structures or customers that are involved with or connected to higher risk

jurisdictions; (5) structures that involve trust assets that originate or reside in higher risk jurisdictions; (6) involvement of PEPs in the structures, including where the PEP may not be the CSP s customer/client; (7) customers that invest or settle using cash or request cash distributions; (8) customers that insist on retaining control of the trust assets; (9) In the case of express trusts, an unexplained relationship between a settlor and beneficiaries with a vested right, other beneficiaries and persons who are the object of a power; (10) an unexplained nature of classes of beneficiaries and classes within an expression of wishes. (11) customers who request third party signatories on bank accounts (including themselves); (12) beneficial owners who wish to retain control over assets through powers delegated; customer does not cooperate with FSP s requests for information; (13) customers who are introduced by an overseas source based in a country noted for drug production or distribution or a customer introduced by an overseas branch, affiliate in a country not assessed by the FSP as having a low degree of risk of ML/TF; (14) customers who are introduced by or engaged as a service provider by other TCSPs, financial institutions, and other designated non-professional businesses and professions who are not subject to adequate AML/CFT laws and measures and who are not adequately supervised; Page 155 of 245 (15) customers who transfer funds or shares to accounts in a country other than those that are assessed by the FSP as having a low degree of risk of ML/TF; or (16) any transaction involving an undisclosed party. Page 156 of 245 GUIDANCE NOTES ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING IN THE CAYMAN ISLANDS PART V SECTOR SPECIFIC GUIDANCE: INSURANCE SECTOR The purpose of this part of the Guidance Notes is to provide some guidance specifically for the Insurance sector. This Insurance sector specific guidance (Part V) covers Insurance Business and, in Part V Section 2, additional details for Insurance Managers and should be read in conjunction with Part I and Part II of the Guidance Notes. Page 157 of 245 SECTION 1 INSURANCE BUSINESS A. OVERVIEW 1. The insurance market of the Cayman Islands is composed of two broad segments: the foreign market, which comprises of captive insurance companies that insure non-domestic risks (Class B licence) and of fully collateralised insurance linked securities (ILS) structures (Class C license), and the domestic market (Class A licence), where insurers, directly or through intermediaries, sell insurance to Cayman Islands residents and business organisations. In addition, reinsurers (Class D license) offer reinsurance products for domestic or foreign risks. 2. While domestic insurers generally have staff or agents in the Cayman Islands, this is not always the case for captive insurance companies, which can be self- managed or managed by an insurance manager. The Insurance Act, 2010, requires Class B and C insurers to either have a physical presence or appoint an insurance manager. Insurance managers are licensed and supervised by the Monetary Authority both for prudential and AML/CFT purposes, and the insurance managers manage the day to day activities of the insurer and provide it with insurance expertise. The insurance companies within the domestic market offer their products directly as well as through intermediaries, namely insurance brokers and insurance agents. 3. The Class B licence is sub-divided into three categories. Class B(i) which includes insurers with at least 95% of the written net premiums originating from the insurer s related business. Class B(ii) is for insurers with over 50% of the net premiums written originating from the insurer s related business, and Class B(iii) includes insurers with 50% or less of the written net premiums originating from the insurer s related business. B. SCOPE 1. The AMLRs are mainly applicable to insurance

business as specified in its Schedule, which includes life and annuity business, and all of which are described as long-term insurance. Whilst the AMLRs do not apply directly to general insurers, from a sound risk management and internal controls perspective, such insurers are still expected to have policies and procedures in place to prevent ML/TF, in accordance with these Guidance Notes. 2. Section 4 of the AMLRs states that the AMLCO shall ensure that measures set out in the AMLRs are adopted by companies carrying out relevant financial business. For insurance business, this means companies involved in long-term business as defined within the Insurance Act (2010) (i.e. insurers, insurance managers, insurance agents, and insurance brokers). The AMLRs will therefore apply directly to insurance managers, insurance agents or insurance brokers in relation to long- term business. However, managers, agents and brokers are still expected to have policies and procedures in place to prevent ML/TF in respect of any general insurance business they are involved in. 3. This sector specific guidance seeks to provide practical assistance to all insurers and insurance intermediaries in complying with the AMLRs, interpreting and Page 158 of 245 applying the general provisions of these Guidance Notes and to adopt sound risk management and internal controls for their operations. 4. The principal obligation to perform AML/CFT procedures under the AMLRs falls on each FSP in respect of the parties with which it directly transacts, that is to say its own applicants/customers. For example, in the case of an insurance manager, its applicants will largely be insurance companies, which themselves, as licensees also, will have their own independent obligations to perform AML/CFT checks as appropriate on policyholders and beneficiaries, or others with whom they conduct relevant financial business. 5. As a practical matter, however, many insurers, particularly those without their own dedicated staff, may often delegate the operation of AML/CFT procedures to insurance managers. However, each FSP retains ultimate responsibility for ensuring that appropriate steps are taken in respect of its own applicants/customers. Where an insurer is un-staffed, Section 9 of Part II of the Guidance Notes as relates to the MLRO/AMLCO will still be applicable. In the absence of the MLRO, the Deputy MLRO shall discharge the MLRO functions. C. ML/TF RISKS: 1. As an international financial centre, the Cayman Islands face greater external, rather than internal, ML/TF threats. Theft, corruption and drug trafficking are the main threats emanating from domestic origins. Fraud, the evasion by foreigners of taxes overseas, and drug trafficking in other jurisdictions, present potential threats to the Cayman Islands from foreign origins. 2. The ability to use the insurance sector for ML/TF is generally regarded as lower than that of other sectors such as banking, and securities, which present better opportunities for criminals to quickly deposit and withdraw funds. 3. Regardless, there is some ML/TF risk within the international insurance sector. As with many other financial vehicles, captive insurance companies may be misused for ML/TF purposes. As such, FSPs (such as ILs structures) must be vigilant to prevent criminals from using them for ML/TF purposes. Some of the risks can be mitigated by ensuring the source of funds and identity of investors is understood and appropriate due diligence is performed accordingly. 4. Generally, international insurers operating as commercial insurance companies, especially those engaged in long-term insurance business or annuity products, as well as domestic insurers engaged in long-term insurance business and annuity products, may present a higher ML/TF risk compared to other insurers. Insurance fraud, including staged motor vehicle accidents, has been known to be used as a means of raising funds for terrorist organizations. 5. Even international insurers covering their own risk/related risks, (i.e. pure captives) still have ML/TF risks and captive owners

and insurance managers need to be aware and mitigate such risks. Insurance managers managing captives need to ensure they understand the rationale for the set-up of the captive and monitor any potential ML/TF risks, especially as it relates to money flows, including inter-company loans. Page 159 of 245 D. RISK BASED APPROACH 1. Companies conducting insurance business must apply a risk-based approach to mitigate the risk that their company will be used for ML/TF. The risk-based approach requires an FSP to take steps to identify the risks relating to: (1) its type of customers, such as retail or corporate, and new or existing customer; (2) the country or geographic area in which its customers reside or originate, for example, is it a country that has robust ML/TF regulations or not; (3) the products, services and transactions of the company: for example, does the product have a cash-in value and can it easily be used for ML/TF purposes; (4) the delivery channels used by the company: for example, does the company distribute its own products or does it use other intermediaries and are these intermediaries licensed by a reputable regulator or not. 2. Section 3 of Part 2 of these Guidance Notes explains how FSPs should operationalise the risk-based approach. Section E below provides specific guidance for insurers and intermediaries about risk factors applicable to the business of insurance. E. NATURE OF PRODUCTS UNDERWRITTEN/SOLD 1. The risk-based approach should lead the FSP to consider the inherent risk within the nature of the product being underwritten/sold, the amounts involved, the ability to surrender the product for a cash value, the ability to add riders to the policy, amongst other things. A few examples of these risks are provided in this section. GENERAL (NON-LIFE) (1) In relation to insurance business, significant factors that will affect the level of risk of any transaction or business relationship include: (a) the mode/method of payment of the premium (e.g. cash, credit card, bank transfer etc.); (b) the nature product to be underwritten or sold e.g. does it have a cash-in value or surrender value, and can loans be taken against the policy; (c) the amount of premium (e.g. higher premium policies could be more attractive to ML/TF). (2) A significant factor determining the level of ML/TF risk in any product is the level of premium payable on the policy and method of payment. For example, a motor policy with an annual premium of $1000 will present a much lower risk than one on a luxury car or car fleet in the case of a commercial motor policy, which commands a much higher premium and value at risk. (3) Premium payments made in cash present a higher risk than payments made via a bank account. For example, premiums for property and casualty policies in the case of condominium developments may be significant and insurers should be especially vigilant when requests are made for large premiums to be paid in cash. Electronic/card or cheque Page 160 of 245 payments may present a lower risk than cash, especially where large premium payments are involved, but both domestic and international insurers must be aware of the inherent risks that might emanate from electronic/card payments, such as fraud, and put appropriate controls in place. (4) In addition to vigilance about the means of payment, sound claims management is essential as ML/TF can occur through inflated or bogus claims, e.g. by arson or other means causing a fraudulent claim to be made. Features of High Risk and Low Risk General Insurance Products with examples: (5) Some of the features of high risk and low risk general insurance products are listed below: Low risk Low premiums, inability to make claims without substantial reliable evidence of loss. Note that products rated as low AML/CFT risk may also be rated a low fraud risk, but not always. Example of low risk A single, individual travel policy may be considered low risk simply because the premium

is low, and the term date is short. Other travel policies, however, for example, annual or group, may be considered to pose a relatively increased risk and thus controls should be applied appropriately. High risk High premium amounts and the ability to pay in cash, to overpay premiums, and to cancel the policy to seek a premium refund. Also, the greater risk of fraud will generally mean a greater risk of AML/CFT. Example of high risk May include Cash-In-Transit policies or Fidelity Guarantees where the likelihood of manipulation and conspiracy is greater. LONG TERM (LIFE) Features of high risk and low risk long term (life) insurance products with examples: (6) Significant factors that will affect the level of risk of any transaction or business relationship for long-term policies include: (a) The nature of the product to be underwritten or sold, e.g. does it have a cash-in value or surrender value, and can loans be taken against the policy. (b) The mode/method of payment of the premium, e.g. cash, credit card bank transfer etc. (c) The manner of transaction, e.g. face-to-face, online etc. FSPs must apply a risk-based approach and consider any additional risks that might apply to digital transactions. (d) The amount of premium e.g. higher premium policies could be more attractive to ML/TF. Page 161 of 245 (7) Some of the features of low risk and high-risk life and long-term insurance products are listed below: Low 1. Life insurance policies where the total premium payable annually is no more than CI$800, or a single premium of no more than CI$2000. 2. Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral 3. A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member s interest under the scheme. High 1. Unit-linked or with profit single premium contracts 2. Single premium life insurance policies that store cash value 3. Fixed and variable annuities 4. (Second hand) endowment policies 85 . F. SYSTEMS, POLICIES AND PROCEDURES 1. Companies conducting insurance business must establish and fully implement robust systems, policies and procedures to forestall their products and services from being used for ML/TF. 2. This will include, amongst other things, conducting risk assessments, identifying who is a customer/applicant; CDD; simplified/enhanced due diligence; internal controls, ongoing monitoring, record keeping and reporting. G. APPLICANTS - ESTABLISHING A BUSINESS RELATIONSHIP 1. Before an insurance contract is concluded between an applicant/customer and insurer there is already a pre-contractual business relationship between the customer and the person selling the policy, be that the insurer or an intermediary. 2. After a policy is taken out: (1) the insurer covers a certain risk described in the contract and policy conditions; (2) certain transactions may take place such as premium payments, payments of advance or final benefits; and (3) certain events may occur such as a change in cover or a change of beneficiaries. 85 Secondhand endowment policies are also known as traded endowment policies (TEPs). Endowment policies are investment funds made up of savings, bonds, and shares. An individual wanting to cash in an endowment policy has two choices: to surrender it back to the life insurance company, generally for a poor return, or to sell it on the second- hand market, often at a much better price. Page 162 of 245 3. The insurer will need to carefully assess the specific background, and other conditions and needs of the customer. This assessment is already being carried out for commercial purposes (determining the risk exposure of the insurer and setting an adequate premium) as well as for reasons of active client management. This will lead to a customer profile, which could serve as a reference to establish the purpose of the contract and to monitor subsequent transactions and events. 4. The insurer should realise

that creating a customer profile is also of importance for AML/CFT purposes and therefore for the protection of the integrity of the insurer and its business. Generally, it will be appropriate to obtain information as outlined below, but other circumstances may require alternative information. H. INSURANCE SPECIFIC INFORMATION THAT MAY BE REQUESTED TO SUPPLEMENT AS NECESSARY THAT OUTLINED IN PART II OF THESE GUIDANCE NOTES 1. The following are some of the insurance specific information that may be requested to supplement the other information required under the section CDD of Part II of the Guidance Notes. Applicant for business (proposer) Insurance specific information Personal 1. That the person is the proposer and has an insurable interest in the risk to be insured 2. The property or other risk to be insured and its valuation. 3. Any other beneficiaries with insurable interests and/or claims on the policy. 4. The source of funds for the payment of the premium. Corporate 1. That the person proposing represents and is authorised to represent the company, which has an insurable interest in the risk to be insured. 2. The property or other risk to be insured, and its valuation. 3. Any other beneficiaries with insurable interests and/or claims on the policy. 4. Source of funds for the payment of the premium. When must identity be verified? 2. In principle, identification and verification of customers and beneficial owners should normally take place when the business relationship is established. This means that the policyholder (or its owner / controller) needs to be identified and Page 163 of 245 their identity verified before, or at the very latest at the moment when, the insurance contact is concluded. 3. That said, identification and verification of the beneficiary may take place after the insurance contract has been concluded with the policyholder, provided the ML/TF risks are not significantly high and are effectively managed. One example could be an insurer providing a customer with immediate temporary motor insurance. However, that might be subject to the customer providing evidence of proof of his/her address within an agreed timeline. Another example is where an insurance contract permits an applicant to delay naming a beneficiary, or permits changes to beneficiaries during the life of the insurance policy, the identity of the beneficiary may be obtained as soon as the beneficiary is identified or designated and no later than at the time of the pay-out. 4. However, subject to (6) below, where the verification information is not forthcoming at the outset or within a reasonable time after initial contact the proposed business relationship must be re-evaluated and transactions must not proceed. 5. Where the ML/TF risks are assessed as standard or lower than standard, and appropriate risk-mitigation measures are applied, verification of a beneficiary s identity may take place: (1) At or before the time of any pay-out or premium refund; (2) At or before the time the beneficiary exercises any vested right under the policy. Simplified/Enhanced due diligence 6. An FSP may apply SDD measures where lower risks have been identified, through an adequate analysis of risks by the country or the FSP itself. The simplified measures CDD shall be commensurate with the lower risk factors but are not acceptable whenever there is suspicion of ML or TF, or higher risk scenarios apply. CDD is required on all life policies. FSPs must take due care and ensure that CDD is also carried out on life insurance beneficiaries. As outlined in the Systems, Policies and Procedures section above, CDD and EDD must be ongoing and not just at the time a policy is placed on risk. 7. It is recommended that EDD be applied for high risk situations and in situations where the insurer is particularly exposed to reputational risk. There will be certain occasions where EDD will be required, for example: (1) when there is an identified high-risk factor accompanied by no face-to- face contact with the insured; (2) where the customer is a PEP; (3) where the

beneficiary of a policy can be transferred; and (4) when the customer is involved in a business that is considered to present a high risk for ML/TF. 8. With respect to EDD, in addition to those listed in Part II of the Guidance Notes, the following additional information might be requested in relation to the proposed transaction, business or source of funds: Page 164 of 245 (1) In insurance, various transactions or trigger events occur after the contract date and indicate where due diligence may be required. These trigger events include claims notification, surrender requests and policy alterations, including changes in beneficiaries. (2) The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors. (3) In this respect transactions should be interpreted in a broad sense, meaning inquiries and applications for an insurance policy, requests for changes in cover, redemption, cancellation, claim submission premium payments, requests for changes in benefits, beneficiaries, duration, etc. How should the business of the customer be monitored? 9. The FSP must pay attention to all requested changes to the policy and/or exercise of rights under the terms of the contract. 10. The FSP must also assess if the change/transaction does not fit the profile of the customer and/or beneficial owner or is for some other reason unusual or suspicious. I. ML/TF WARNING SIGNS What warning signs or red flags should FSPs (i.e., insurance entities covered under this section) be alert to? 1. The following are some of the warning signs or red flags to which FSPs should be alert. The list is not exhaustive, but includes the following: (1) Requests for a return of premium to be remitted to persons other than the policy holder. (2) Claims payments paid to persons other than policyholders and beneficiaries. (3) Unusually complex holding company or trust ownership structure. (4) Making a false claim. (5) A change in beneficiaries (for instance, to include non-family members). (6) A change/increase of the premium payment (for instance, which appear unusual in the light of the policyholder s income or where there are several overpayments of policy premiums after which the policyholder requests that reimbursement is paid to a third party). (7) Use of cash and/or payment of large single premiums. (8) Payment/surrender by a wire transfer from/to foreign parties. (9) Payment by banking instruments that allow anonymity of the transaction. (10) Change of address and/or place of residence of the policyholder. (11) Lump sum top-ups to an existing life insurance contract. (12) Lump sum contributions to personal pension contracts. (13) Requests for prepayment of benefits. (14) Use of the policy as collateral/security (for instance, unusual use of the policy as collateral unless it is clear that it is required for financing of a mortgage by a reputable financial institution). (15) Change of the type of benefit (for instance, change of type of payment from an annuity to a lump sum payment). Page 165 of 245 (16) Early surrender of the policy or change of the duration (particularly where this results in penalties). (17) Requests for multiple policies to be taken out for premiums slightly below any publicised limits for performing checks, such as checks on the source of wealth or cash payments. 2. As the above list is not exhaustive, insurers should consider other types of transactions or trigger events, which are appropriate to their type of business. J. RECORD KEEPING 1. FSPs must ensure that their record-keeping procedures are maintained in accordance with Part VIII of the AMLRs. 2. All records, including discharge documents must be readily accessible and available without delay upon request by competent authorities. Page 166 of 245 SECTION 2 INSURANCE MANAGERS A. NATURE OF THE PRODUCTS UNDERWRITTEN/SOLD 1. ML/TF can occur either by establishing fictitious (re)insurance companies or reinsurance intermediaries, and fronting arrangements, or by the misuse of normal reinsurance

