British Virgin Islands Financial Services Commission

A MONEY SERVICES BUSINESS GUIDE

to the Prevention of Money Laundering & Terrorist Financing Activities in and from within the Virgin Islands

Issued Pursuant to Section 41A of the Financial Services Commission Act, 2001

Approved by the Board of Commissioners.....25th October, 2016
Issued by the Financial Services Commission .....16th November, 2016
Published .....17th November, 2016
Coming into Force .....19th December, 2016

TABLE OF CONTENTS

1. Introduction 4
2. Definitions 5
3. What is Money Laundering? 5
4. What is Terrorist Financing? 6
5. Anti-money Laundering (AML) 7
6. Countering the Financing of Terrorism (CFT) 7
7. Proliferation Financing 7
8. Financial Inclusion and AML/CFT 8
9. Money Services Business 9
10. Licensing of MSBs 9
11. Duty of Vigilance 9
    - Consequences of Failure 10
12. A Risk-based Approach 10
13. Customer Due Diligence (CDD)/Enhanced Customer Due Diligence (ECDD) 11
    - Applying CDD Measures 12
    - Simplified CDD Measures 12
    - Enhanced CDD Measures 13
    - Ongoing CDD and Transaction Monitoring 13
14. Internal Controls 14
    - Product/Service Risk 15
    - Transaction Risk 15
    - Customer Risk 16
    - Geographic/Country Risk 17
    - Agent/Distribution Risk 18
    - Senior Management Role in Risk Management 18
    - Ensuring Compliance 19
15. Reporting a Suspicious Activity 20
16. Indicators of Suspicious Activity 20
    - New customers and occasional or 'one-off' transactions 20
    - Regular and established customers 21
    - Examples where customer identification issues have potential to indicate suspicious activity 21

- Examples of activity that might suggest there could be potential terrorist activity 21

17. Record Keeping 21

18. Staffing 22

- Vetting and Recruitment 22
- Employee Training 22

19. Obligations in Relation to Agents of MSBs 23

- Training and Awareness of Agents 24
- Monitoring of Agents 24

20. Combatting Money Laundering and Terrorist Financing 24

- Information Exchange 24

21. Meeting International Standards 25

- Financial Action Task Force (FATF) 25
- Caribbean Financial Action Task Force (CFATF) 26

22. Relevant Legislation 26

- Financing and Money Services Act, 2009 (FSMA) 26
- Proceeds of Criminal Conduct Act, 1997 (PCCA) 26
- Anti-money Laundering Regulations, 2008 (AMLR) 27
- Anti-money Laundering and Terrorist Financing Code of Practice, 2008 (AMLTF Code of Practice) 28
- The Terrorism (United Nations Measures) (Overseas Territories) Order 2001 (TUNMOTO) 28
- Anti-Terrorism (Financial and Other Measures) (Overseas Territories) Order 2002 (ATFOMOTO) 28

23. Conclusion 28

1. Introduction

Money services business (MSB) in the Virgin Islands is regulated by the Financial Services Commission ("the Commission") under the Financing and Money Services Act, 2009. Entities which wish to provide MSB must be duly licensed by the Commission and must adhere to all regulatory legislation, including the Anti-money Laundering Regulations, 2008 and the Anti-money Laundering and Terrorist Financing Code of Practice, 2008.

MSBs provide an important service within the financial services sector by providing an avenue for the transfer of remittances by persons who may not have access, or are unable to meet the criteria, to use traditional banking methods or who simply find it to be a more efficient or cheaper medium for transacting business. However, the use of such services creates risk of misuse by persons who may attempt to exploit these services to launder ill-gotten proceeds of crime.

The purpose of these Guidelines, therefore, is to ensure protection of MSBs and the wider financial services industry, and help in the efforts against money laundering (ML), terrorist financing (TF), and other financial crime. The Guidelines aim to provide MSBs with basic guidance on understanding what is ML and TF, and emphasizing the importance of AML/CFT procedures in the fight against ML/TF. They outline the licensing requirements of MSBs, the need to execute their duties with vigilance and the consequences of failing to do so.