transactions. 2. Examples include: (1) the deliberate placement via the insurer of the proceeds of crime or terrorist funds with reinsurers in order to disguise the source of funds; (2) the establishment of bogus reinsurers, which may be used to launder the proceeds of crime or to facilitate terrorist funding; and (3) the establishment of bogus insurers, which may be used to place the proceeds of crime or terrorist funds with legitimate reinsurers. 3. For Class B insurers the line of business or risk assumed is much less relevant to the assessment of AML/CFT risk, than the persons or applicants involved. This is because even the typically lowest risk product could potentially be used for ML. For example, workers compensation schemes may be established for fictitious personnel or be funding mechanisms for terrorists awaiting assignment. 4. One factor that should help to mitigate this risk is the involvement of independent third parties e.g. medical practitioners, claims adjusters and government agencies to substantiate claims. In the international market the scope for lines of business in insurers is unlimited. 5. The focus for FSPs entering into relationships with Class B insurers should be the operators and owners of the insurer, the business rationale for the insurer, its relationships and source of funding. B. APPLICANTS 1. The applicant for business may be either an existing insurer, possibly already under management and regulated, or it may be a company or group of individuals seeking to establish a new insurer. 2. The following guidance regarding due diligence and documentation to be obtained falls outside and is separate from that which the manager may necessarily obtain in preparing a licence application for an insurer or insurer to be formed as per the Insurance Act and Regulations thereunder. C. EXISTING INSURER TO BE MANAGED 1. It is recognised that where insurers already formed and licensed are transferred to an Insurance Manager, although the insurer, as an applicant, may be regarded as an acceptable applicant for the purpose of verification requirements as per Section 22 of the AMLR, the nature of the relationship between the manager and the insurer may require that additional commercial due diligence is obtained and maintained in order to discharge its obligations as manager and for on-going monitoring. See, Sections 27 29 of the AMLR. Page 167 of 245 How should the business of the customer be monitored? 2. All changes to the nature of the business of the Class B insurer should be assessed and a decision made whether such constitutes a trigger requiring further verification or investigation/information. 3. At a minimum the Annual Statement of Operations filed with the Monetary Authority provides a periodic opportunity to review the relationship and the business of the customer, or upon renewal of the service agreement. D. ML/TF WARNING SIGNS What warning signs or red flags should Insurance Managers be alert to? 1. The following are some of the warning signs or red flags to which service providers should be alert. The list is not exhaustive, but includes the following: (1) Requests for a premium refund to be remitted to persons other than the policy holder. (2) Dividends paid to persons other than shareholders. (3) Unusually complex holding company or trust ownership structure. (4) Concealment of identity of the customer or the beneficial owner; or of the ownership of funds. (5) Incomplete application details and lack of willingness to provide evidence to answers required. (6) Unexplained changes in investment pattern; investment taken against advice or not appropriate to insurer's real needs; (7) Sudden changes in intermediary transaction pattern; (8) Unexplained receipt of bulk premiums from intermediary accounts. (9) Third party transactions (payments or withdrawals); (10) Multiple sources of payment or cross jurisdiction funding for payment; (11) Payment of premiums from early surrender of another investment in unusual circumstances; (12) Payment from obscure or unregulated organisations; (13) Unnecessarily complex transactions or intentions; (14)

Requests for part investment and return of surplus funds; (15) Immediate interest in surrender penalties or requests for large withdrawals or policy loans; (16) Early surrender of a contract; (17) Receipt of unexplained wire transfers and requests to return wire transfers; (18) Requests for no correspondence to go to customer. E. RECORD KEEPING What specific AML/CFT records should be kept and where? 1. See Sections 31 and 32 of the AMLRs and, in addition, all documentation listed above together with initial and subsequent information necessary for on-going monitoring should be held, whether as duplicate or back up by the Manager at its office in Cayman. Page 168 of 245 F. OTHER RELEVANT SECTORS 1. Catastrophe bonds and other ILS may be a source for ML/TF due to the large amount of money that is invested into them. FSPs need to apply a risk-based approach to ensure they understand who the customer/investors are; the source of funds; the jurisdictions of the customer/investors; the beneficial owners of the policy, where a trust structure might be in place; and means of payments such as cash and bank transfers. Page 169 of 245 GUIDANCE NOTES ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERAITON FINANCING IN THE CAYMAN ISLANDS PART VI SECTOR SPECIFIC GUIDANCE: MUTUAL FUNDS AND MUTUAL FUNDS ADMINISTRATORS The purpose of Part VI of the Guidance Notes is to deal with AML / CFT matters pertaining to Mutual Funds (MFs) and Mutual Fund Administrators (MFAs) that require more explanation or are more complex issues than are dealt with in the general body of these Guidance Notes. This section must be read in conjunction with Part I and Part II of the Guidance Notes and the Appendices. MFs and MFAs may also find Part VIII of these Guidance Notes to be of some relevance. Page 170 of 245 SECTION 1 MUTUAL FUNDS AND MUTUAL FUND ADMINISTRATORS A. OVERVIEW 1. The Mutual Funds Act (2021 Revision) (the MFL) gives the Monetary Authority responsibility for regulating certain categories of Mutual Funds (defined below) operating in and from the Cayman Islands, as well as Mutual Fund Administrators (defined below). 2. The Monetary Authority regulates Mutual Funds and Mutual Fund Administrators in accordance with: (1) the Acts and regulations applicable to all regulated entities and those specifically governing this sector, namely, the MFL; the Mutual Funds (Annual Returns) Regulations; the Retail Mutual Funds (Japan) Regulations; and the Mutual Fund Administrators Licence (Applications) Regulations; (2) the relevant rules, guidance, policies and procedures issued by the Monetary Authority from time to time; and (3) relevant international standards set by international bodies such as, but not limited to, the International Organization of Securities Commissions (IOSCO) and the Offshore Group of Collective Investment Scheme Supervisors (OGCISS). 3. The definition of a Mutual fund, as established in the MFL, can be summarised as follows: any company, trust or partnership either incorporated or established in the Cayman Islands, or if outside the Cayman Islands, managed from the Cayman Islands, which issues equity interests redeemable or purchasable at the option of the investor, the purpose of which is the pooling of investors' funds with the aim of spreading investment risk and enabling investors to receive profits or gains from investments. 4. Note that funds commonly referred to as hedge funds fall within the definition of a Mutual Fund and are thus covered by the MFL. 5. The Cayman Islands has company, trust, partnership and related Acts that allow a high degree of flexibility for establishing Mutual Funds. The four vehicles commonly used for operating Mutual Funds are the exempted company, the segregated portfolio company, the unit trust and the exempted limited partnership. 6. A Mutual Fund Administrator is a person who conducts

mutual fund administration as defined in the MFL; that is: a person managing (including controlling all or substantially all of its assets) or administering a Mutual Fund; a person providing the principal office of a Mutual Fund in the Cayman Islands; or providing an operator to the Mutual Fund as defined in Section 2 of the MFL (a trustee of a unit trust, a general partner of a partnership or a director of a company). Page 171 of 245 B. SCOPE 1. The sector specific guidance contained in this section is applicable to regulated Mutual Funds and Mutual Fund Administrators, separated accordingly where applicable. C. MONEY LAUNDERING AND TERRORIST FINANCING RISKS 1. As is the case with most financial products, Mutual Funds carry a certain degree of ML/TF risks. 2. Listed below are some, but not all, of these relevant risks. (1) Country Risk having investors located in multiple international locations can increase the risk of money laundering and terrorist financing. Mutual Funds and Mutual Fund Administrators should be especially careful when dealing with investors who are PEPs of a foreign jurisdiction or those from a country on a sanctions list. (2) Investor Profile in addition to the country of domicile of investors, the types of individuals/entities that make up the investor base can also increase the risk of money laundering and terrorist financing. All things equal, institutional investors from large financial institutions that are regulated and/or listed on a stock exchange could be considered less risky than investors in the form of trusts, charities or high net worth individuals for example. (3) Source of Funds Mutual Funds with lower minimum investment thresholds pose a greater risk of money laundering, especially if those funds are not coming from a regulated financial institution. Mutual Fund Administrators and Operators must remain cognisant of, and have controls in place surrounding, subscription and redemption activity in Mutual Funds, in the same way bankers must do so for bank account deposits and withdrawals. (4) Redemption Terms persons attempting to partake in money laundering need the ability to move funds out of the Mutual Fund in order to effectively layer transactions. Some Mutual Funds have liquidity structures with limited or no lock-up periods and/or redemption restrictions. D. RISK-BASED APPROACH (refer also to Section 3 of Part II) 1. Low and high-risk indicators including the ML/TF risks outlined in Section C above and the ML/TF warning signs outlined in Section I below should be considered when the Mutual Fund and/or Mutual Fund Administrator is conducting risk assessments. 2. FSPs should be aware of, and take into account, additional risk factors or risk variables that may be introduced where services, functions or activities of the FSP itself or the FSPs customers are outsourced or delegated, particularly so if the service provider is not subject to adequate AML/CFT laws and measures and / or is not adequately supervised. 3. One risk factor set out in Part II Section 3 that is of particular relevance (to mutual funds and (perhaps to a lesser degree) fund administrators is the non-face-to- face basis for subscriptions, redemptions and transfers. While the presence of a Page 172 of 245 high-risk factor does not necessarily make the customer high risk, FSPs should consider this factor along with all the other relevant risk factors and mitigants and undertake appropriate CDD measures. A possible mitigating measure, which in turn requires robust systems and controls, is the use of reputable and regulated EI. 4. Other risk factors or risk variables to consider may include: (1) A history of frequent and / or unexplained changes in service providers; and (2) A customer, or principals of a customer, that is or has been the subject of criminal / civil or regulatory proceedings for crime, corruption, misuse of public funds or known to associate with such persons. 5. Risk assessments should take place as a customer or investor is on-boarded and be reviewed and changed if necessary, during

periodic reviews of the customers and investors as discussed in the Ongoing Monitoring section. The methodology used by the entity to assess the risk should be based on the ML/TF risks posed, including the factors discussed above. Customers and investors that are risk classified as low (or the equivalent) may be subject to SDD procedures. However, entities must be aware that their risk classification of a Customer/Investor being low risk is only valid if the finding is consistent with the findings of the NRA or the Supervisory Authority, whichever is most recently issued. Customers and investors that are risk classified as medium risk (or the equivalent) may be subject to normal CDD procedures. Customers and investors risk classified as high risk must be subject to EDD procedures. 6. On-going monitoring should take place to ensure that documents, data, information collected during the various due diligence procedures on the customers or investors are kept up-to-date and relevant. FSPs should ensure that the customers or investors are periodically screened against the vigilance databases/sanction lists and periodic reviews should also be conducted on the customers or investors based on their risk rating. E. APPLICANT FOR BUSINESS (refer also to Part II) Who should be treated as the Applicant for Business? 7. The applicant for business may be any one of the following: E.g. FSP Applicant for Business 1. The Mutual Fund. (1) Investors should be treated as such for the purposes of the Guidance Notes. 2. FSP incorporating a company/setting up a limited partnership/unit trust as part of a Mutual Fund structure (including acting as investor, shareholder and/or providing initial registered office). (1) Promoters (as defined in the MFL). (2) Where the mutual fund is a unit trust, the trustees; or (3) Where the mutual fund is a limited partnership, the general partner; or (4) Where the mutual fund is a corporation, the directors (see the Page 173 of 245 section on Company Formation and Management). 3. FSP providing registered office for Mutual Fund/general or limited partner (other than at the date of incorporation). FSP providing a principal office for a Mutual Fund Administrator. (1) The Mutual Fund. (2) The Mutual Fund Administrator 4. Mutual Fund Administrator. (1) The Mutual Fund (and the relevant Operators thereof). (2) When the Mutual Fund for which documentary evidence should be obtained is a unit trust or a limited partnership, it will usually be sufficient to obtain evidence of the identity of the Trustee or the controlling General Partner. (3) Given the special circumstances of mutual funds, it is recommended as good practice that a Mutual Fund Administrator should not rely on the Mutual Fund falling into the specified scenarios in which SDD would apply by virtue of it being subject to the Regulations. However, the Administrator may be satisfied that the Mutual Fund, if not itself carrying out customer identification or record keeping, has in place appropriate safeguards to ensure that its obligations under the Regulations are met. (4) Promoters: Whilst promoters are not to be treated as applicants for business for the purposes of these Guidance Notes, it is industry best practice to ascertain the identity and background of any promoter relied upon. FSP otherwise issuing and administering subscriptions/redemptions. (1) The Mutual Fund. Page 174 of 245 F. CUSTOMER DUE DILIGENCE (refer also to Section 4 of Part II) When must the identity be verified? 1. The Regulations provide that there should be procedures in place requiring, as soon as reasonably practicable after contact is first made with an applicant for business, either satisfactory evidence of the applicant s identity or that steps are taken which will produce satisfactory evidence of identity. 2. The time span in which satisfactory evidence has to be obtained depends on the particular circumstances and the practicalities of obtaining evidence before commitments are entered into between

parties and before money passes. How might identification of existing customers be carried out? 3. Refer to Section 4 (Customer Due Diligence) of Part II of the Guidance Notes. 4. If, after having conducted a risk assessment, verification procedures or identification of an investor have not been completed prior to the date on which redemption is due to take place, the Mutual Fund should use the opportunity of redemption to seek satisfactory evidence of identity. Payment of the redemption proceeds should be made only to the investor and not to a third party and only when the outstanding due diligence documentation has been collected and verified. If payment is to be made to or from an account in the name of the investor with a regulated bank in the Cayman Islands or in a country assessed by the FSP as having a low degree of risk of ML/TF, and the requirements set out in Section 5 of Part II of the Guidance Notes are adhered to, that will be sufficient evidence of identity. Particular Issues on Verification of Identity of Investors One-off transactions 5. For the purpose of the Guidance Notes a subscription to a Mutual Fund should not be treated as a one-off transaction (for which see Section 4 of Part II of the Guidance Notes). If the investor is a fund domiciled outside of a country assessed by the FSP as having a low degree of risk of ML/TF but is administered in a country assessed by the FSP as having a low degree of risk of ML/TF 6. In such a case, the investor may fall within one of the specified scenarios in which SDD would apply. 7. Evidence may also be satisfactory if the investor's administrator: (1) is subject to anti-money laundering oversight in its home country; and (2) confirms in writing that it has obtained and maintains customer verification evidence in accordance with the procedures of the country assessed by the FSP as having a low degree of risk of ML/TF. Payment on an Account in a Bank in the Cayman Islands or a country assessed by the FSP as having a low degree risk of ML/TF Page 175 of 245 8. See Section 5 D of Part II of these Guidance Notes. Corporate Group Introduction 9. It will not be necessary for identity to be re-verified or records duplicated if the identity of an investor has been verified by another entity within a group in a manner compatible with the Regulations and provided that written confirmation is obtained that the identification records will upon request be provided. 10. This is so even in circumstances when neither the investor nor the Bank from which he sends funds or investment is located in a country assessed by the FSP as having a low degree of risk of ML/TF. G. INTERNAL CONTROLS AND ONGOING MONITORING (refer also to Part II) 1. Regulated Mutual Funds and Mutual Fund Administrators must have policies and procedures in place as required by the AMLRs. These shall include policies and procedures to- (1) identify and report suspicious activity; (2) monitor and ensure compliance with AML/CFT legislative and regulatory requirements; and (3) test the efficacy and efficiency of their AML/CFT systems and update such systems, if necessary, to comply with their AML/CFT obligations (the "Procedures"). 2. Both Mutual Funds and their Mutual Fund Administrators subject to the AMLRs have separate obligations to maintain and implement such Procedures in respect of their relevant financial business. 3. The ultimate responsibility for maintaining and implementing adequate Procedures and complying with the applicable AML/CFT obligations remains with the Mutual Funds and Mutual Fund Administrators. 4. Mutual Funds and Mutual Fund Administrators may meet their obligations in relation to their Procedures by either- (1) implementing their Procedures directly; (2) delegating the performance of the Procedures to a person; or (3) relying on a person to perform the Procedures. 5. Where an FSP that is a Mutual Fund or Mutual Fund Administrator chooses to delegate the performance of the Procedures to a person, the FSP should adopt the principles set out in Part II, Section 10. C. (Outsourcing). 6.

Similarly, where an FSP that is a Mutual Fund or Mutual Fund Administrator chooses to rely on a person for the performance of the Procedures, the FSP should adopt the principles set out in paragraphs 1 through 5 of Part II, Section 2. C. 7. The operators of the Mutual Funds or Mutual Fund Administrators should document, either as a board resolution or other appropriate documentation (such as a supplement/update to existing policies and procedures or detailed appendix to an existing agreement, in the case of a delegation or reliance arrangement), the manner in which the FSP has met its obligation to maintain and implement Procedures. Page 176 of 245 Mutual Funds 8. All Mutual Funds must designate a natural person as their MLRO/DMLRO. After such designation, Mutual Funds may choose to delegate the performance of this function to their mutual fund administrator or any other service provider or rely on their mutual fund administrator or any other service provider to perform this function. Where a Mutual Fund chooses to delegate the performance of the function to a person, the Mutual Fund should adopt the principles set out in Part II, Section 10. C. (Outsourcing). Similarly, where a Mutual Fund chooses to rely on a person for the performance of the function, the Mutual Fund should adopt the principles set out in paragraphs 1 through 5 of Part II, Section 2. C. Mutual Fund Administrators 9. A Mutual Fund Administrator must designate a natural person as their MLRO/DMLRO. After such designation, the Mutual Fund Administrator may choose to delegate (or sub-delegate where the Mutual Fund Administrator is a delegate) the performance of the MLRO/DMLRO function to a person, or rely on a person to perform the function. Further, a Mutual Fund Administrator may also choose to delegate/sub-delegate the performance of the Procedures to a person(s) or rely on a person(s) to perform the Procedures. Where a Mutual Fund Administrator chooses to delegate/sub-delegate the performance of the Procedures or any function to a person, the Mutual Fund Administrator should adopt the principles set out in Part II, Section 10. C. (Outsourcing). Similarly, where a Mutual Fund Administrator chooses to rely on a person for the performance of the Procedures or any function, the Mutual Fund Administrator should adopt the principles set out paragraphs in 1 through 5 of Part II, Section 2. C. H. RECORD KEEPING (refer also to Section 8 and 11 of Part II) What specific records should be kept and where? 1. Refer to Sections 54 and 55 of the Companies Act (2023 Revision) 2. It may be impractical for a regulated Fund itself to maintain records but it must ensure that all appropriate records are maintained on its behalf. 3. Mutual Fund Administrators must ensure that they have customer verification evidence appropriate to the administration of Mutual Funds and, if the function is delegated to them, must maintain records on behalf of the Mutual Fund for the requisite period. When procedures required by the Regulations may be maintained by a party not based in the Cayman Islands. 4. Maintenance by a person or institution regulated in in a country assessed by the FSP as having a low degree of risk of ML/TF of all records and compliance with the procedures of that country will be regarded as compliance with the Regulations and the Guidance Notes, subject to compliance with the provisions of Section 5 of Part II of the Guidance Notes. Page 177 of 245 When may a successor Mutual Fund Administrator rely on the customer verification evidence obtained by its predecessor? 5. Where a successor firm is acquiring administration of an existing Mutual Fund, the successor must ensure that the necessary due diligence has been performed prior to performing the administration. 6. It may be possible to rely upon the evidence of identity obtained by a predecessor Mutual Fund Administrator provided that the original files, or certified copies of the original files, are transferred to the successor Mutual Fund Administrator and the successor firm has assessed

the quality of the evidence on investor identity. 7. Where insufficient evidence exists, it may be appropriate to supplement with additional evidence to meet the standards required by these Guidance Notes. 8. At no time would it be appropriate to rely upon an EI letter as a method for the customer verification evidence obtained by its predecessor. I. MONEY LAUNDERING/TERRORIST FINANCING WARNING SIGNS 1. In addition to the risk factors in Section 3 of Part II and the warning signs set out in Appendix D of the Guidance Notes, risk factors and ML/TF warning signs to which Mutual Funds and/or Mutual Fund Administrators must have regard to in order to satisfactorily assess the ML/FT risks pertaining to a particular business relationship or transaction include: (1) When an investor is more concerned about the subscription and redemption terms of the Mutual Fund than with other information related to the investment strategy, service providers, performance history of the investment manager, etc. (2) Lack of concern by an investor regarding losses or (large) fees or offering to pay extraordinary fees for early redemption; (3) Sudden and unexplained subscriptions and redemptions; (4) Quick purchase and redemption of units despite penalties; (5) Requests to pay redemptions proceeds to a third (unrelated) party; (6) A fund, or principals of a fund (i.e. a client of a mutual fund administrator) that exhibits unusual concern with compliance with AML/CFT reporting requirements or other (AML/CFT) policies and procedures; and (7) When a promoter/manager attempts to launch a new Mutual Fund with large amounts of seed capital from one source, either from an internal or external source. (The source of funds must be properly verified.) Page 178 of 245 GUIDANCE NOTES ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING IN THE CAYMAN ISLANDS PART VII SECTOR SPECIFIC GUIDANCE: MONEY SERVICES BUSINESS, OTHER REGULATED FINANCIAL INSTITUTIONS AND UNSUPERVISED LENDERS The purpose of this part of the Guidance Notes is to provide some guidance specifically for the Money Services Business Sector, the Cayman Islands Development Bank (CIDB) and Un- supervised Lenders. These guidance (Part VII) cover the MSB sector in Section 1 and the CIDB in Section 2 and un-supervised lending activity in Section 3. This Part VII should be read in conjunction with Part I, Part II and the Appendices of the Guidance Notes. Page 179 of 245 SECTION 1 MONEY SERVICES BUSINESS A. OVERVIEW 1. Section 2 of the Money Services Act (2020 Revision) defines money services business (MSB) as- (1) the business of providing, in or from within the Islands, any of the following services: (a) money transmission; (b) cheque cashing; (c) currency exchange; (d) the issuance, sale or redemption of money orders or traveller s cheques; and (e) such other services as the Cabinet may specify by notice published in the Gazette. 2. Money transmission business can be described as the business of accepting funds for their transmission to persons in another country or domestic location. MSBs cater primarily to the resident domestic market, in particular, the expatriate workers of lower income. 3. The cash-intensive nature of the industry raises potential ML/TF concerns. The money remittance sector has challenges accessing banking services, which is an increasing global trend. The lack of access to traditional banking services may increase the level of vulnerability. 4. Typically, users of money remittance services are individuals, expatriate workers and smaller entities that send cash to other individuals thereby bypassing a traditional bank. The speed with which transactions occur can help individuals dispose of illicit proceeds instantaneously. Cross border fund flows also increase the risk of illicit funds being introduced into the Cayman Islands economy/financial system. With the Cayman Islands being a major cruise

destination, employees of the cruise lines are known to be users of the remittance system, although this would be a miniscule population. B. SCOPE 1. This part of the sector specific guidance seeks to provide practical assistance to MSBs in complying with the AMLRs, interpreting and applying the general provisions of the Part II of these Guidance Notes, and for MSBs to adopt sound risk management and internal controls for their operations. 2. The AMLRs apply to MSBs as indicated in the list of activities falling within the definition of Relevant Financial Business in the Sixth Schedule of the Act. This section should be read in conjunction with Part I and II of these Guidance Notes. 3. It is the responsibility of each MSB to have systems and training in place to prevent ML/TF. Each MSB must maintain adequate AML/CFT systems which include CDD measures, record-keeping procedures, and such other procedures and controls appropriate for the purposes of forestalling and preventing ML/TF. Page 180 of 245 C. ML/TF RISKS 1. The fleeting relationship with their customers makes MSBs vulnerable to ML/TF. A person would typically have to be a customer with an account at a bank, for example, to be able to access the services of that bank, whereas a person does not have that type of relationship with the MSB and can repeatedly use different MSBs to transact business. The money transmission part of the MSB is particularly vulnerable, given the high volume of cash handled on a daily basis and the ability to transmit funds instantly to any part of the globe. 2. While the international remittance system is typically used by expatriate workers to send a part of their earnings back home, it can also be used to transmit the illegal proceeds of criminal activities and thereby poses ML/TF risk. The rapid movement of funds across multiple jurisdictions presents a challenge to investigators, particularly if the identity of the originator is unclear. For this reason, international standards have been developed with respect to payer (and payee) information that should accompany wire transfers to mitigate the above- mentioned risk. 3. Cheque cashing is another important segment of the business for some MSBs. MSBs should be aware that endorsed third party cheques from overseas are a ML/TF risk. Even where a Cayman Islands cheque, endorsed by a third party, is presented to the MSB for cashing, the MSB should take appropriate steps to ascertain the economic purpose behind the endorsement to that person presenting the cheque. Large value cheques originating from unknown individuals present a greater ML/TF risk compared to small cheques originating from well- established businesses. MSBs must have board approved AML/CFT policies and procedures that give staff clear guidance in dealing with these situations. 4. Currency exchange is another important segment of the business for some MSBs. MSBs who offer this type of service must have policies and procedures specific to the risks posed by this activity. D. RISK BASED APPROACH 1. MSBs should adopt a risk-based approach to manage and mitigate ML/TF risks. In so doing, in addition to assessing risks inherent to their business, MSBs must develop risk profiles of their customers, thereby familiarising themselves to customers personal or business needs for the services provided. 2. While conducting risk assessments, MSBs should take into consideration the factors such as: (1) the types of products and services that they offer; (2) their customer types (customer occupation or type of business operated); (3) the geographical location of customers or where funds are transmitted; and (4) the average cash value of typical transactions and the $15,000 customer identification threshold as per the AMLRs. 3. As much as possible, MSBs should use computer technology to conduct the risk assessment. As provided in Part II of these Guidance Notes, customers, products, geography and services should be ranked (for example as high, medium, or low risk). For instance, the transfer of a part of an expatriate

worker s weekly Page 181 of 245 wage to his/her family in his/her home country should be less risky compared to the transmission of a large sum by a visitor to numerous recipients. 4. High risk customers, products, geographical regions and services should be subject to EDD and transaction monitoring. The risk model should be documented, with its rationale clearly stated, and should be updated on a regular basis to keep in line with changes in the business, customer profile or the ML/TF risks. See guidance provided in Section 3 of Part II of these Guidance Notes. E. CUSTOMER DUE DILIGENCE 1. MSBs shall adopt sound CDD policies and procedures. Requiring appropriate due diligence information and documentation, verifying the information, and being alert to unusual or suspicious transactions can help an MSB deter and detect ML/TF schemes. 2. A customer identification and verification policy tailored to the operations of a particular business: (1) helps detect unusual/suspicious activity in a timely manner; (2) promotes compliance with the relevant Acts, regulations, rules and guidance; (3) promotes safe and sound business practices; (4) minimises the risk that the MSB will be used for ML/TF and other criminal activities and as a result reduces the risk of government seizure and forfeiture of funds associated with customer transactions (such as outstanding money orders/traveller s cheques and outstanding money transfers); and (5) protects the reputation of the MSB and reduces or minimises the risk of de-risking. Whose Identity must be verified? 3. The applicant may be an individual, a corporate customer, a partnership or an unincorporated business. 4. The MSB must have documented steps that are utilized to distinguish between someone who is acting on his own behalf and someone who is acting on behalf of another (money mules/straw men). If it is determined that the person is acting on behalf of another, then the procedures for verifying the identity of the ultimate applicant must apply (see Section 4 of Part II of these Guidance Notes). 5. All applicants for business undertaking money transmission via electronic funds transfer, in which case MSBs must comply with the requirements set out for wire transfers as specified in Section 11 of Part II of the Guidance Notes and in the AMLRs. (Regulations in Part X of the AMLRs apply to transfers of funds which means any transaction carried out on behalf of a payer through a payment service provider by electronic means...). 6. Notwithstanding that there may be some transaction that are definitely one-off, the nature of business for many of the MSBs licensed in Cayman, tend to be transactions carried out by customers on a frequent, habitual or regular basis or Page 182 of 245 may be linked. Given this and the ML / TF risks identified above, MSBs should therefore also: (1) verify identity for applicants, for money transmission and other services, where the customer, product or geography risk is deemed to be high risk in the risk assessment conducted; (2) Verify identity for applicants where there is an ongoing relationship akin to a business relationship as defined in the ALMRs; (3) For services other than wire transfer money transmission, establish more diligent thresholds other than the $15,000 stipulated in the AMLRs. The threshold should be derived from the risk assessment, bearing in mind what- (1) the amount that the average customer would transact and (2) the reporting threshold of US$3,500 on the quarterly MSB form reported to the Monetary Authority. 7. Applicants/Customers may fall within the following categories: Applicant for Business Requirements (Highlights and supplementary only please refer to Section 4 of Part II of the Guidance Notes for the full (normal) CDD requirements). Natural Persons (1) Identification documentation should be obtained for the applicant/customer him/herself. (2) Identification documentation should be obtained for beneficial owner of funds. (3) Identification documentation should be obtained for Third Party sending funds. (4) Satisfactory evidence of identity, name and

address, confirmed by using one or more of the verification methods in Section 4 of Part II of these Guidance Notes. Corporate Customer (1) The company (evidence that it exists) e.g. a trade and business licence or a certificate of registration. (2) Consistent with that required for direct personal customers, documentary evidence of identity for all directors; all those with signing powers, including third parties; and beneficial owners. (3) Documentary evidence of identity of the new owner/controller where there is a change in ownership or control, in accordance with that required for direct personal relationships. (4) Satisfactory evidence, confirmed by at least one of the following independent checks, of company s existence: (a) Memorandum and Articles of Association and Certificate of Incorporation (b) Information about the identity of controlling shareholders and directors, e.g., Register of Directors, Register of Members Page 183 of 245 (c) Understanding of all relevant third party and inter-company relationships (d) It may be appropriate to obtain information relating to customers or suppliers and the background of major shareholders and directors Partnership s / Unincorpor ated Businesses (1) The entity, evidence that it exists. (2) Consistent with that required for direct personal customers, documentary evidence of identity required for partners/managers; all those with signing powers, including third parties; and beneficial owners. (3) Documentary evidence of identity of the new owner/partner/controller where there is a change in ownership/partnership or control, in accordance with that required of direct personal relationships. (4) Satisfactory evidence, confirmed by at least one of the following independent checks, of existence of partnership / unincorporated business: (a) Partnership agreement or excerpt if relevant; (b) Certificate of Registration; (c) Information about the identity of controlling partners / shareholders, e.g., excerpt from partnership document; (d) Establish all relevant third party relationships. When must identification documentation be obtained? 8. Customer identification documentation is to be obtained prior to a transaction being carried out. 9. If identification information is not obtained, the transaction should not proceed. What should be done if there are Doubts as to the Identity of an Existing Customer? 10. If in the process of reviewing identification documentation, the MSB has doubts about the veracity or adequacy of previously obtained customer identification data, then the MSB must take reasonable steps to verify the data. 11. Depending on the assessed ML/TF risk of the customer, the MSB could either wait for the customer to transact business again if he is a regular customer, or it can contact the individual by requesting that she/he submit the relevant additional documentation. 12. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of ML/TF in relation to that customer, or where the customer s pattern of transactions changes from what is deemed to be normal for that customer. What Is Considered to Be An Appropriate Description Of Source Of Funds ? 13. The appropriate description of a customer s source of funds include: Page 184 of 245 (1) Salary supported by documentation on employment should be requested; (2) Sale of property including documentation evidencing the sale; and (3) Loan proceeds including documentation evidencing the grant of the loan. 14. The following on their own would not be considered appropriate descriptions of the ultimate source of funds : (1) Partners 86 ; (2) Savings. 15. In the case of Partners, additional enquiries such as confirmation from the banker would be appropriate, while in the case of Savings, a bank statement should be provided. Partners and savings are nonetheless sources of funds for which additional proof of salary, dividends, sale proceeds, or loan (ultimate sources) should be provided. Why Is It Important to Establish The Purpose Of

The Transaction? 16. It is important to establish the purpose for those transactions that are large, complex or unusual (see Section 2 B of this document for further details). 17. The threshold for large transactions should be determined from the MSB s risk assessment. 18. Similar to a Bank, an MSB should ask the customer about the purpose of the transaction that is beyond the MSB s threshold. In that way, the MSB should be able to establish if the purpose is lawful and whether the transaction will be a one-off event or part or a regular occurrence. 19. Information on the purpose of the transaction helps the MSB to develop a profile of normal activity for that customer. If the MSB is unable to establish what normal activity is, then it would be challenging to distinguish the unusual activities for further analysis to determine which ones are suspicious. It is therefore imperative for MSBs to consistently work towards developing customer profiles for all customers using the service. 20. Securing information on the relationship of the recipient of the transfer is useful in assisting with establishing the purpose of the transaction. F. ELECTRONIC FUNDS TRANSFER What Information Should Accompany the Transfer Of Funds? 1. MSBs must ensure that information on the payer and the payee accompanies the transfer of funds. 2. For details on the payer and payee information that need to accompany a transfer of funds, see Section 11 of Part II of the Guidance Notes as that section and the regulations in Part X of the AMLRs apply to transfers of funds which means any 86 Partners is an informal saving and credit scheme in the Caribbean in which a group of people regularly deposit a fixed amount of money with a main organiser, the 'banker', into a central fund. The banker distributes the total sum (the 'hand') to members in a pre-arranged order. This system of credit operates almost completely on trust, in that each person who collects his/her lump sum must be trusted to continue paying in the contributions until all members have collected their 'hand.' This scheme operates usually with no written agreement. Page 185 of 245 transaction carried out on behalf of a payer through a payment service provider by electronic means... . G. SYSTEMS, POLICIES AND PROCEDURES What policies and procedures should be documented? 1. At the very least, MSBs should have documented policies and procedures on: (1) the assessment of risks; (2) risk mitigation and management measures; (3) customer identification and due diligence; (4) when will EDD be applied and what does it entail; (5) transaction monitoring, including complex and unusual transactions; (6) suspicious activity reporting; (7) internal controls; and (8) staff training. How Should the Business of a Customer Be Monitored? 2. Because of the large number of customers involved and the relatively small amounts transacted, it is imperative for MSBs to have adequate systems in place to collate relevant information and monitor customers activities. 3. The amount of information collected may be broadened to include details of the recipient of the funds. This information will assist MSBs to determine whether there is any ML/TF risk when the customer is utilising multiple recipients or whether multiple customers are remitting multiple small sums that are accumulated with one recipient. What to Do About Complex and Unusual Transactions? 4. As mentioned in Section 9 of the part II of these Guidance Notes, where a transaction is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, the transaction must be considered unusual, and the staff member put the transaction on enquiry . 5. An example of an unusual pattern of transactions would be where an MSB s database reveals that several seemingly unrelated individuals are receiving or sending small amounts of money from or to one individual abroad. In such case, the MSB may request additional information on the receivers including the information on the relationship between sender and receiver(s).