These Guidelines also explain the responsibilities of MSBs in relation to conducting proper customer due diligence (CDD) on their customers, how these measures should be applied and under what circumstances simplified or enhanced CDD may be applied. Further, the Guidelines also outline the importance of establishing proper internal control procedures and identifies and provides examples of the various risk factors that MSBs should be aware of when entering into business relationships or executing one-off transactions.

It is important that MSBs are able to identify suspicious activity as well as understand their obligation to report such activity to the Financial Investigation Agency. The Guidelines provide examples of indicators of suspicious activity to make it easier for MSBs to identify such behaviour, and explain the role and responsibility of the money laundering reporting officer (MLRO) in ensuring that such activity is properly documented and reported.

Record keeping is an important aspect of any AML/CFT regime. Maintenance of proper records is extremely important to MSBs, as accurate record keeping enables MSBs to show their compliance with the AML/CFT laws and guidelines. Furthermore, such record keeping may prove crucial if there is an investigation into a customer or suspicious business transaction. The Guidelines, therefore, explain the types of records that should be kept and for what period, and the formats in which records may be maintained.

As a cash intensive business, it is important that the persons employed by, or appointed as agents of, MSBs are of sound character and integrity. The Guidelines outline what MSBs should look for in potential staff during the vetting and recruitment stages of employment. They further outline the obligation for MSBs to provide continual relevant training for both staff and agents and to ensure that proper testing is conducted on staff and agents alike. MSBs are also required to monitor the activities of their agents to assess and address any potential systemic risks which may arise as a consequence of inadequate training, lax internal control procedures, or poor individual judgment or performance.

Finally, the Guidelines take a look at the regional and international standards setting bodies that promote the effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing, proliferation financing and other related threats to the integrity of the international financial system, and outlines the legislation relevant to all MSBs.

2. Definitions

"*business relationship*" is a relationship in which an entity engages in business with another party on a frequent or habitual basis;

"*key staff*" is an employee who deals with customers or clients and their transactions;

"MLRO" means money laundering reporting officer – this is a person appointed to ensure compliance by the MSB with all AML/CFT legislation and internal reporting and compliance procedures, and to act as the liaison between the MSB and the Financial Investigation Agency on matters relating to suspicious activities;

"*one-off transaction*" is a transaction carried out other than in the course of an established business relationship.

NOTE: *The Anti-money Laundering Regulations, 2008 and Anti-money Laundering and Terrorist Financing Code of Practice, 2008 provide definitions to other terms used in these Guidelines and Users of these Guidelines should refer to both the Regulations and the Code of Practice in adhering to and applying the provisions of these Guidelines.*

3. What is Money Laundering?

Money laundering is the generic term used to describe the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear as if they are derived from a legitimate source.

Money laundering activities typically aim to generate and maximize income for as little cash outflow as possible, with no regard for the probable negative economic and social implications. These activities also include income-generating actions that aim to raise funds for separate illegal activities.

There are three stages of money laundering, which may occur in sequence but often overlap.

Placement is the first stage of money laundering and constitutes the introduction of criminal proceeds into the financial system. These proceeds usually take the form of cash. Placement may be achieved by a wide variety of means according to the opportunity afforded to, and the ingenuity of, the criminal, his or her advisers and their network. Typically, it may include:

- placing cash on deposit at a bank (often intermingled with a legitimate credit to obscure the audit trail), thus converting cash into a readily recoverable debt;
- physically moving cash between jurisdictions;
- wiring cash to various locations within and between jurisdictions;
- making loans in cash to businesses which seem to be legitimate or are connected with legitimate businesses, thus also converting cash into debt; and

- purchasing high-value goods (such as vehicles and furniture) for personal use or expensive presents (such as jewellery) to reward existing or potential colleagues.

Layering is the second stage of money laundering and constitutes the separation of criminal proceeds from their source. This is carried out by creating layers of transactions designed to disguise the audit trail and provide the appearance of legitimacy. Again, this may be achieved by a wide variety of means and may typically include:

- rapid switches of funds between banks and/or jurisdictions;
- use of cash deposits as collateral security in support of legitimate transactions;
- switching cash through a network of legitimate businesses and companies not engaged in any known business activity across several jurisdictions; and
- resale of goods/assets.

Integration is the final stage in money laundering in which criminal proceeds are treated as legitimate. If layering has succeeded, integration places the criminal proceeds back into the economy in such a way that they appear to be legitimate funds or assets.

The processes by which criminally derived property may be laundered are extensive. Though criminal money may be successfully laundered without the assistance of any financial sectors, the reality is that hundreds of billions of dollars of criminally derived money is laundered through financial institutions annually. The nature of the services and products offered by the financial services industry means that it is vulnerable to abuse by money launderers and hence the need for vigilance against abuse and misuse of those services and products.

Laws (comprising Acts of the House of Assembly and subsidiary legislation comprised in Regulations and Orders) and guidelines have been put in place to facilitate a better understanding, and the detection and prevention, of money laundering. These laws and guidelines target activities that may include market manipulation, improper trading of goods, one-off transactions, corruption of public funds, and evasion of tax, and require financial institutions to have proper internal procedures in place to allow them to know their customers, maintain proper records and identify and report suspicious activities. Such laws and guidelines are expected to be complied with by all financial institutions, including MSBs.

4. What is Terrorist Financing?

Terrorist financing is the activity of providing or collecting funds directly or indirectly, with the aim or with the knowledge that the funds are to be used to carry out terrorist activity or used by a terrorist or terrorist organization. Such activities may involve funds raised from legitimate sources, such as personal donations and profits from businesses and charitable organizations, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping, extortion and other criminal activity.

Terrorists use techniques like those of money launderers to evade authorities' attention and to protect the identity of their sponsors and of the ultimate beneficiaries of the funds. However, financial transactions associated with terrorist financing tend to be in smaller amounts than is the case with money laundering, which makes MSBs more vulnerable to such activities given the propensity for persons to engage MSBs rather than banks for the transfer of these smaller sums of

money, and the fact that MSBs' fees tend to be lesser compared to those of other financial institutions (such as banks). When terrorists raise funds from legitimate sources, the detection and tracking of these funds becomes more difficult. It is therefore important to exercise vigilance at all times, but especially with respect to business relationships and transactions.

5. Anti-Money Laundering (AML)

Anti-money laundering (AML) refers to a set of procedures, laws and guidelines designed to stop the practice of generating income through illegal actions. In most cases, money launderers hide their actions through a series of steps that make it look like money that came from illegal or unethical sources was earned legitimately.

The implications of AML laws are extremely far-reaching. For example, the Anti-money Laundering Regulations, 2008 (AMLR) require financial institutions, when entering into business relationships or executing one-off transactions, and throughout their relationship with customers, to complete due-diligence procedures to ensure that these institutions are not aiding in money-laundering activities. The onus to perform these procedures is on the institutions (MSBs for example), not on the customers or the supervisory authority. The success of these institutions in combatting these activities has wider implications for the Territory, as the compliance, or lack thereof, with these requirements directly impacts the Virgin Islands' ability to meet its international AML/CFT obligations, which itself could have a negative economic impact on the Territory.

6. Countering the Financing of Terrorism (CFT)

Like AML, countering the financing of terrorism (CFT) refers to a set of procedures, laws and guidelines designed to stop persons from generating income with the ultimate aim of making such income (whether wholly or partially) available for use in activities related to terrorism. Quite often persons involved in terrorist financing derive the income through legitimate sources (for example through fund raising for charitable purposes) and apply the income or part thereof to fund persons (including organisations) knowing that such persons will use the income to advance terrorist activities. It is also possible for one to unknowingly contribute funds which end up being applied to terrorist activities. That would normally be the case where one makes a contribution towards a charitable purpose (such as contributing to a fund raising exercise to build a school in a foreign country).

It is therefore important that financial institutions (including MSBs) engage in active due diligence by not only collecting relevant data from their clients/customers, but also taking the necessary steps to ensure that they know such clients/customers and their source of income.