Additionally, the FSP may conduct an internet or screening database search to find out more about the senders and/or recipients. 6. MSBs should follow the procedures as explained in part II Section 9 (and more particularly items D, E and F) of these Guidance Notes for the purpose of identifying and dealing with unusual and suspicious transactions. Page 186 of 245 What Specific Records Should Be Kept and Where? 7. The MSB must keep adequate records of the identity of its customers and all transactions conducted by that customer for a period of 5 years following the last transaction, the closing of an account, or the termination of the business relationship. 8. Refer to Section 8 of Part II of the Guidance Notes for guidance on Record Keeping Procedures . Filing A SAR 9. Refer to Section 9 of Part II of the Guidance Notes, and Section 34 of the AMLRs and Section 136 of the Act for the role of the MLRO and reporting obligations. 10. It is important to note that SARs must be filed with the FRA in case of a suspicious transaction even if the transaction did not proceed. Training 11. Staff should be educated in the "Know Your Customer" requirements for the prevention of ML/TF. 12. Training should therefore cover not only the need to know the customer's true identity, but also, where a business relationship is being established, the need to know enough about the type of business activity expected in relation to the customer at the outset (and on an ongoing basis) so that normal activity can be distinguished from suspicious activity in the future, as it relates to that person. 13. New frontline agents should not be allowed to process transactions until they have participated in the required training and successfully passed the requisite test(s). They should also be adequately trained on the factors which may give rise to suspicions about customers activities and the procedures to adopt when a transaction appears suspicious. 14. For further details, refer to Section 10 of Part II of the Guidance Notes. Independent Audit Function 15. MSBs must have procedures of internal control including an appropriate internal audit function for the prevention of ML/TF. The internal audit function serves to test the MSB s system of internal control and is to be appropriate to the MSB s size and to the nature of its operations. 16. Testing should be risk-based, with particular emphasis on high-risk operations. 17. It should be independent, conducted periodically, and reported directly to the Board. The audit report must include, but not be limited to, the following: (1) review of high risk accounts, transactions, and customers; (2) one-off transactions in excess of the limit set by the MSB and suspicious activity reporting; Page 187 of 245 (3) assessment of money remittance, currency exchange and check cashing transactions (to ensure whether they are in accordance with the relevant Acts, regulations, rules and guidance); (4) review of adequacy of customer identification information and CDD; and (5) complex and unusual transactions. H. ML / TF WARNING SIGNS OR RED FLAGS Customer Profile 1. The following are some of the warning signs and red flags that money transmission/remittance provider (MRPs) should be alert to in respect of a customer s profile. The list is not exhaustive, but includes: (1) The Customer s area of residence is inconsistent with other profile details such as employment; (2) The size or frequency of the transaction(s) is not consistent with the normal activities of the customer; (3) The goods/currencies purchased, and/or the payment arrangements are not consistent with normal practice for the type of business concerned; (4) The customer s only address is a post office box or a c/o (in care of) address; (5) The customer s address is that of a company service provider (domiciliation service); (6) The customer s address information is difficult to verify; (7) The stated address does not exist; (8) A large number of persons are registered at the stated address, or there are a very large number of changing occupants, or other information is available indicating that it is not the real address of residence or domicile; (9)

The address of customer s residence does not correspond to the customer s financial arrangements; (10) The customer changes address frequently; (11) The customer is a business whose name and purpose do not correspond with its transactions; (12) The customer cannot immediately provide additional identification documents; (13) Identification documents appear to be unused; (14) Identification documents are soiled making it difficult to read the necessary information; (15) The customer is known to have a criminal history; (16) The customer is close to a person who is known to have a criminal history; (17) Sudden change in the customer s lifestyle; (18) The customer drives very expensive cars that do not correspond to his/her income situation; (19) The customer hires or leases costly assets (e.g., real estate or cars) that do not correspond to his/her income situation. Customer Behaviour 2. The following are some of the warning signs and red flags that MRPs should be alert to in respect of a customer s behaviour. The list is not exhaustive, but includes: Page 188 of 245 (1) The customer is unwilling to provide details of his/her identification information and references; (2) Use of false identification documents to send money; (3) Customer changes a transaction after learning that he/she must show ID; (4) The customer shows no interest in costs or rates; (5) The customer does not choose the simplest way to carry out a transaction; (6) The customer has no connection with the area where the customer relationship is established; (7) Transaction is a price-raising link in a series of transactions with no obvious reasons for the choice; (8) The customer gives a rather detailed explanation that appears to be rehearsed concerning the reasons for the customer relationship or the transaction; (9) The customer does not respond to communication/letters to the stated address; (10) The customer has many newly established companies; (11) The customer contracts a loan secured on lodging of equivalent security; (12) The customer has companies abroad that are not justified by the customer s business; (13) The customer explains that expensive assets are a loan from or financed by a third party; (14) The customer uses a payment card from a country which is not his country of residence. Transactions General 3. The following are some of the warning signs and red flags that MRPs should be alert to in respect transactions generally. The list is not exhaustive, but includes: (1) The transaction seems to involve unnecessary complexity; (2) Use of front/straw men and/or shell companies; (3) Transactions in a series are structured just below the threshold for due diligence identity checks; (4) The customer appears to be trying to avoid reporting requirements by using two or more locations or cashiers on the same day or in quick succession to break one transaction into smaller transactions; (5) Two or more customers appear to be trying to avoid reporting requirements and seem to be working together to break one transaction into two or more transactions; (6) Transactions are carried out by the customer on behalf of third parties without there being an appropriate business relationship with such parties; (7) Frequent transaction orders are made by the same customer; (8) Sudden increases in the frequency/value of transactions of a particular customer without reasonable explanation; (9) An unusually large (cash) transaction; (10) The amount of the transaction is unusually large for the typical customer or for the MSB; (11) The transaction has no apparent purpose or no obvious economic/financial basis; (12) Unnecessary routing of funds through third parties; (13) A customer sends/receives funds to/from him/herself, for no apparent purpose; Page 189 of 245 (14) There is no genuine reason for the customer to use the services of the MSB; (15) Transfers of large sums of money to or from overseas locations with instructions for payment in cash; (16) One legal/natural person transfers sums to many legal/natural persons; (17) One legal/natural person receives sums from many legal/natural

persons (from various countries); (18) Many legal/natural persons (who have no obvious blood/business relation) are beneficial owners of transfers ordered by one legal/natural person; (19) An under-aged person receives funds from many legal/natural persons and/or from different locations; (20) A customer sends/receives funds to/from counterparts located in jurisdictions which are known to be exposed to ML/TF risks, for example, drug trafficking, terrorism financing, smuggling; (21) Transactions are accompanied by information which appears clearly false or contradictory; (22) The customer is unwilling to provide routine information when requested or the information provided is insufficient, false, or hard for the MSB to verify; (23) No or limited information about the origin of funds; (24) The explanation for the business activity and/or the funds involved is not credible; (25) Electronic transfers involving large sums of money does not include data allowing for the clear identification of such transactions; (26) The customer is accompanied by others who keep a low profile or stay just outside the location; (27) The customer reads from a note he apparently did not write himself; (28) The customer receives instructions from others; (29) The customer appears to be in doubt when asked for further details; (30) Difficulty in obtaining details of the beneficial owners; (31) No relationship between sender and beneficiary; (32) The supporting documentation does not add validity to the other information provided by the customer; (33) The customer is in a hurry to rush a transaction through, with promises to provide the supporting information later; (34) The customer represents a business but seems to have no business experience; (35) The authority for others to collect funds does not seem to be well-founded; (36) Correspondence is to be sent to another person other than the customer; (37) Form is filled in advance; (38) The pattern of transactions has changed since the business relationship was established; (39) Money transfers to high-risk jurisdictions without reasonable explanation, which are not consistent with the customer s usual foreign business dealings; (40) Sudden increases in the frequency/value of transactions of a particular customer without reasonable explanation; (41) Instruction on the form of payment changes suddenly just before the transaction goes through; (42) The customer, without a plausible reason, repeatedly goes to agents located far from his/her place of residence or work; (43) Funds are sent at a time not associated with salary payments; (44) Remittance sent or received outside customers remittance corridors. Page 190 of 245 Cash transactions 4. The following are some of the warning signs and red flags that MRPs should be alert to in respect of cash transactions. The list is not exhaustive, but includes: (1) Unusually large cash payments in circumstances where payment would normally be made by cheque, bank draft, etc; (2) Cash is in used notes and/or small denominations (possible indication that the money originates from the criminal offence) and dirty or has an unusual odour; (3) Customer refuses to disclose the source of cash; (4) Customer has made an unusual request for collection or delivery; (5) Stains on the notes indicating that the funds have been carried or concealed, or the notes smell musty, are packaged carelessly and precipitately; (6) When the funds are counted, there is a substantial difference between the actual amount and the amount indicated by the customer (over or under); (7) Detection of counterfeit banknotes in the amount to be transferred or exchanged; (8) Presenting funds in cash with further transfer of funds to another person on the same or next Day. Other Indicators for Money Remittance /Transmission Providers General 5. The following are some of other indicators to which MRPs should be alert. The list is not exhaustive, but includes: (1) Transferring funds without any apparent economic reason; (2) Money transfers to high-risk jurisdictions without reasonable explanation, which are not consistent with the customer s usual business

dealing; (3) Transfers paid by large cash amounts in different sums in a short period of time; (4) Personal remittances sent to jurisdictions that do not have an apparent family or business link; (5) Remittance made outside migrant remittance corridors (e.g., Asian foreign domestic remits funds to South America); (6) Personal funds sent at a time not associated with salary payments; (7) The customer seems only after the counting to know which amount is being transferred; (8) The customer shows no interest in the transfer costs; (9) The customer has no relation to the country where he/she sends/receives the money and cannot sufficiently explain why money is sent there/received from there; (10) The customer has a note with information about payee but is hesitating if asked whether to mention the purpose of payment; (11) Large or repeated transfers between the account of a legal person and a private account, especially if the legal person is not a resident; (12) Large or frequent transfers of money; (13) Use of groups of people to send money; (14) Use of different money remittance businesses; (15) Amounts sent are higher than usual; (16) The operations are irregular; Page 191 of 245 (17) Receiving money from different parts of the world (developed countries) from different people; (18) Money is received during short periods of time; (19) Money is received from different money remittance companies; (20) Multiple senders to a single individual. Other Indicators for Currency Exchange Service Providers General 6. The following are some of other indicators to which Currency Exchange Providers should be alert. The list is not exhaustive, but includes: (1) Exchange of large quantities of low denomination notes for higher denominations; (2) Exchange of large amounts or frequent exchanges that are not related to the customer s business; (3) Structuring of large amounts; (4) Repeated requests for foreign exchange purchasing-selling transactions in the amounts slightly less than the transaction limit for identification in a short period of time; (5) The customer requests currency in large denomination notes; (6) The customer buys currency that does not fit with what is known about the customer s destination; (7) The customer buys currency from an unusual location in comparison to his/her own location; (8) The customer apparently does not know the exact amount being exchanged; (9) The customer looks around all the time and does not watch the counting of money; (10) The customer is happy with a poor exchange rate; (11) Currency purchases with large cash amounts; (12) Large exchanges between foreign currencies; (13) Frequent exchange of cash into other currencies; (14) Exchange of primarily one type of currency; (15) The amounts exchanged are significantly higher than usual; (16) There is no link between the amount of money exchanged and holiday periods; (17) High frequency of currency exchange transactions over a period of time; (18) Many currency exchange offices used by the same person; (19) Requests to exchange large amounts of foreign currency which is not convertible (or not frequently used) to another kind of foreign currency. Page 192 of 245 SECTION 2 CAYMAN ISLANDS DEVELOPMENT BANK A. OVERVIEW 1. The CIDB is solely owned by the Cayman Islands Government. The principal function of CIDB is to mobilise, promote, facilitate, and provide finance for the expansion and strengthening of the economic development of the Islands. The Bank does this by providing financing for tertiary education, housing, agriculture and the development of small businesses. The CIDB does not accept deposits and therefore the sector guidance are geared toward ML/TF risks in loans. B. SCOPE 1. This section is applicable to the CIDB. C. ML/TF 1. The involvement of multiple parties may increase the risk of ML/TF when the source and use of the funds are not transparent. This lack of transparency can create opportunities in any of the three stages of ML/TF schemes. These schemes could include the following: (1) Loans are made for an ambiguous or illegitimate purpose. (2) Loans are

made for, or are paid for, a third party. (3) The customer attempts to sever the paper trail between the borrower and the illicit funds. D. RISK BASED APPROACH 1. The CIDB must adopt a risk-based approach to managing ML/TF risks. The RBA aims to support the development of mitigation measures that are commensurate to the ML/TF risks identified. Entities should refer to Section 3 of the Part II of these Guidance Notes. E. CUSTOMER DUE DILIGENCE Who is the customer/applicant for business? 1. The applicant may be any one of the following: (1) Natural persons; (2) Corporate persons or persons holding a trade and business licence. 2. The below table shows minimum identification information requirements; however, FSPs shall consider the relevant guidance provided under Section 4 of Part II of these Guidance Notes. Page 193 of 245 Applicant for Business Minimum Requirements Natural Person (1) Identification documentation should be obtained for the applicant/customer him/herself. (2) Satisfactory evidence, confirmed by using one or more of the verification methods: (a) Current valid passport; (b) Any valid uniquely numbered government-issued ID card showing the photograph of the applicant, such as a driver s licence or a voter s registration card; and (c) A Cayman Islands employer ID card bearing the photograph and signature of the applicant. Corporate Customer (1) The company (evidence that it exists) e.g. a trade and business licence or a certificate of registration. (2) Consistent with that required for direct personal customers, documentary evidence of identity for all directors; all those with signing powers, including third parties; and beneficial owners. (3) Satisfactory evidence, confirmed by at least one of the following independent checks, of company s existence: (a) Memorandum and Articles of Association and Certificate of Incorporation (b) Copy of Trade and Business Licence When must identification be obtained? 3. Customer identification information is to be obtained prior to extending any loan facility to the customer. 4. If identification information is not obtained, the loan facility should not proceed. F. INDEPENDENT AUDIT FUNCTION 1. The CIDB must have internal control procedures including an appropriate internal audit function for the prevention of ML/TF. The CIDB should have policies, procedures, and processes to monitor, identify, and report unusual and suspicious activities. The sophistication of the systems used to monitor lending account activity should conform to the size and complexity of the lending business. Page 194 of 245 2. The CIDB must liaise with the internal auditor to ensure that AML/CFT audits are regularly conducted in order to strengthen the processes and procedures and readily identify and address any risks of ML/TF. G. WHAT WARNING SIGNS OR RED FLAGS SHOULD THE CIDB BE ALERT TO? 1. The following are some of the warning signs and red flags that the CIDB should be alert to in respect of a customer s profile. The list is not exhaustive, but includes: (1) Sudden/unexpected payment on loans. A customer may suddenly pay down or pay off a large loan, with no evidence of refinancing or other explanation. (2) Reluctance to provide the purpose of the loan, or the stated purpose is ambiguous, inconsistent or inappropriate (use of loan proceeds). (3) Loan payments by third parties. Loans that are paid by third party could indicate that the assets securing the loan are really those of the third party who may be attempting to hide the ownership of illegally gained funds. (4) Collateral pledged by a third party. (5) Financial statement composition of a business differs greatly from those of similar businesses. (6) Mortgage financing with a request for an unusually short maturity term. H. TRAINING 1. Staff should be educated in various areas of AML/CFT compliance, and mainly in relation to CDD requirements and identification of suspicious activities for the prevention of ML/TF. Training should therefore cover not only the need to know the customer's true identity, but

also, where a business relationship is being established, the need to know enough about the (type of business) activity expected in relation to the customer at the outset (and on an ongoing basis) so that normal activity can be distinguished from suspicious activity in the future, as it relates to that person. 2. For further details, refer to Section 10 of Part II of the Guidance Notes. I. DOCUMENTATION OF POLICIES AND PROCEDURES 1. The CIDB should have documented policies and procedures in relation to various AML/CFT systems such as: (1) the assessment of risks; (2) Risk management and mitigation measures; (3) customer identification and due diligence; (4) when will EDD be applied and what does it entail; (5) suspicious activity reporting; (6) internal controls; and (7) staff training. J. RECORD KEEPING 1. The CIDB must keep adequate records of the identity of its customers, all transactions conducted by and any information relevant to that customer for a Page 195 of 245 period of 5 years following the last transaction, the closing of an account, or the termination of the business relationship. 2. Refer to Section 8 of Part II of the Guidance Notes for further details on record keeping procedures. K. FILING A SAR 1. Refer to Section 9 of Part II of the Guidance Notes, and Section 34 of the AMLRs and section 136 of the Act for the role of the MLRO and reporting obligations. 2. It is important to note that SARs must be filed with the FRA in case of a suspicious transaction even if the transaction did not proceed. Page 196 of 245 SECTION 3 LOANS BY UN-SUPERVISED LENDERS A. OVERVIEW 1. The Monetary Authority does not supervise all lenders within the Cayman Islands; however, there has been and continues to be a need for persons/organisations engaged in facilitating short term loans to adhere to the AML/CFT legislative requirements. These facilities usually include Pay Day Loans . 2. Un-supervised lenders 87 are governed by the AMLRs and these Guidance Notes and must operate their businesses in line with the laws of the Cayman Islands. B. SCOPE 1. This section of the Guidance Notes provides guidance to the un-supervised lenders. C. ML/TF RISKS 1. The Un-supervised lenders risk assessments should take into consideration factors such as: (1) Its customer types (taking into account customer occupation or type of business operated); (2) The geographical location of customers or where funds are transmitted; and (3) The purpose of the loan. D. RISK BASED APPROACH 1. Un-supervised lenders must adopt a risk-based approach to managing the ML/TF risks inherent to their business and associated with their customers. The RBA aims to support the development of mitigation measures that are commensurate to the ML/TF risks identified. Entities should refer to Section 3 of the Part II of these Guidance Notes. E. CUSTOMER DUE DILIGENCE Who is the Customer/Applicant for business? 1. The applicant may be any one of the following: (1) Natural persons; (2) Corporate persons; or (3) Persons holding a trade and business licence. 2. The below table shows minimum identification information requirements; however, Un-supervised lenders shall consider the relevant guidance provided under Section 4 of Part II of these Guidance Notes. 87 FSPs that are conducting lending activity but are not supervised (by any supervisory authority) Page 197 of 245 Applicant for Business Minimum Requirements Natural Person (1) Identification documentation should be obtained for the customer him/herself. (2) Satisfactory evidence, confirmed by using one or more of the verification methods: (a) Current valid passport; (b) Any valid uniquely numbered government-issued ID card showing the photograph of the applicant, such as a driver s licence or a voter s registration card; and (c) A Cayman Islands employer ID card bearing the photograph and signature of the applicant. Corporate Customer (1) The company (evidence that it exists) e.g. a trade and business licence or a certificate of registration. (2) Consistent with