7. Proliferation Financing (PF)

Proliferation financing (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 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[11]. In more simple terms, proliferation financing facilitates the development of goods or materials for illegal or terrorist activities. The financing of proliferation can pose a significant threat to global stability whereby funds provided facilitate the development of weapons that may be used with devastating consequences to human society. Considering the possibilities of weapons of mass destruction getting into the hands of terrorists, for example, the FATF standards require countries to take adequate and effective measures to prevent and identify any act tending towards the financing and development of such weapons. The mechanics used to advance or facilitate terrorist financing are essentially the same as those for proliferation financing. Accordingly, a reference in these Guidelines to CFT and/or TF should be read to include proliferation financing.

8. Financial Inclusion and AML/CFT

Financial inclusion is about 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 regulated financial sector at an affordable cost in a fair and transparent manner. It is also about making a broader range of financial services available to individuals who currently may have access to only basic financial products[2].

MSBs play an important role in supporting financial inclusion as they are used for transferring remittances by persons who may not have access, or are unable to meet the criteria, to use traditional banking methods. MSBs, therefore, provide an important financial service for people in many developing countries and are a powerful enabler of financial inclusion. For AML/CFT purposes, however, it is important that financial products and services, including those provided by MSBs, are provided through financial institutions that are subject to proper supervision and regulation. Such regulation is aimed at potentially reducing the overall ML/TF risk in the financial system by bringing these customers into a regulated environment.

For some, MSBs may be their first or only interaction with the financial sector. It is important, therefore, that established AML/CFT policies and supervisory frameworks for MSBs are well-designed and function in such a way as to foster greater financial inclusion. A risk-based approach (RBA) to the provision of money services business may help foster financial inclusion, especially in the case of low-income individuals who experience difficulties in accessing the mainstream financial system. Conversely, an indiscriminate termination or restriction of business relationships to MSBs without proper risk assessment and mitigation measures could potentially increase the level of financial exclusion. Such action could divert customers towards riskier services and channels that are not properly regulated, or has the potential to push the business underground, taking it outside the scope of any regulatory oversight.

[1] FATF report *Combating Proliferation Financing: A Status Report on Policy Development and Consultation*2010
[2] Pg 17 FATF Guidance for a Risk-based Approach for Money or Value Transfer Services

9. Money Services Business (MSB)

Money Services Business (MSB) refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value, and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MSB belongs.

Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions and are described using a variety of specific terms, including *hawala*, *hundi*, and *fei-chen*.

The Financing and Money Services Act, 2009 ("the Act"), defines Money Service Business to describe the following activities:

(a) Money transmission services;

(b) Cheque cashing services;

(c) Currency exchange services;

(d) The issuance, sale or redemption of money orders or traveller's cheques; or

(e) Operating as an agent or franchise holder of a person carrying on any business specified in sub-paragraphs (a) to (d) above.

10. Licensing of MSBs

MSBs can only be conducted in, or from within, the Virgin Islands, by an entity established as a BVI Business Company (BVIBC) or a foreign company, and must be duly licensed by the Commission. An MSB is licensed by the Commission after satisfying the requirements of the Act.

In accordance with the Act, where a BVIBC carries on, or holds itself out as carrying on, money services business outside the Virgin Islands, it is considered to be carrying on, or holding itself out as carrying on money services business from within the VI, and is therefore subject to all licensing requirements.

11. Duty of Vigilance

MSBs can perform their duty of vigilance by having in place systems which enable them to perform the following:

- determine (or receive confirmation of) the true identity of customers requesting their services;
- recognize and report suspicious transactions to the Financial Investigation Agency;
- keep records for the prescribed period of time;
- establish internal controls that provide appropriate policies, processes and procedures for forestalling and preventing money laundering and terrorist financing; and

- train *key staff*.

All employees and, in particular, all *key staff,* are at risk of being or becoming involved in criminal activity if they are negligent in their vigilance. Vigilance systems should enable *key staff* to react effectively to suspicious occasions and circumstances by reporting them to the relevant personnel in-house. Every MSB is required to have and appoint an MLRO who should receive suspicions of money laundering activity and then report such activity to the Financial Investigation Agency.