that required for direct personal customers, documentary evidence of identity for all directors; all those with signing powers, including third parties; and beneficial owners. (3) Satisfactory evidence, confirmed by at least one of the following independent checks, of company s existence: (a) Memorandum and Articles of Association and Certificate of Incorporation (b) Copy of Trade and Business Licence 3. Un-supervised lenders are required to collect identification documentation for all loans issued. (See Section 4 of Part II of the Guidance Notes) F. WHAT WARNING SIGNS OR RED FLAGS SHOULD FSPs BE ALERT TO? 1. The following are some of the warning signs and red flags that should be alert to in respect of a customer s profile. The list is not exhaustive, but includes: (1) Sudden/unexpected payment on loans. A customer may suddenly pay down or pay off a large loan, with no evidence of refinancing or other explanation; (2) Reluctance to provide the purpose of the loan, or the stated purpose is ambiguous, inconsistent or inappropriate use of loan proceeds; and (3) Loan payments by third parties. Loans that are paid by a third party could indicate that the assets securing the loan are really those of the third party who may be attempting to hide the ownership of illegally gained funds. Page 198 of 245 GUIDANCE NOTES ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING ,TERRORIST FINANCING AND PROLIFERATION FINANCING IN THE CAYMAN ISLANDS PART VIII SECTOR SPECIFIC GUIDANCE: SECURITIES INVESTMENT BUSINESS This purpose of Part VIII of the Guidance Notes is to deal with AML / CFT matters pertaining to Securities Investment Businesses that require more explanation or are more complex issues than are dealt with in the general body of these Guidance Notes. This section must be read in conjunction with Part I and II of the Guidance Notes and the Appendices. Page 199 of 245 SECTION 1 SECURITIES INVESTMENT BUSINESSES (SIBS") A. OVERVIEW 1. Schedule 1 of the Securities Investment Business Act (2020 Revision) (SIBA) defines securities as: (1) shares, or stock of any kind in the share capital of a company; (2) debentures, loan stock, bonds certificates of deposit and any other instrument that creates or acknowledges debt (excluding various banking and monetary instruments e.g. cheques, mortgage instruments and land charges); (3) warrants and other instruments which confer contractual or property rights; (4) options on any security and on any currency, precious metal or an option on an option; (5) futures, and (6) rights under contracts for differences (e.g. cash-settled derivatives such as interest rate and stock index futures, forward rate agreements and swaps). 2. The SIBA provides for the regulation of persons carrying on securities investment business, including the regulated activities of market makers, broker-dealers, securities arrangers, securities advisors and securities managers, in or from the Cayman Islands. 3. Pursuant to the SIBA, persons engaged in securities investment business must hold a Securities Investment Business Licence, unless the person falls in one of the categories set out in Schedule 4 of the SIBA who do not require a licence to conduct securities investment business. 4. Under the SIBA, the Monetary Authority is directly responsible for licensing, and for supervision and enforcement in respect of licensees. It is also responsible for the investigation of persons where it believes that they are, or have been undertaking securities investment business without a licence or an exemption as an Excluded Person under Section 5(2) and Schedule 4 of the SIBA to do so. 5. The Monetary Authority regulates securities investment business in accordance with: (1) the SIBA and its regulations, namely: (a) The Securities Investment Business (Licence Applications and Fees) Regulations, 2003; (b) The Securities Investment Business (Conduct of Business) Regulations, 2003; and (c) The Securities Investment Business (Financial Requirements

and Standards) Regulations, 2003; (2) the relevant rules, guidance, policies and procedures issued by the Monetary Authority; and (3) international supervisory standards issued by the IOSCO. Page 200 of 245 6. The Monetary Authority s powers and duties are more particularly set out in Sections 16 and 17 of the SIBA. Under Section 18, the Monetary Authority can apply to the Grand Court for injunctions and restitution and disgorgement orders. B. SCOPE 1. The sector specific guidance contained in this section is applicable to persons carrying on securities investment business (SIB) as defined in the PoCA wherein SIB has the meaning assigned in the SIBA. Although not required to be licensed, persons specified in Schedule 4 of the SIBA are considered to be carrying on SIB and therefore required to comply with the AMLRs and PoCA. Parts I and II and this Part (VII) of the Guidance Notes are therefore applicable to persons licensed under the SIBA and to persons specified in Schedule 4 of SIBA. C. MONEY LAUNDERING AND TERRORIST FINANCING RISKS 1. Securities investment business activities carry a certain degree of ML/TF risks due to having exposure to factors including but not limited to: Products and services (1) Securities arranging and advising may be deemed less risky than broker dealers, market makers and investment managers because a securities advisor may not be directly involved with the exchange of funds from their customers; and a securities arranger may bring two parties together to facilitate a transaction only. (2) At times, particular activities may not involve face to face identity verification as for example calls to place trades may be executed by a securities investment business and/or access to remotely execute such trades may occur although identity theft, cybersecurity and pretexting may be prevalent in such circumstances. (3) Other factors for consideration with products can be based on the complexity, liquidity, volume and value of products being bought or sold on behalf of customers. Are there ethical agreements for discretionary trading accounts between customers and security investment businesses? Are third party deposits accepted? Are credit cards accepted for payment? (4) Full due diligence should be conducted for all parties that have outsourcing responsibilities for registered and/or licensed securities investment businesses and should be monitored on a regular basis. Country Risk (5) Having customers located in multiple international locations can increase the risk of money laundering and terrorist financing. Security investment businesses should be especially careful when dealing with investors who are PEPs of a foreign jurisdiction or those from a country on a sanctions list. (6) Customers based in/controlled or owned by persons based in high risk jurisdictions should also be particularly monitored. Page 201 of 245 Customer Type/Investor Profile (7) In addition to the country of domicile of customers, the types of individuals/entities that make up the customer base can also increase the risk of money laundering and terrorist financing. (8) All things being equal, institutional customers from large financial institutions that are regulated and/or listed on a stock exchange could be considered less risky than investors in the form of companies and trusts with complex structures, PEPs, charities or high net worth individuals for example. (9) Smaller institutions may have less awareness/insufficient staff to deal with potential red flags and/or ML/TF issues. Source of Funds/Transparency (10) Investments with higher return rates such as equities, derivatives and options pose a greater risk of money laundering, especially if those trades are not coming from a regulated financial institution/trading platform i.e. OTC or a regulated jurisdiction. (11) Securities investment businesses must remain cognizant of, and have controls in place surrounding, types of trading activities in discretionary accounts, locations of funds and understand the risks posed by allowing such trading on their accounts. Market Manipulation (12) Market manipulation

tactics can be undertaken if securities investment businesses do not highly monitor the trading activities of their customers. For example, commission-based trading may lead to conflicts of interest/churning tactics. D. RISK BASED APPROACH (refer also to Section 3 of Part II) 1. FSPs carrying on Securities Investment Business are required to adopt a risk- based approach to managing ML and TF risks as set out in the AMLRs and in section 3 of Part II of these Guidance Notes. 2. SIBS should pay particular attention to risk assessment factors and risk variables that are in addition to those in Part II Section 3 or which present higher risks or greater inherent risks for SIBs. Such factors and variables may include the ML/TF risk included in Section C above, the warning signs included in Section I below and other customer, product, service, transaction or delivery issues contained in these (Part VII) sector specific guidance. Page 202 of 245 E. SYSTEMS, POLICIES AND PROCEDURES Who is the applicant for business? 1. The applicant for business may be one of the following: Where the Financial Services Provider Applicant for Business is acts as agent in buying, selling, managing, subscribing for or underwriting securities. the principal acts as principal or makes arrangements in buying, selling, managing, subscribing for or underwriting securities. the counterparties advises an investor or potential investor on the merits for buying, selling, managing subscribing for or underwriting securities. the investor or potential investor Customer Due Diligence (refer also to Section 4 of Part II) When must the identity be verified? 2. The Regulations provide that there should be procedures in place requiring, as soon as reasonably practicable after contact is first made with an applicant for business, either satisfactory evidence of the applicant s identity or that steps are taken which will produce satisfactory evidence of identity. 3. The time span in which satisfactory evidence has to be obtained depends on the particular circumstances and the practicalities of obtaining evidence before commitments are entered into between parties and before money passes. How might identification of existing customers be carried out? 4. Refer to Section 4 of Part II of these Guidance Notes. 5. If, after having conducted a risk assessment in accordance with Section 4 of Part II of the Guidance Notes, verification procedures or identification of an investor have not been completed prior to the date on which a redemption is to take place, the Securities Investment Business should use the opportunity of the redemption to seek satisfactory evidence of identity. 6. Payment of the redemption proceeds should be made only to the investor and not to a third party and only when the outstanding due diligence documentation has been collected and verified. 7. If payment has been made from an account in the name of the investor with a regulated bank in the Cayman Islands or in in a country assessed by the FSP as having a low degree of risk of ML/TF and the criteria set out in Section 4 of Part II of these Guidance Notes are adhered to, that will be sufficient evidence of identity. Page 203 of 245 8. It is important to note that the above scenarios are only permissible in circumstances where SDD is permissible. Particular issues on Verification of identity of investors One-off transactions 9. Refer to Section 4 of Part II of these Guidance Notes. Payment on an Account in a Bank in the Cayman Islands or in a country assessed by the FSP as having a low degree of risk of ML/TF 10. Refer to Section 4 of Part II of these Guidance Notes. Enhanced Due Diligence 11. SIBs should carry out EDD in situations as stipulated in the ALMRs and or in Part II of these Guidance Notes and or where the SIBA has identified or assessed that it is exposed to high ML/ FT risks. Examples of where EDD may be required include categories of customers specified in Section 4 of Part II of these Guidance Notes such as Associations, Not for Profit (Including Charities), PEPs, and those from High-Risk Countries. 12. Additional examples would

include cases in which a customer is confidentiality- driven, or presents a multi-layered structure of beneficial ownership for no apparent business reason, or when red flags are noticed. Information that should be obtained in relation to the proposed transaction, business and source of assets in addition to that listed in the Guidance Notes 13. Where the principal, counterparty(ies), or investor or potential investor is a natural person, sufficient information should be collected to anticipate normal business activity, including type of products required and general level of likely activity and investment goals. 14. Where the principal, counterparty(ies), or investor or potential investor is a legal person or legal arrangement, in addition to the information needed to establish normal business activity, sufficient information regarding intra-group relationships, if any; customers; service providers; and trading partners should also be collected to establish a trading profile which can be monitored against transactions. Internal Controls and Ongoing Monitoring 15. For each investment transaction, the Securities Investment Business should record the information required under Section 8 of Part II of these Guidance Notes. In addition, the Securities Investment Business should consider whether the transaction is consistent with the customer profile and customer s stated investment goals and expectations, and should also be alert to the red flags listed below. 16. Securities Investment Businesses must have internal reporting procedures in place to (1) identify and report suspicious activity, (2) monitor and ensure internal Page 204 of 245 compliance with Acts relating to money laundering, and (3) test the AML/CFT system consistent with the Regulations; and the Guidance Notes (Procedures). Although ultimate responsibility for maintaining and implementing satisfactory Procedures remains with the Securities Investment Businesses, the obligations may be met by delegating or outsourcing those functions. 17. A Securities Investment Business may delegate any of the Procedures to a regulated person in the Cayman Islands or a person in a country assessed by the FSP as having a low degree of risk of ML/TF, that is subject to the AML/CFT regime of that country, consistent with the requirements of Section 4 of Part II of these Guidance Notes, where applicable. The Securities Investment Business will be regarded by the Monetary Authority as being compliant with the Regulations and the Guidance Notes with respect to the Procedures if the delegate complies with the Procedures of such jurisdiction. 18. A Securities Investment Business may also delegate any or all of its obligations with respect to the maintenance of Procedures to a suitable third party or parties, whether within or outside the Cayman Islands, provided that such appointment is consistent with the requirements of Section 4 Part II of these Guidance Notes, where applicable. 19. The operators of the Securities Investment Business should document, either as a board resolution or otherwise, the manner in which the entity has met its obligation to maintain Procedures. Record Keeping What specific records should be kept and where? 20. Refer to Section 8 and 11 of Part II of these Guidance Notes. When may a successor Securities Investment Business rely on the customer verification evidence obtained by its predecessor? 21. Where a successor firm is acquiring existing Securities Investment Business, the successor must ensure that the necessary due diligence has been performed prior to performing the additional transactions. It may be possible to rely upon the evidence of identity obtained by a predecessor Securities Investment Business provided that the original files, or certified copies of the original files, are transferred to the successor Securities Investment Business and the successor firm has assessed the quality of the evidence on investor identity. Where insufficient evidence exists, it may be appropriate to supplement with additional evidence to meet the standards required

by these Guidance Notes. 22. At no time would it be appropriate to rely upon third parties, such as EIs. F. MT/TF WARNING SIGNS 1. It should be acknowledged that although the presence of any of the below- referenced behaviours does not necessarily indicate an inappropriate or illegal act, the Securities Investment Business should make enquiries and be satisfied with any explanations provided especially as more and more of these activities are present. Page 205 of 245 (1) Some of the warning signs are as follows: (a) customers who are unknown to the securities investment business and verification of identity / incorporation proves difficult; (b) customers who wish to deal on a large scale but are completely unknown to the securities investment business; (c) customers who wish to invest or settle using cash; (d) customers who use a cheque that has been drawn on an account other than their own; (e) customers who change the settlement details at the last moment; (f) customers who insist on entering into financial commitments that appear to be considerably beyond their means; (g) customers who accept relatively uneconomic terms, when with a little effort they could have a much better deal; (h) customers who have no obvious reason for using the services of the Securities Investment Business (e.g.: customers with distant addresses who could find the same service nearer their home base; customers whose requirements are not in the normal pattern of the service provider s business which could be more easily serviced elsewhere); (i) customers who refuse to explain why they wish to make an investment that has no obvious purpose; (j) customers who are introduced by an overseas agent based in a country noted for drug trafficking or distribution or a customer introduced by an overseas branch, affiliate or other service provider based in in a country not assessed by the FSP as having a low degree of risk of ML/TF; (k) customers who transfer funds or shares to accounts in a in a country not assessed by the FSP as having a low degree of risk of ML/TF; (l) customers who indulge in much activity with little or no profit over a number of jurisdictions; (m) customers who carry out large numbers of transactions with the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction, particularly if the proceeds are also then credited to an account different from the original account; (n) customers who purchase low grade securities in an overseas jurisdiction, sell locally and then purchase high grade securities with the proceeds; (o) customers who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments; (p) customers who wish to maintain a number of trustee or customers accounts which do not appear consistent with the type of business, including transactions which involve nominee names; (q) any transaction involving an undisclosed party; (r) transfer of the benefit of an asset to an apparently unrelated third party, or assignment of such benefit as collateral; (s) significant variation in the pattern of investment without reasonable or acceptable explanation. (2) Securities investment businesses also need to be aware that their employees could be targeted by money launderers and therefore should be aware of among the other characteristics or behaviour: Page 206 of 245 (a) changes in employee characteristics (e.g.: lavish lifestyles or avoiding taking holidays), and (b) changes in employee or agent performance, (e.g.: a dealer has remarkable or unexpected increase in performance). Page 207 of 245 GUIDANCE NOTES ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING IN THE CAYMAN ISLANDS PART IX SECTOR SPECIFIC GUIDANCE: VIRTUAL ASSET SERVICE PROVIDERS