Employees should be aware that they can face criminal prosecution if they commit any of the offences under the Proceeds of Criminal Conduct Act (see pages 10 and 11 below where these offences are specifically identified). MSBs and any director, member, manager or other senior officer of an MSB may also become criminally liable for prosecution if they commit any of those offences.

Consequences of Failure

The **first consequence** of failure in vigilance is likely to be commercial. MSBs that, however unwittingly, become involved in money laundering risk the loss of their good market name and position and the incurring of nonproductive costs and expenses. This may also affect the business relationships they have with other financial institutions, such as banks.

The **second consequence** may be to raise issues of supervision and fit and proper standing should an MSB be found to be involved in money laundering related activities.

The **third consequence** is the risk of criminal prosecution of the institution and its senior officers for the commission of an offence under the Proceeds of Criminal Conduct Act.

For the individual employee, it should be self-evident that the consequences of failure are not dissimilar to those applicable to the MSB itself. The employee's good name within the industry is likely to suffer and he or she may face the risk of prosecution for the commission of an offence under the Proceeds of Criminal Conduct Act.

It should be noted that certain offences under the Proceeds of Criminal Conduct Act are concerned with assistance given to the criminal. There are two necessary aspects to such criminal assistance:

- the provision of opportunity to obtain, conceal, retain or invest criminal proceeds; and
- the knowledge or suspicion (actual or, in some cases, imputed) of the person assisting where criminal proceeds are involved.

The determination of involvement is avoidable on proof that knowledge or suspicion was reported without delay in accordance with the vigilance systems of the institution and pursuant to the reporting safeguards provided under the Proceeds of Criminal Conduct Act.

12. A Risk-based Approach (RBA)

The RBA to AML/CFT means that MSBs are expected to identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively and efficiently.[3]

[3] Pg 14 FATF Guidance for a Risk-based Approach for Money or Value Transfer Services

In assessing ML/TF risks, MSBs must be able to analyse and understand how the ML/TF risks they identify affect them, and take appropriate measures to mitigate and manage those risks. MSBs should maintain an understanding of the overall ML/TF sector risk, as well as risk specific to their products and services, customer base, and the effectiveness of the internal control mechanisms that they have in place.

This risk assessment will then provide the basis for the risk-based application of AML/CFT measures, and should enable an MSB to understand how, and to what extent, it is vulnerable to ML/TF. Risk assessments should be proportionate to:

- the nature, size and complexity of the business, taking into account agent relationships and the range of financial products and services being offered;
- the type of products and services offered, and the extent to which the products and services offered are consistently below a given threshold;
- customers' characteristics based on developed risk profiles, including the level of customer diversity across different geographical locations;
- the conditions of the proposed transactions; and
- the distribution channels used by the MSB.

AML/CFT risk assessments also help MSBs identify the nature and extent of AML/CFT resources necessary to mitigate and manage that risk, and should be properly documented, regularly updated and communicated to relevant personnel.

13. Customer Due Diligence (CDD)/Enhanced Customer Due Diligence (ECDD)

MSBs are considered to have business relationships with persons who execute transactions on an ongoing basis. In such circumstances, MSBs are required to carry out CDD to verify the identities of such individuals against any information previously collected and held as a result of a prior transaction. Similar identity verification is required in the case of one-off transactions.

In addition to carrying out CDD measures when one sets up a business relationship with a customer or carries out an occasional transaction, CDD should also be carried out if the MSB suspects money laundering or terrorist financing; determines that the relationship presents a higher than normal risk; or has any doubt about any information provided by the customer for identification or verification purposes. In essence, CDD relates to forestalling and preventing the activity of money laundering.

Performing CDD means taking steps to identify a customer and verify that the customer is who he or she says he or she is. In practice this means obtaining a customer's:

- Name;
- Photograph on an official document which confirms identity; and
- Residential address or date of birth.

Where a person is conducting a transaction on behalf of a company, the following information should also be collected in addition to the information listed above:

- Name of company;

- Address of company;
- Ultimate beneficial owner of the company – that is, the natural person(s) that owns the company; and
- Controllers of the company (such as the director(s) of the company).

To effectively carry out the act of CDD, an MSB must:

- have systems to identify those persons who cannot produce standard documents;
- take account of the greater potential for money laundering in higher risk cases, specifically in respect of politically exposed persons[4];
- not deal with certain persons or entities if due diligence cannot be executed, or the results are not satisfactory ; and
- have a system for keeping customer information up-to-date.

Applying CDD Measures

The extent to which CDD measures are applied may vary, to the extent permitted or required by law, based on the ML/TF risk identified or associated with the business relationship or one-off transaction. This means that the amount or type of information obtained, or the extent to which this information is verified, must be increased where the risk associated with the business relationship or transaction is higher. It may also be simplified where the risk associated with the business relationship or transaction is lower. It should, however, be noted that applying and adopting simplified CDD measures is not acceptable whenever there is a suspicion of ML or TF, or where specific higher-risk scenarios apply.

Simplified CDD Measures

Where an MSB determines that a customer poses a significantly low risk, simplified CDD measures may be applied. In cases where an MSB determines that simplified CDD measures may be applied, the following actions may be taken:

- fewer elements of customer identification data may be obtained (production of one form of ID instead of two, for example);
- less robust identity verification procedures may be employed;
- collection of specific information or the carrying out of specific measures to understand the purpose and intended nature of the business relationship may not be required (the purpose and nature of the business relationship may be inferred from the type of transactions or business relationship established);
- the identity of the customer and the beneficial owner(s) may be verified after the establishment of the business relationship;
- in the case of an existing business relationship, the frequency of customer identification updates may be reduced; and
- the degree and extent of on-going monitoring and scrutiny of transactions may be reduced, based on a reasonable monetary threshold.

[4] Politically exposed persons (PEPs) are persons (foreign and domestic) who are, or have been, entrusted with prominent public functions (Heads of state or government, politicians, senior government officials, judicial or military officials, senior executives of statutory bodies, senior political party officials) or who hold prominent functions within an international organization (senior managers and members of the Board).

Enhanced CDD Measures (ECDD)

ECDD refers to the additional steps an entity is required to undertake to limit or manage the risk posed by a customer who is considered to pose a high risk. This will be the case in relation, for instance, to a politically exposed person, a person from a jurisdiction that is considered to pose a geographic risk or a person who trades in products that are of a complex nature. In cases where an MSB determines that ECDD measures may be applied, the following actions may be taken:

- additional identifying information from a wider variety or more robust sources should be obtained and corroborated and the information used to inform the individual customer's risk profile;
- additional searches (e.g. verifiable adverse internet searches) should be carried out to better inform the individual customer's risk profile;
- where appropriate, further verification procedures should be undertaken on the customer or beneficial owner to better understand the risk that the customer or beneficial owner may pose to the MSB;
- the source of funds and wealth involved in the transaction or business relationship should be verified to satisfy the MSB that they do not constitute the proceeds of crime;
- the information provided with regard to the destination of funds and the reasons for the transaction should be evaluated; and
- additional information about the purpose and intended nature of the transaction or the business relationship should be sought and verified.

Where an MSB is unable to verify the identity of an individual, it should not enter into a business relationship or execute a one-off transaction with that individual. If the business relationship already exists, the MSB should terminate the business relationship. In all circumstances the MSB should consider filing a suspicious transaction report in relation to the customer or individual.

Ongoing CDD and Transaction Monitoring

Once a business relationship is established, the MSB has an obligation to ensure that CDD measures are carried out on an ongoing basis. Such measures are required to determine whether executed transactions are consistent with the MSB's information about the customer and the nature and purpose of the business relationship, wherever appropriate. These ongoing CDD measures should allow MSBs to identify changes in customer profiles (for example, their behaviour, use of products and the amount of money involved), and to keep them up to date, which may require the application of enhanced CDD measures.

An essential component in identifying transactions that are potentially suspicious is transaction monitoring. Transactions that do not fit the behaviour expected from a customer's profile, or that deviate from the usual pattern of transactions, may be potentially suspicious. Monitoring should, therefore, be carried out on a continuous basis; however, it may also be triggered by specific transactions.