This purpose of Part IX of the Guidance Notes is to provide guidance for virtual asset service

providers (VASPs) that require further explanation on issues than are dealt with in the general body of these Guidance Notes. This section must be read in conjunction with Part I and Part II of the Guidance Notes and the Appendices. Page 208 of 245 SECTION 1 VIRTUAL ASSET SERVICE PROVIDERS A. OVERVIEW 1. This guidance is issued to assist Virtual Asset Service Providers (VASPs), as defined in the Virtual Asset (Service Providers Act), (2022 Revision) (VASP Act), in better understanding and fully implementing their obligations as it relates to anti- money laundering/ countering financing of terrorism/countering proliferation financing (AML/CFT/CPF) 1 . 2. Schedule 6 of the PoCA lists activities falling within the definition of relevant financial business which includes providing virtual asset services . 3. The VASP Act provides a framework for the conduct of virtual asset service business in the Islands, the registration and licensing of persons providing virtual asset services and for incidental and connected purposes. 4. Sections 9(3)(d) and (e) of the VASP Act provides that all VASPs: must comply with the Anti-Money Laundering Regulations (2020 Revision) and other laws relating to the combating of money laundering, terrorist financing and proliferation financing; and for the purpose of ensuring compliance with the Anti-Money Laundering Regulations (2020 Revision), put in place anti-money laundering systems and procedures . 5. Both the VASP Act and PoCA define the terms virtual asset and virtual asset service in a similar manner. The VASP Act also defines the terms virtual asset service provider , virtual asset custodian , virtual asset custody service , virtual asset trading platform and virtual asset issuance . 6. When determining if an activity falls within the definition of a virtual asset service (VAS), it is important to consider the nature of the service and its function in practice. An activity such as issuing and/or trading in non-fungible tokens or virtual service tokens may still fall under the definition of a VAS if the tokens are to be used for payment or investment purposes in practice. Regardless of the terminology, activities should be considered on a case-by-case basis. B. SCOPE 1. The sector specific guidance contained in this section seeks to provide practical assistance to VASPs in complying with the AMLRs, interpreting and applying the general provisions of these Guidance Notes, and for VASPs to adopt sound risk management and internal controls for their operations. The Monetary Authority expects all VASPs to take account of this guidance and to fully comply with the relevant obligations as set out in the PoCA and the AMLR. 1 In this guidance where AML/CFT omits PF , reference should still be made (for any equivalent PF provisions) to Part II, Section 14 of the Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing. Page 209 of 245 2. The AMLRs have been extended to entities providing VAS as defined in the VASP Act and the PoCA. This is regardless of what technology or method of delivery is used by the VASP to conduct the virtual asset activities, and whether the VASP uses a decentralised or centralised platform, smart contract, or some other mechanism. 3. It is the responsibility of each VASP to have systems, policies, procedures and training in place to prevent ML/TF/PF. This means that each VASP must maintain identification verification and ongoing monitoring procedures, record-keeping procedures, and such other procedures and controls appropriate for the purposes of forestalling and preventing ML/TF/PF. 4. In accordance with the VASP Act, the term VASPs includes the following types of persons: (1) Virtual asset trading platforms; (2) Virtual assets (VAs) custodians such as wallet service providers; (3) Virtual asset issuers, whether registered or licensed; and (4) Professionals that participate in or provide, financial services related to virtual asset

issuance or the sale of a virtual asset. (5) Existing licensees conducting virtual asset services (including virtual asset custodial services, virtual asset trading platform services and virtual asset issuance). (6) Any person facilitating (i) the exchange or transfer of VAs to/from another virtual asset or fiat currency, (ii) the transfer of VAs, or (iii) the exchange between one or more other forms of convertible VAs on behalf of another person or entity. 5. Virtual service tokens, as defined in the VASP Act, are not captured in the Guidance Notes. Such items are non-transferable, non-exchangeable and non-refundable such as credit card awards, or similar loyalty program rewards or points, which an individual cannot sell onward in a secondary market. 6. The PoCA and VASP Act do not seek to regulate the technology that underlies VAs but rather the persons that may use technology or software applications to conduct, as a business, VAS on behalf of a natural or legal person. A person who develops or sells either a software application of a new virtual asset platform (i.e. a fintech service provider) therefore does not constitute a VASP when solely developing or selling the application or platform, but they may be a VASP if they also use the new application or platform to engage as a business in exchanging or transferring funds or VAs or conducting any of the other VAS or operations on behalf of another natural or legal person. Similarly, a decentralised finance (DeFi) application (i.e. the software program) is not a VASP but any person who maintains control or sufficient influence in the DeFi arrangements, even if those arrangements seem decentralised, may fall under the definition of a VASP where they are providing or actively facilitating VASP services. 7. Further, the PoCA and VASP Act do not aim to capture natural or legal persons that provide ancillary services or products to a virtual asset network, including hardware wallet manufacture and non-custodial wallets, to the extent that they do not also engage in or facilitate as a business any of the aforementioned VA activities on behalf of their customers. Page 210 of 245 C. FACTORS THAT GIVE RISE TO MONEY LAUNDERING, TERRORIST FINANCING, AND PROLIFERATION FINANCING RISKS Privacy and Anonymity: 1. VAs due to their features and characteristics, may have a higher ML/TF/PF risk associated with them. VASPs should be aware that a significant proportion of VAs held or used in a transaction may be associated with privacy-enhancing features or products and services that potentially obfuscate transaction or activities and inhibit a VASP s ability to know its customers and implement CDD and other effective AML/CFT/CPF measures, such as: a) Mixers or tumblers; b) Anonymity Enhanced Currencies (AEC) c) Obfuscated ledger technology; d) Internet Protocol (IP) anonymizers; e) Ring signatures; f) Stealth addresses; g) Ring confidential transactions; h) Atomic swaps; i) Non-interactive zero-knowledge proofs; j) Privacy coins; and k) A significant proportion of the VAs held or used in a transaction is associated with third party escrow services. 2. VAs can enable non-face-to-face business relationships and can be used to quickly move funds globally to facilitate a range of financial activities from money or value transfer services to securities, commodities or derivatives-related activity, among others. Risk-based scrutiny of customers and transactions should be applied in accordance with the type of business conducted and the value and volume of transactions. VASPs should consider utilizing a range of monitoring and digital footprint tools to mitigate risks such as; undertaking an analysis of the relevant blockchain, for the purpose of assessing any nexus to sources of risk, including the darknet and blacklisted addresses, particularly where the risk is significant or the volume of transactions is substantial. Decentralised Nature of VASPs business models: 3. VASPs business models can be centralised or decentralised.

Where it is decentralised, there is no central server or service provider that has overall responsibility for identifying users, monitoring transactions, reporting suspicious activity and acting as a contact point for law enforcement. Consequently, individuals and transactions may not be subject to risk assessment and mitigation processes equivalent to those required by AML/CTF/CPF regulation. Where VASPs deal with funds originating from decentralised systems, risk-based mitigation measures, such as blockchain analysis, should be applied. Cross Border Nature: 4. VASPs connections and links to multiple jurisdictions may give rise to ML/TF/PF risks. VASPs will need to ensure that they are able to effectively apply all AML/CTF/CPF processes in the jurisdictions in which they operate and compensate for any additional risk introduced by the cross-border nature of a transaction on a risk-sensitive basis. Page 211 of 245 Segmentation: 5. The infrastructure used to operate a virtual asset trading platform, make transfers and execute payments may be complex and may involve several entities in different jurisdictions. This increases the risk through partial oversight of virtual asset systems and may hinder access to relevant actors by law enforcement. In such instances, VASPs should seek to work together with other parties in the value chain so as to compensate for segmentation and provide a more robust AML/CTF/CPF framework. VASPs working with outsourced service providers or agents will retain responsibility for AML/CTF/CPF compliance by outsourced service providers and agents. Acceptability, Immutability and Convertibility: 6. A wide availability of points of acceptance of VAs to conduct transactions, the ability to exchange VAs into money or other VAs makes it harder to track transactions and gives rise to new types of financial crime not associated with traditional payment and financial services products including the risk of money laundering. While there may be no single mitigation control, a number of measures may be employed to mitigate the arising risks including documenting and tracking financial crime typologies. 7. Once a transaction has been validated, the record cannot easily be altered. This makes it more difficult for misappropriated VAs to be retrieved. Customers should be made aware of such risks to minimise the likelihood of accidental loss. Operational structure: 8. VASPs should take into account their operational structure in seeking to assess and mitigate risks in their operations. These include: (a) Whether the VASP operates entirely online (e.g. platform-based exchanges) or in person (e.g. trading platforms that facilitate peer-to- peer exchanges or kiosk-based exchanges); (b) The nature and scope of the VA account, product, or service (e.g., small value savings and storage accounts that primarily enable financially excluded customers to store limited value); (c) The nature and scope of the VA payment channel or system (e.g., open- versus closed-loop systems or systems intended to facilitate micro-payments or government-to-person/person-to-government payments); and (d) Any parameters or measures in place that may potentially lower the provider s (whether that provider is a VASP or other obliged entity that engages in VA activities or provides VA products and services) exposure to risk (e.g., limitations on transactions or account balance). 9. Specific higher-risk factors that VASPs should have regard to (in addition to the higher-risk classification factors set out in Section 3D of Part II of these Guidance Notes) include: (a) The ability of users to: (i) operate more than one account with the provider; (ii) operate accounts on behalf of third parties. (b) The customer: Page 212 of 245 (i) Is involved in virtual asset mining operations (either directly or indirectly through relationships with third parties) that take place in a high-risk jurisdiction, relate to higher-risk VAs (such as privacy coins) or where its organisation gives rise to higher risk;

(ii) Uses VPN, TOR, encrypted, anonymous or randomly generated or a temporary service; (iii) Requests an exchange to or from cash, privacy coins or anonymous electronic money; (iv) Sends VAs to a newly created address; (v) Persistently avoids thresholds through smaller transactions; (vi) Sends or receives VAs to/from peer-to-peer exchanges, or funds/withdraws money without using the platform s other features; (vii) Exploits technological glitches or failures to his advantage. (c) The VA comes from, or is associated with, the darknet or other illegal/high-risk sources, such as an unregulated exchange, or is associated with market abuse, ransomware, hacking, fraud, Ponzi schemes, sanctioned bitcoin addresses or gambling sites. 10. Specific low risk classification factors VASPs may consider (in addition to the factors set out in Section 3D of Part II of these Guidance Notes) include: (a) A low-risk nature and scope of the account, product, or service (e.g., small value savings and storage accounts that primarily enable financially-excluded customers to store limited value); (b) Product parameters or measures that lower the provider s exposure to risk, such as limitations on transactions or account balance; (c) The customer requests an exchange and either the source of or destination for the money is the customer s own account with a bank in a jurisdiction assessed by the VASP as low risk; (d) The customer requests an exchange and either the source of or destination for the virtual asset is the customer s own wallet that has been whitelisted or otherwise determined as low-risk; (e) The customer requests an exchange and either the source of or destination for the virtual asset relates to low value payments for goods and services; and (f) The results of a blockchain analysis indicate a lower risk. D. RISK MANAGEMENT Risk Assessment 1. Prior to engaging in VAS activities, VASPs must carry out a comprehensive and detailed risk assessment associated with the relevant technology, product, or business practice associated with VAs, in accordance with Section 3C of these Guidance Notes. 2. The obligation to conduct such a risk assessment is enshrined in Regulations 8 and 9 of the AMLRs, which require persons carrying out relevant financial business to take steps, appropriate to the nature and size of the business, to identify, assess, and understand its ML/TF risks in relation to customers, country, geographic region, Page 213 of 245 products, services or transactions, and delivery channels, and to undertake such a risk assessment in relation to new products and business practices, new delivery mechanisms, and new or developing technologies prior to their launch. a. Customer risk: (i) A customer s business and risk profile will determine the level and type of ongoing monitoring necessary and support the VASP s decision whether to enter into, continue, or terminate the business relationship. Risk profiles can apply at the customer level (e.g., nature and volume of trading activity, origin of virtual funds deposited, etc.) or at a cluster level, where a cluster of customers display homogenous characteristics (e.g., clients conducting similar types of transactions or involving the same VA). (ii) VASPs should periodically update customer risk profiles of business relationships in order to apply the appropriate level of CDD including ongoing monitoring. Monitoring transactions involves identifying changes to the customer s business and risk profile (e.g., the customer s behaviour, use of products, whether transactions to/from unhosted wallets, off-chain transactions where applicable and the amounts involved) and keeping it up to date, which may require the application of Enhanced Due Diligence measures. (iii) As part of its ongoing monitoring, a VASP should screen its customer s and counterparty s wallet addresses against any available blacklisted and/or sanctioned wallet addresses that countries might have made available. If there is a positive hit, the VASP should determine

whether additional mitigating or preventive actions are warranted, and where necessary not establish or continue the business relations. b. Product risk: The features of the service offered as well as the VA which customers may hold, store, transfer or exchange determine the overall risk associated with the product. Any changes to the service or VAs offered should be assessed for their impact on risk prior to their introduction. (See also Section 3D (11&12) of Part II of these Guidance Notes on risk assessment in relation to the use or development of new products/services etc). c. Transaction risk: The risk of a transaction is established by analysing the blockchain, where possible, to obtain transaction information. The transaction is scored for its risk by investigating the provenance of the relevant VAs establishing the time that has elapsed since any higher-risk event and the proportion of higher-risk VAs within the transaction. Blockchain analysis (also called blockchain tracing) is sometimes outsourced to an external service provider. However, outsourcing does not remove the VASP s Page 214 of 245 responsibility under the AMLRs, and VASPs should ensure that they undertake due diligence on the outsourced service provider when integrating that service into their business activities. Whether to employ blockchain analysis, the degree of analysis and the use of third parties should be decided using a risk-based approach. d. Geographical risk: Geographical risk relates both to the customer s place of establishment and the provenance of the virtual asset. Where information about the destination of funds is collected, this will also inform the assessment of geographical risk. Apart from the requirements relating to transactions and relationships involving high-risk third countries, VASPs should take into account publicly available information about the regulatory treatment and use of VAs in particular jurisdictions to assess geographical risk. e. Delivery channel risk: The risks related to how customers access a VASP s products or platform need to be considered. For example, whether they are only accessible online or whether physical infrastructures are being used and the manner by which a VA account is funded. 3. As part of its risk assessment, VASPs should determine whether the relevant risks, discussed above, can be appropriately mitigated and managed. In line with Regulation 8 of the AMLRs, the risk assessment must be documented, kept current, and be kept in a way that it is readily available to the Monetary Authority and other competent authorities under the PoCA. Risk Mitigation: AML/CFT Internal Controls 1. Pursuant to Regulation 8(2)(e) of the AMLRs, VASPs are required to implement policies, controls and procedures that enable them to manage and mitigate the risks that have been identified either at the national level through the NRA or by the VASP itself through its business risk assessment as set out in Chapter C, and to have such policies, controls and procedures approved by senior management. Such internal controls must be adequate to ensure proper risk management across the VASP s operations, departments, branches and subsidiaries, both domestically and, where relevant, abroad, and include appropriate governance arrangements where responsibility for AML/CFT is clearly allocated and a compliance officer is appointed at management level; controls to monitor the integrity of staff; ongoing training of staff; and an independent audit function to test the system. 2. In terms of operations, and in particular the conduct of transactions, control measures that may be employed (in addition to those outlined at Section 3E of Part II of these Guidance Notes) include: (a) Transaction limits, including limits on the total value of VAs that may be held, stored, transferred or exchanged; (b) Time delays before certain automated and manual transactions can be carried out with a view to restrict the rapid movement of funds,

where the delay implemented will depend on the product in question and associated risk typologies; and Page 215 of 245 (c) The prohibition of transfers of money to third parties (i.e., the name on source and destination accounts must match where money is exchanged for VAs or VAs for money). 3. The internal policies, controls and procedures must furthermore address the various topics detailed in Regulation 5 of the AMLRs, which include: (a) Customer due diligence (CDD) measures; (b) Related Measures for CDD such as Know Your Customer (KYC), Source of Funds etc; (c) Record keeping; (d) Implementation of targeted financial sanctions; and (e) Internal and SAR procedures. E. CUSTOMER DUE DILIGENCE 1. It is important to note who is the customer for the purposes of implementing CDD as it pertains to the use of VAs. For virtual asset trading platforms, the customer is generally the person requesting the exchange, regardless of the means of doing so. For custodian service providers, the customer is generally the person on behalf of whom they hold or transfer a virtual asset. For issuers, the customer is generally the person who is purchasing the newly created virtual asset. 2. Pursuant to Regulations 10 to 20 of the AMLRs, VASPs must apply the full set of CDD measures, including identification and verification measures in relation to customers and beneficial owners, obtaining information on the purpose and intended nature of the business relationship, and to conduct ongoing CDD throughout the lifespan of the business relationship. 3. Regardless of the nature of the relationship or transaction, VASPs must have in place effective procedures to identify and verify the identity of a customer, including when establishing business relations with that customer; where VASPs may have suspicions of ML/TF/PF, regardless of any exemption of thresholds; and where they have doubts about the veracity or adequacy of previously obtained identification data. 4. Pursuant to Regulation 12 of the AMLRs, VASPs and other related parties should collect the relevant CDD information on their customers when they provide services to or engage in virtual asset activities on behalf of their customers and verify the customer s identity using reliable independent source documents, data or information. Such information would include the customer s name and further identifiers such as physical address, date of birth, and a unique national identifier number (e.g., national identity number or passport number). As stipulated in Regulation 12 of the AMLRs, VASPs are also required to collect additional information to assist in verifying the customer s identity when establishing the business relationship at onboarding, determine the customer s business and risk profile and conduct ongoing due diligence on the business relationship. Such information could include, for example an IP address with an associated time stamp; geo-location data; device identifiers; wallet addresses; and transaction hashes. VASPs may also match a customer s addresses against a list of blacklisted addresses on popular blockchains, e.g. addresses that have been misused or have been found to have been used by malicious individuals. The VASP should also seek to determine the provenance of a virtual asset e.g. if it has been moved from a blacklisted address recently. Page 216 of 245 5. In cases where a VASP carries out a one-off transaction, VASPs will be expected to undertake CDD measures in respect of each one-off transaction to be conducted. 6. Pursuant to Regulations 18 and 19 of the AMLRs, if a VASP is unable to obtain customer information, the transaction should not proceed and the VASP should consider filing a SAR to the FRA. 7. As prescribed in Regulations 27 and 28 of the AMLRs, where the ML/TF risk is higher based on the existence of any of the circumstances listed in Regulation 27 of the AMLRs, EDD measures must be taken. For

example, VA transfers from or associated with countries with significant levels of organised crime, corruption, terrorist or other criminal activity, including source or transit countries for illegal drugs, human trafficking, smuggling, and illegal gambling, or countries subject to sanctions or embargos, or countries with weak governance, enforcement and regulatory regimes may present higher risks for ML and TF. Other indicators may be risk factors associated with the VA product, service, transaction, or delivery channel, including whether the activity involves pseudonymous or anonymous transactions, non-face-to-face business relationships or transactions, and/or payments received from unknown or un-associated third parties. 8. EDD measures that may mitigate the potentially higher risks associated with the factors mentioned in Regulation 27 of the AMLRs include: a. corroborating the identity information received from the customer, such as a national identity number, with information in third-party databases or other reliable sources; b. tracing the customer s IP address; c. searching the Internet for corroborating information consistent with the customer s transaction profile; d. obtaining additional information on the customer and intended nature of the business relationship; e. obtaining information on the source of funds of the customer; f. obtaining information on the reasons for intended or performed transactions; and g. conducting enhanced monitoring of the relationship. 9. VASPs should also apply the requirements of Part VII AMLR on Politically Exposed Persons (PEPs). F. RELATED MEASURES FOR CDD 1. KYC a. KYC includes identifying and verifying the customer s identity, assessing the purpose and intended nature of the business relationship or transaction and identifying and taking reasonable measures to verify the identity of beneficial owners. b. The information collected as part of the KYC process may include wallet addresses and transaction hashes. Page 217 of 245 c. Where multiple VASPs are involved in one transaction, it may be helpful to develop reliance or outsourcing agreements on a bilateral basis in order to minimise duplication of KYC processes and improve the customer experience. 2. Blockchain Analysis a. Blockchain analysis processes are additional to KYC processes and take account of the unique opportunities afforded to virtual asset trading platform and virtual asset custodians by the blockchain. Blockchain analysis helps these providers to assess the risk of transactions. VASPs should consider how blockchain analysis may be appropriate to apply in line with a risk-based approach, including taking into account the nature of the business of the trading platform or virtual asset custodian and whether it would be appropriate to use it for all transactions. 3. Source of Funds a. Evidence of the source of funds must be collected with respect to all transactions that present a higher risk, including those that involve: An exchange of VAs for money or vice versa; An exchange of one virtual asset for another if the customer claims the virtual asset has been obtained through mining; and The transfer of a customer s VAs from one exchange to another. For transactions carried out under a business relationship, this evidence may only need to be collected once. b. It is good practice to collect information about the destination of funds in order to inform the assessment of risk (e.g., geographical risk) and aid transaction monitoring processes. Where a recipient s name has been collected, sanctions obligations apply in the usual way. 4. Ongoing Monitoring a. Monitoring transactions is an essential component in identifying transactions that are potentially suspicious (as discussed at Sections 3F and 16 of Part II of these Guidance Notes) including in the context of virtual asset transactions. Transactions that do not fit the behaviour expected from a customer profile, or that deviate from the usual pattern of

transactions, may be potentially suspicious. b. Monitoring should be carried out on a continuous basis and may also be triggered by specific transactions. Where large volumes of transactions occur on a regular basis, automated systems may be the only realistic method of monitoring transactions, and flagged transactions should go through expert analysis to determine if such transactions are suspicious. VASPs and other related entities should understand their operating rules, verify their integrity on a regular basis, and check that they account for the identified ML/TF/PF risks associated with VAs, products or services or activities. c. Monitoring under a risk-based approach allows VASPs and other related entities to create monetary or other thresholds to determine which activities will be reviewed. Defined situations or thresholds used for this purpose should be reviewed on a regular basis to determine their adequacy for the risk levels established. Page 218 of 245 G. RECORD KEEPING 1. VASPs are to maintain records on transactions and information obtained through CDD measures in line with Part VIII of the AMLRs, which shall include: information relating to the identification of the relevant parties, the public keys (or equivalent identifiers), addresses or accounts involved (or equivalent identifiers), the nature and date of the transaction, and the amount transferred. 2. The public information on the blockchain or other relevant distributed ledger of a particular virtual asset may provide a beginning foundation for record keeping, provided VASPs and third-party entities can adequately identify their customers. However, reliance solely on the blockchain or other type of distributed ledger underlying the virtual asset for recordkeeping is not sufficient. For example, the information available on the blockchain or other type of distributed ledger may enable relevant authorities to trace transactions back to a wallet address, though may not readily link the wallet address to the name of an individual. Additional information and procedures will therefore be necessary to associate the address to a private key controlled by a natural or legal person. H. IMPLEMENTATION OF TARGETED FINANCIAL SANCTIONS 1. VASPs are under a clear obligation to freeze without delay the funds or other assets (including VA) of designated persons or entities and to ensure that no funds or other assets are made available to or for the benefit of designated persons or entities in relation to the targeted financial sanctions related to terrorism or terrorist financing, or proliferation of weapons of mass destruction. Please refer to Section 13 of Part II of the Guidance Notes for more information on sanctions. 2. VASPs should be aware that some sanction lists may now include information on wallet numbers in addition to/instead of names. I. INTERNAL AND SAR REPORTING PROCEDURES 1. VASPs should have the ability to flag for further analysis any unusual or suspicious movements of funds, value or transactions or activity that is otherwise indicative of potential involvement in illicit activity regardless of whether the transactions or activities are fiat-to-fiat, virtual-to-virtual, fiat-to-virtual, or virtual-to-fiat in nature. 2. VASPs and their related entities should have appropriate systems so that such funds or transactions are scrutinised in a timely manner and a determination can be made as to whether funds or transactions are suspicious. Pursuant to Regulation 19 of the AMLRs, VASPs must promptly report suspicions of ML/TF to the FRA, including those involving or relating to VAs and/or providers that are suspicious. 3. Some indicators of unusual or suspicious activities related to VAs are: (a) In Relation to Transactions: (i) Structuring VA transactions (e.g. exchange or transfer) in small amounts under record-keeping or reporting thresholds, where applicable, similar to structuring cash transactions or making multiple high-value transactions (1) in a staggered and regular pattern, with no further transactions recorded

during a long period afterwards, which is particularly common in Page 219 of 245 ransom ware-related cases; or (2) to a newly created or to a previously inactive account. (ii) Transferring VAs immediately to multiple VASPs, especially to entities registered or operating in another jurisdiction, including obliged entities, where there is no relation to where the customer lives or there is a non-existent or weak AML/CFT/CPF regulation. (iii) Accepting/depositing funds from VA addresses that have been identified as holding stolen funds, or VA addresses linked to the holders of stolen funds. (iv) Depositing VAs at an exchange and then immediately withdrawing the VAs from a VASP immediately to a private wallet. This effectively turns the exchange/VASP into an ML mixer. (v) Converting a large amount of fiat currency into VAs, or a large amount of one type of VA into other types of VAs with no logical business explanation. (b) In relation to Anonymity: (i) The services of a VASP serve to generate anonymity. (ii) The VAs have a history (above average) of one or more mixers or trade history on the Dark web. (iii) Moving a VA that operates on a public, transparent blockchain, such as Bitcoin, to a centralised exchange and then immediately trading it for an AEC or privacy coin. (iv) VAs transferred to or from wallets that show previous patterns of activity associated with the use of VASPs that operate mixing or tumbling services or P2P platforms. (v) Funds deposited or withdrawn from a VA address or wallet with direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (e.g. ransomware) and/or theft reports. (c) In relation to Customers (whether sender or receiver): (i) Creating separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed by VASPs. (ii) Incomplete or insufficient CDD information, or a customer declines requests for CDD documents or inquiries regarding source of funds. (iii) A customer s VA address appears on public forums associated with illegal activity. (iv) A customer significantly older than the average age of platform users opens an account and engages in large numbers of transactions, suggesting their potential role as a VA money mule or a victim of elder financial exploitation. (v) A customer frequently changes his or her identification information, including addresses, IP addresses, or financial information, which may also indicate account takeover against a customer. (vi) Bulk of a customer s source of wealth is derived from investments in VAs, initial coin offerings (ICOs), or fraudulent ICOs, etc. Page 220 of 245 (vii) Customer has provided forged documents or has edited photographs and/or identification documents as part of the on- boarding process. (viii) A customer provides identification or account credentials (e.g. a non-standard IP address, or flash cookies) shared by another account. (d) In relation to Geographical risks: (i) Customer s funds originate from, or are sent to, an exchange that is not registered in the jurisdiction where either the customer or exchange is located. (ii) Customer sends funds to VASPs operating in jurisdictions that have no VA regulation, or have not implemented AML/CFT/CPF controls. 4. In the context of virtual asset issuers and ICOs, factors that could give rise to suspicious activity are: a) An ICO-project does not display team members, company information nor physical address. Team members do not have a social media profile. b) An ICO-project is trying to hide the amount of funds raised, by providing misleading, incomplete or suspicious information on their website or not providing proof of investments. c) An ICO-project either has no cap as to the amount of money required to develop its product or has set an extremely high cap. d) There is a guarantee of high returns that seems impossible to fulfil. e) An ICO-project has lack of information on the project or

lack of detail on how the technology works, there is no well-designed website. f) There are no development goals on a clear timeline. g) The ICO intends to convert a portion of the raised funds to fiat. h) The virtual currency has anonymity features that aid in the commission of illegal activity, services or transactions. 5. The above noted indicators (at paras 3 and 4) are neither exhaustive nor applicable in every situation. Indicators should be considered in the context of other characteristics about the customer and relationship, or a logical business explanation along with the general matters identified at Part II of these Guidance Notes. For more information on red flag indicators, see FATF Report on VAs Red Flag Indicators of Money Laundering and Terrorist Financing (September 2020), and any subsequent related documents. 6. Where a VASP detects suspicious activity, in relation to an incoming transfer of VAs from an external party that cannot be stopped due to processes associated with the blockchain, steps should be taken to restrict the actions that can be performed by its customer in relation to the suspicious funds, freeze the assets/funds (where possible) and report the suspicious activity. 7. VASPs should, where possible, implement the necessary controls to hold incoming VAs deemed suspicious and ensure that they are not released to their customers. 8. VASPs that control both the originating and beneficiary VASP must consider the information from both to determine whether to file a SAR. VASPs should file the suspicious activity report in the country from which the transfer of VAs originated or to which the transfer of VAs was destined and make relevant transaction Page 221 of 245 information available to the Financial Reporting Authority and the relevant authorities in the country from which the transfer originated or to which it was destined. 9. When assessing a transfer of VAs, or any related transaction, beneficiary VASPs should consider incomplete information about the originator as a factor in determining whether a transaction is suspicious. Where the transaction has been determined to be suspicious, this must be reported to the FRA. J. IDENTIFICATION AND RECORD-KEEPING FOR VIRTUAL ASSET TRANSFERS 1. When engaging in or providing services related to transfers of VAs in or from within Cayman Islands, VASPs are expected to collect and record information as follows: a) Originating VASPs should obtain and hold accurate originator and beneficiary information on virtual asset transfers, submit this information to the beneficiary VASP or financial institution (if any) immediately and securely 2 , and make it available on request to appropriate authorities. b) Beneficiary VASPs should obtain and hold required accurate originator information and required accurate beneficiary information on virtual asset transfers and make it available on request to appropriate authorities. c) VASPs receiving a VA transfer from an entity that is not a VASP or other obliged entity (e.g., from an individual VA user using his/her own DLT software, such as an unhosted wallet) or sending to a non-obliged entity, should obtain the required originator/beneficiary information from their customer. 2. Information to be collected and recorded for the originating VASP include the: a) originator s name (i.e., the sending customer) and the name of the beneficiary; b) where an account is used to process the transfer of VAs by (i) the originator, the account number of the originator; or (ii) the beneficiary, the account number of the beneficiary; c) the address of the originator, the IP address, the wallet address, the number of a Government issued document evidencing the originator s identity or the originator s customer identification number or date and place of birth; and d) where an account is not used to process the transfer of VAs, the unique transaction reference number that permits traceability of the transaction. 3. Information to be collected and recorded for the beneficiary

VASP include the: a) originator s name (i.e., the sending customer) and the name of the beneficiary; b) where an account is used to process the transfer of VAs by (i) the originator, the account number of the originator; or (ii) the beneficiary, the account number of the beneficiary; c) the address of the beneficiary, the IP address, the wallet address, the number of a Government issued document evidencing the beneficiary s 2 Immediately means that VASPs should submit the required information prior, simultaneously, or concurrently with the transfer itself. Securely is meant to convey that VASPs should transmit and store the required information in a secure manner. This is to protect the integrity and availability of the required information to, inter alia, facilitate record-keeping, facilitate the use of such information by the receiving VASPs or other obliged entities and protect the information from unauthorised disclosure. Page 222 of 245 identity or the beneficiary s customer identification number or date and place of birth; and d) where an account is not used to process the transfer of VAs, the unique transaction reference number that permits traceability of the transaction. 4. VASPs are expected to keep records of complete information on the originator and beneficiary which accompanies each transfer of VAs for at least five years. 5. Where technical limitations prevent an intermediary VASP from sending the required originator or beneficiary information with the transfer of VAs, including interoperability issues, the intermediary VASP must keep a record of all the information received from the originating VASP, obliged entity or other intermediary, for at least five years. 6. VASPs should submit the required information simultaneously or concurrently with the transfer. 7. Other requirements such as monitoring of the availability of information and taking freezing action and prohibiting transactions with designated persons and entities also apply. The same obligations apply to financial institutions when sending or receiving virtual asset transfers on behalf of a customer. K. TRANSFERS OF VAS 1. VASPs must use all relevant documents and data obtained to effectively verify the information on the originator when conducting the transfer of VAs; and the beneficiary when receiving the transfer of VAs. 2. Originating VASPs may provide the required information to beneficiary VASPs either directly, by attaching the information to the transfer, or by providing the information indirectly. 3. VASPs must ensure that transfers of VAs are conducted using a system which prevents the unauthorized disclosure of information. L. BATCH FILE TRANSFERS OF VAS 1. VASPs should ensure that, for batch file transfers of VAs from a single originator where the transfers of VAs are bundled together, the batch file should contain- i. the name of the originator; ii. the account number of the originator, where an account is used to process the transfer of VAs by the originator; iii. the address of the originator, the number of a Government-issued document evidencing the originator s identity or the originator s customer identification number or date and place of birth. 2. A batch file must contain the name, account number or unique identifier of the beneficiary that is traceable in the beneficiary country. Page 223 of 245 M. OBLIGATIONS OF A BENEFICIARY VASP 1. Beneficiary VASPs must have procedures in place to detect whether the system they are using to effect a transfer of VAs is obtaining all the required information. This can be either the messaging, or payment and settlement system, or any equivalent system. N. TRANSFERS OF VAs WITH MISSING OR INCOMPLETE INFORMATION ABOUT THE ORIGINATOR 1. Originating VASPs must not execute transfers of VAs where they are unable to collect and maintain the required information on the originator and beneficiary. 2. Beneficiary VASPs must have effective systems in place to detect missing required information on both the originator and beneficiary. 3. Where a

beneficiary VASP detects when receiving transfers of VAs, that the required originator information is missing or incomplete, the beneficiary VASP must either reject the transfer of VAs or request complete information on the originator. 4. Where the required originator or beneficiary information is incomplete, beneficiary VASPs must have risk-based policies and procedures to determine a) whether to execute, reject or suspend a transfer of VAs; b) the decision-making process and the resulting actions to be taken (for example any internal escalation and/or external reporting procedures). 5. Where an originating VASP regularly fails to supply the required information on the originator, the beneficiary VASP must adopt reasonable measures to rectify the non-compliance. This includes notifying the originating VASP of the non- compliance, giving reasonable timeframes for rectification, obtaining information as to the reasons for non-compliance and documenting the actions taken. This should be done prior to rejecting any future transfers of VAs, restricting its business relationship or terminating its business relationship with that originating VASP. The beneficiary VASP must report to the FRA and to the Authority its decision to restrict or terminate its business relationship with that originating VASP. O. REQUIREMENTS FOR INTERMEDIARY VASPS 1. Intermediary VASPs must have documented risk-based policies and procedures to determine when to execute, reject or suspend a transfer of VAs that is lacking the required originator or required beneficiary information. These policies and procedures must also address that the appropriate follow-up action to be taken which should include documenting the decision-making process. 2. Intermediary VASPs that participate in a transfer of VAs must ensure that all information received on the originator and the beneficiary that accompany a transfer of VAs is kept with the transfer of VAs. 3. Intermediary VASPs must take reasonable measures, which are consistent with straight-through processing, to identify transfers of VAs that lack required originator or beneficiary information. 4. Intermediary VASPs must also adopt risk-based policies and procedures for determining when to execute, reject or suspend a transfer of VAs for straight- Page 224 of 245 through processing of transfers of VAs, where the required originator or beneficiary information is incomplete. The policies and procedures must also include the decision-making process and the resulting actions to be taken (for example any internal escalation and/or external reporting procedures). P. OBLIGATION OF A VASP TO COMPLY WITH REQUIREMENTS 1. VASPs must comply with all relevant requirements in the countries in which they operate, either directly or through their agents. Page 225 of 245 GUIDANCE NOTES ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING IN THE CAYMAN ISLANDS PART X SECTOR SPECIFIC GUIDANCE: SECURITIZATION This purpose of Part X of the Guidance Notes is to provide guidance for special purpose vehicles (SPVs) carrying on relevant financial business under the Proceeds of Crime Act (POCA) as amended that require further explanation on issues than are dealt with in the general body of these Guidance Notes. This section must be read in conjunction with Part I and Part II of the Guidance Notes and the Appendices. 1. Page 226 of 245 SECTION 1 SECURITIZATION A. OVERVIEW 1. Securitization is a process that involves creating new financial instruments by pooling and combining existing financial assets, typically through an off-balance sheet bankruptcy remote special purpose vehicle (SPV), which purchases the assets using proceeds of securities issued to investors, usually in the form of debt. Payments of interest and principal on these securities is backed by the cash flow generated from the asset pool. Securitization transactions include the issuance of

collateralized debt obligations, collateralized loan obligations and asset backed securities, as well as all other similar transactions. The term investor refers to any person or entity purchasing a security issued by the SPV, including a bondholder, noteholder, preference shareholder and unitholder. 2. The Cayman Islands has company, trust, partnership and related Acts that allow a high degree of flexibility for establishing SPVs. Because of their structure, securitization SPVs that are not insurance securitization vehicles are generally not required to be registered or licensed by the Authority under any regulatory Act. Regardless, such securitization transactions may present ML/TF/PF risks. B. SCOPE 1. The sector specific guidance contained in this Part is applicable to non-insurance SPVs; the parties that provide services to such SPVs, including trustees, law firms, placement agents, clearing systems, asset servicers and administrators; and to securitization originators, investment managers, arrangers or sellers of assets (sponsor). 2. SPVs themselves are considered to be carrying on relevant financial business under the Proceeds of Crime Act (POCA) as amended, and as such are required to comply with the Anti-Money Laundering Regulations (AMLRs) as amended and the General AML/CFT/CPF Guidance provided in Part II of the Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands, August 2023 (Guidance Notes). In addition, various service providers to the SPVs may also be considered as carrying on relevant financial business under the POCA. 3. In this Part of the guidance, a reference to SPV captures only non-insurance securitization vehicles, whereas a reference to FSP includes the SPV as well as all its relevant service providers (i.e. those that are carrying on relevant financial business under the POCA). For guidance on insurance special purpose vehicles please see Part V of these Guidance Notes. C. MONEY LAUNDERING, PROLIFERATION FINANCING AND TERRORIST FINANCING RISKS 1. As is the case with most financial products, SPVs carry a certain degree of ML/TF/PF risks. Listed below are some, but not all, of these relevant risks. (1) Country Risk having counterparties located in multiple international locations or in high risk countries that have weak AML/CFT/CPF regimes can increase the risk of ML/TF/PF. (2) Counterparty/Investor Profile in addition to the country of domicile of investors, the types of individuals/entities that make up the investor base can also increase the risk of ML/TF/PF. All things equal, institutional investors and large financial institutions including Clearing Systems (see Section E.3 below), that are regulated and/or listed on a stock exchange could be considered less risky than investors in the form of trusts, charities or high net worth individuals for example. SPVs should be especially careful when dealing with investors who are PEPs of a foreign jurisdiction or those from a country on a sanctions list, including targeted financial sanctions relating to proliferation. (3) Source of Funds Administrators/asset servicers must remain cognizant of and have controls in place surrounding the source of subscription funds and the destination of distributions of SPVs. (4) Source of Assets in the Pool In circumstances where the sponsor originated the assets or purchased the assets before selling them to the SPV, the sponsor may procure the assets to be pooled using laundered funds or otherwise have illegitimately obtained the asset or may have misrepresented the source of the assets. (5) Terrorist Financing Risk On-going cash flows to investors generated by the asset pool can be an attractive source of funds for terrorist financiers. In addition, in circumstances where the sponsor sold the assets to the SPV, the sponsor could use the proceeds from the sale of the asset to finance terrorist activities. D. RISK-BASED APPROACH (refer also to Section 3 of Part II) 1. SPVs should carry out an

AML/CFT/CPF risk assessment of their overall structure. Given the lack of staff within an SPV, this risk assessment could be conducted by an external AML/CFT/CPF party contracted by the SPV. In this risk assessment, SPVs should consider risks arising from the nature and size of their business model, the geographical location of counterparties, the complexity of the transaction, the non-face-to-face basis for subscriptions, distributions and transfers, and types of securitized products that might be more attractive for financial crime. 2. Low and high-risk indicators, including the ML/TF/PF risks outlined in Section C above and the ML/TF/PF warning signs outlined in Section J below, should be Page 224 of 242 Page 225 of 245 considered when conducting risk assessments. SPVs should be aware of, and take into account, additional risk factors or risk variables that may be introduced where services, functions or activities of the SPV are outsourced or delegated, particularly so if the service provider is not subject to adequate AML/CFT/CPF laws and measures and/or is not adequately supervised. Background information, including information from rating agencies may be used to record the purpose of the transaction and to assess ML/TF/PF risks. E. APPLICANT FOR BUSINESS (refer also section 4 of Part II) 1. In order to forestall financial crime, including ML/TF/PF, it is important that background knowledge is obtained about all the participants in a securitization transaction, and not just those who are investors. This background gathering exercise should include measures to understand the ownership and control structure of the SPV as well as look at the beneficial ownership and any possible involvement of PEPs, establishing the purpose and intended nature of the business relationship and whether this is consistent with the transaction being undertaken. 2. An FSP that is the service provider to an SPV, in addition to verifying the identity of the sponsor and its beneficial owners, should satisfy itself that the securitization has a legitimate economic purpose. 3. In securitization transactions, securities can be issued in global form through clearing systems. The Depositary Trust Company in the United States, Euroclear and Clearstream Banking soci t anonyme in Europe, and the Canadian Depository for Securities are regulated financial institutions based in jurisdictions with strong AML/CFT/CPF regimes. Clearing Systems stand between the issuer and the buyer (becoming the buyer to the issuer and the seller to the buyer) and perform CDD on their participants and account holders. Reliance on a clearing system should be done on a risked-based approach and form part of an FSP s risk documentation. Table 1 - Who should be treated as the Applicant for Business? FSP Applicant for Business 1. The SPV (1) Investors; or (2) Clearing System 2. FSP incorporating a company or otherwise organizing the securitization structure (including providing the registered office) (1) Sponsor; and (2) Where the SPV is a trust, the trustees; or (3) Where the SPV is a limited partnership, the general partner; or (4) Where the SPV is a company, the directors (see the section on Company Formation and Management) Page 226 of 245 3. FSP issuing and administering subscriptions/redemptions. (1) The SPV; and (2) The investors or Clearing System 4. Share trustee (1) The SPV; and (2) The beneficiary of any trust holding the shares of the SPV 5. Note trustee/Indenture trustee (1) The SPV; and (2) Investors or Clearing System 6. Placement agent/arranger (1) Investors 7. Clearing system (1) The SPV; (2) Its participants and account holders; and (3) Placement agent/arranger F. CUSTOMER DUE DILIGENCE (refer also to Section 4 of Part II) When must the identity be verified? 1. The AMLRs provide that there should be procedures in place which require that, as soon as reasonably practicable after contact is first made with an applicant for business, either satisfactory evidence of the applicant s identity should be obtained, or that steps are taken

which will produce satisfactory evidence of identity. 2. The time span in which satisfactory evidence should be obtained depends on the particular circumstances and the practicalities of obtaining evidence before commitments are entered into between parties and before money is transferred. 3. Customer risk assessments relating to particular investors should take place as an investor is on-boarded and should be reviewed and changed, if necessary, during periodic reviews of the investors as discussed in the Ongoing Monitoring section below. Customers and investors that are risk classified as low (or the equivalent) may be subject to simplified CDD procedures. However, SPVs must be aware that their risk classification of a Customer/Investor being low-risk is only valid if the finding is consistent with the findings of the Authority, or the of national risk assessment, whichever is more recently issued. Customers and investors that are risk classified as medium risk (or the equivalent) may be subject to at least normal CDD procedures. Customers and investors risk classified as high risk must be subject to enhanced CDD procedures. 4. If, after having conducted a risk assessment and ascertained a lower risk of ML/TF/PF, verification procedures for a counterparty have not been completed prior to the establishment of the business relationship, the SPV may complete the verification before the payment of any proceeds or distributions, including dividends. Payments should be made only to the investor and not to a third party and only when the outstanding due diligence documentation has been verified.Ongoing Monitoring Page 227 of 245 5. Ongoing monitoring should take place to ensure that documents, data, or information collected during the various due diligence procedures on counterparties are kept up-to-date and relevant. SPVs should ensure that the counterparties are periodically screened against the vigilance databases/sanctions lists. Periodic reviews should also be conducted on the counterparties and the frequency of periodic review should be based on their risk rating. Due to the nature of the activities of an SPV, ongoing monitoring will likely be focused primarily on relationships rather than transactions and as such, will likely be performed by persons rather than through the use of electronic systems. For further guidance on on-going monitoring, reference should be made to section 16 of Part II of these Guidance Notes. G. PARTICULAR ISSUES ON VERIFICATION OF IDENTITY OF INVESTORS One-off transactions 1. For the purpose of the Guidance Notes, a subscription to an SPV should not be treated as a one-off transaction (see section 4 of Part II of the Guidance Notes). Depository, Custody and Nominee Arrangements 2. In some cases, depositories, custodians or nominees will be another intermediary between the SPV, the placement agent and the beneficial owner of the securities issued by the SPV. In addition, the ownership of securities may be recorded in book-entry or uncertificated form. In that case, nominee investors, most often the placement agents, are the investor of record for the clearing house but in reality, they hold the security for the benefit of underlying ultimate beneficial investors. In certain cases, the SPV may be able to rely on the due diligence carried out by the nominee investor (as per Section 5, subsection E of these Guidance Notes). H. INTERNAL CONTROLS (refer also to sections 9, 10 and 4 of Part II) 1. FSPs must have policies and procedures in place as required by the AMLRs. These shall include policies and procedures to - (1) identify and report suspicious activity; (2) monitor and ensure internal compliance with laws relating to AML/CFT/CPF; and (3) test the efficacy and efficiency of their AML/CFT/CPF systems and update such systems (the "Procedures"), if necessary, to comply with their AML/CFT/CPF obligations. 2. Both SPVs and their service providers are subject to the AMLRs and each has separate obligations to maintain and implement such Procedures in respect of their carrying on

relevant financial business. The ultimate responsibility for maintaining and implementing satisfactory Procedures remains with each FSP.An SPV can meet its obligations in relation to the Procedures by either- (1) implementing their Procedures directly; (2) delegating the performance of the Procedures to a person; or (3) relying on a person to perform the Procedures. 3. It should be noted that, as they carry on relevant financial business, all SPVs must designate an AMLCO, MLRO and DMLRO 1 . Following this designation, the designated person may delegate the performance of this function to another Page 228 of 245 FSP 2 or rely on any other FSP to perform this function. However, regardless of such reliance or delegation, the SPV remains ultimately responsible for its compliance with AML/CFT/CPF obligations. Refer to Part II, Section 2, Subsection C para 8-14 of the Guidance Notes for further guidance on reliance/delegation of AML/CFT/CPF functions. 4. Where an SPV chooses to delegate the performance of its obligations to another person, the SPV should adopt the principles set out in Part II, Section 10 C. (Outsourcing). Similarly, where an SPV chooses to rely on a person for the performance of its obligations, the SPV should adopt the principles set out in paragraphs 8 through 14 under Part II, Section 2, Subsection C of the Guidance Notes. 5. The directors, trustee or general partner of the SPV should document, either as a board resolution or otherwise, the manner in which the SPV has met the obligations described above. I. RECORD KEEPING (refer also to Sections 8 and 11 of Part II) What specific records should be kept and where? 1. Refer to Sections 54 and 55 of the Companies Act (as amended). 2. There are instances when it may be impractical for the SPV itself to maintain records. However, in such instances, the SPV must ensure that all appropriate records are maintained (as required by the AMLRs) on its behalf. When may a successor FSP rely on the customer verification evidence obtained by its predecessor? 3. Where a successor firm is appointed to perform an FSP function for an existing SPV, the successor must ensure that the necessary due diligence has been performed prior to performing the function. 4. It may be possible to rely upon the evidence of identity obtained by a predecessor FSP provided that the original files, or certified copies of the original files, are transferred to the FSP and the successor firm has assessed the quality of the evidence on investor identity as being adequate. 5. Where insufficient evidence exists or a long time has passed since the due diligence was last updated, it may be appropriate to supplement it with additional evidence to meet the standards required by these Guidance Notes. 6. At no time would it be appropriate to rely upon an eligible introducer letter as a method for the customer verification evidence obtained by its predecessor. J. MONEY LAUNDERING/TERRORIST FINANCING/PROLIFERATION FINANCING WARNING SIGNS 1. In addition to the risk factors in Section 3 of Part II and the warning signs set out in Appendix D of the Guidance Notes, risk factors and ML/TF/PF warning Page 229 of 245 signs to which SPVs and parties to securitizations must have regard to in order to satisfactorily assess the ML/FT/PF risks pertaining to a particular business relationship or transaction include: (1) Assets that are the object of the securitization have been the object of legal measures; (2) The present or previous owner of the assets has criminal convictions; (3) Assets involved in the securitization are difficult to quantify or are in locations difficult to access; (4) Assets exhibit legal inconsistencies with respect to their ownership, possession or tenure, or are overvalued or whose characteristics are not in keeping with the sector; (5) When an investor is more concerned about the subscription and distribution terms of the notes than with other information related to the investment; (6) sudden and unexplained subscriptions and transfers; (7) requests to pay distributions to a third

(unrelated) party; and (8) a client or investor that exhibits unusual concern with compliance with AML/CFT/CPF reporting requirements or other AML/CFT/CPF policies and procedures. Page 230 of 245 GLOSSARY AND ACRONYMS ACC Anti-Corruption Commission 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 (2020 Revision) AMLSG means The Anti-Money Laundering Steering Group AMLSG List means Anti-Money Laundering Steering Group List 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 Banks mean retail and non-retail banks Banking Business means the business of receiving (other than from a bank or trust company) and holding on current, savings, deposit or other similar account money which is repayable by cheque or order and may be invested by way of advances to customers or otherwise, as prescribed in Section 2 of the Banks and Trust Companies Law. BTCA Banks Trust and Companies Act (2021 Revision) Board means the Board of Directors CDD means Customer Due Diligence CIDB means the Cayman Islands Development Bank Companies Management Act means the Companies Management Act (2021 Revision) CSPs means Company Management and Formation Services Professionals Designated person means a person, including any subsidiary or other entity owned or controlled by that person, to whom Security Council of the United Nations anti- proliferation financing measures relates. DMLRO means Deputy Money Laundering Reporting Officer EDD means Enhanced Customer Due Diligence Page 231 of 245 EI means Eligible Introducer Eligible Introducer means a person that introduces applicants for business to an FSP and who satisfies the conditions set out in Regulation 25 of the ALMRs i.e. a person who falls within one of the categories under Regulation 22(d) and who provides a written assurance pursuant to Regulation 24(2)(b) EU means the European Union FATF means Financial Action Task Force FATF Recommendations or the 40 Recommendations means the 40 Recommendations set out in the Financial Action Task Force ("FATF") document International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation', adopted by the FATF in February 2012. FCU means the (Cayman Islands) Financial Crimes Unit FIU means the (Cayman Islands) Financial Intelligence Unit FRA means the (Cayman Islands) Financial Reporting Authority FSPs means Financial Service Providers ICOs means initial coin offerings ILS means Insurance Linked Securities IOSCO means International Organization of Securities Commissions IRS means the Internal Revenue Services KYC means Know-Your-Customer MA means the Cayman Monetary Regulatory Authority International ML means Money Laundering MLRs means the Money Laundering Regulations MLRO means Money Laundering Reporting Officer MRP means money transmission/remittance provider MSB means Money Services Business MSA means the Money Services Act (2020 Revision) MVTS means Money Value Transfer Services NPOs means non-profit organisations Page 232 of 245 NRA means the (Cayman Islands) National Risk Assessment OFAC means the Office of the Foreign Assets Control OGCISS means the Offshore Group of Collective Investment Scheme Supervisors OOIC means the Overseas Orders in Council OFSI means UK s Office of Financial Sanctions Implementation OSP means outsourced service provider PTCR means Private Trust

Companies Regulations PEPs means politically exposed persons PF means Proliferation Financing PFA means the Proliferation Financing Act (Revision 2020) PFPA means the Proliferation Financing (Prohibition) Act (2017 Revision) PoCA Proceeds of Crime Act (2020 Revision) Procedures refer to the AML/CFT Regulations, Guidance Notes PSP means Payment Service Provider PTA means Payable-Through Accounts PTCs means Private Trust Companies RBA means Risk Based Approach RCIPS means the Royal Cayman Islands Police Service Relevant Financial Business has the meaning assigned in the Proceeds of Crime Act (2020 Revision) SAR means Suspicious Activity Report SC means Sanctions Coordinator SDD means Simplified Customer Due Diligence SIBA means the Securities Investment Business Act (2020 Revision) SIBs means Securities Investment Businesses SRB means self-regulatory bodies Page 233 of 245 Source of Funds refers to the origin of the particular funds or assets (for example an immediate source from which property has derived e.g. from a bank account in the name of the applicant for business or a third party) that will be used for the purposes of the business relationship or transaction (e.g. the amount being invested, deposited or remitted) Source of wealth refers to the origin of the entire body of wealth (i.e. total assets). This information will usually give an indication as to the volume of wealth the customer would be expected to have, and a picture of how the customer (applicant/owner/PEP) acquired such wealth. STAR means Special Trust Alternative Regime 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 Acts. TF means terrorist financing TFS means terrorist financing sanctions The Act refers to the Proceeds of Crime Act (2020 Revision) TA means the Terrorism Act (2018 Revision) UK means the United Kingdom UN means United Nations UNSCRs means the UN Security Council US means the United States of America WMD means weapons of mass destruction VAs means virtual assets VASPs means a natural or legal person which falls within the scope of the definition of virtual asset service by virtue of the activities it carries out is referred to in this Guidance Notes Page 234 of 245 APPENDIX A ELIGIBLE INTRODUCER'S (ASSURANCE) FORM Name of Eligible Introducer Eligible Introducers Contact details Address: : 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 a country assessed by the FSP as having a low degree of risk of ML/TF 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 assessed by the FSP as having a low degree of risk of ML/TF. 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. Page 235 of 245 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: : Telephone: Page 236 of 245 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 From: (Stamp of FSP Sending which request is sent) the letter) Dear Sirs, REQUEST FOR VERIFICATION OF CUSTOMER IDENTITY In accordance with the Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands 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. Page 237 of 245 APPENDIX C FLOW CHART WHERE APPLICANT IS INTRODUCED BY EI Page 238 of 245 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. Interaccounty 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. Page 239 of 245 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, withdrawal 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. Page 240 of 245 (3) Use of multiple personal and business accounts or the accounts of NPOs 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 Page 241 of 245 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: (1) settlement of purchases or sales involves (or appears to involve) third parties other than the investor; (2) bearer shares (if available) are requested; (3) (bearer or unregistered securities/near-cash instruments are offered (4) settlement of purchases; (5) there is excessive switching; (6) there is early termination despite front-end loading or exit charges; (7) they become aware that the customer's holding has been pledged to secure a borrowing in order to gear up his investment activities; or (8) 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 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