Transaction monitoring systems may be manual or automated based on the volume of transactions processed by an MSB on a regular basis. However, where automated systems are used, MSBs should understand their operating rules, verify their integrity on a regular basis and check that they take account of the identified ML/TF risks.

The level of transaction monitoring should be based on an MSB's institutional risk assessment and individual customer risk profiles, with enhanced monitoring being executed in higher risk situations.

The adequacy of an MSB's monitoring system, and the criteria used to determine the level of monitoring to be implemented, should be reviewed regularly to ensure that they are in line with the MSB's AML/CFT risk programme.

Transactions performed or initiated by agents must also be subject to regular monitoring under the same conditions as transactions of the MSB itself. Such monitoring should be conducted under the MSB's control by the MSB itself, or in collaboration with the agent, based on appropriate agreement.

MSBs should create monetary or other thresholds, based on a risk-based approach, 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 established risk levels. Criteria and parameters used for customer segmentation and for the allocation of a risk level for each customer group should be transparent and clearly documented. Additionally, MSBs should properly document, retain and communicate to the relevant personnel the results of their monitoring, as well as any queries raised and resolved.

14. Internal Controls

Internal controls are established to ensure entities put appropriate policies, processes and procedures in place to forestall and prevent money laundering and terrorist financing.

MSBs are required to develop internal control systems that will enable the MSBs to effectively assess the risk of their business relationships and the transactions they execute on a daily basis.

Effective internal control measures should allow MSBs to perform a risk assessment of their business relationships or one-off transactions and allow for the management and mitigation of such risk. Established internal controls should be appropriate given the nature of the business relationship or one-off transaction and should ensure compliance with the AMLR and the AMLTF Code of Practice, etc.

Section 11(3) of the AMLTF Code of Practice outlines the matters that should be included in an MSB's internal controls. These matters include (but are not limited to):[5]

- focusing on operations, such as products, services, customers or geographical locations that are more vulnerable to abuse by money launderers and other criminals;
- designating a senior level person to be responsible for managing AML/CFT compliance;
- adequately meeting record keeping and reporting requirements;
- implementing risk-based CDD polices, processes and procedures;
- providing adequate and periodic training for all key staff;
- providing adequate supervision of employees that handle currency transactions and monitor for suspicious activity; and
- providing mechanisms for timely identification of suspicious transactions and accurate filing of such reports.

In addition, processes should be developed to ensure that ML/TF risks can be managed before entering into, or maintaining, business relationships or offering services that are associated with

[5] For a complete list of the matters that should be included in an MSB's internal controls, see section 11 (3) of the AMLTFCOP.

excessive ML/TF risks, and that business relationships are not established when the ML/TF risks cannot be mitigated and managed.

ML/TF risks may be measured in various ways. Developing proper risk categories allows MSBs to ensure their customers are subject to proportionate controls and oversight. The most commonly used risk criteria are: product/service risk; transaction risk; customer risk; country/geographic risk; and agent/distribution risk. How an MSB assesses these risk categories (individually or in combination) as part of its overall risk mitigation strategy is dependent on its individual circumstances and may vary from one institution to another.

Product/Service Risk

This is the risk associated with the products or services offered by the MSB. MSBs should pay special attention to new or innovative products or services that it does not offer, but which make use of its services to deliver the product or service. A risk assessment under this category should take the following into account:

- Products or services that have a very high or no transaction limit;
- The global reach of the product or service offered;
- The complexity of the product or service offered;
- Products or services that permit the exchange of cash for a negotiable instrument, such as a stored value card or a money order; or
- Products or services that seek to provide anonymity or layers of opacity, or that can readily cross international borders, such as cash, online money transfers, stored value cards, money orders and international money transfers by mobile phone.

Transaction Risk

There are inherent risks associated with every transaction that may be executed by an MSB due to the sheer nature of the industry. The risk associated with each transaction may vary depending on whether the MSB is sending or receiving the transaction. An overall risk assessment should include a review of transactions as a whole and should include a consideration of the following factors:

a) Transactions sent or attempted:

- MSBs should be aware of a customer's behaviour at point of origination, particularly where:
  - Transactions appear to be structured in such a way as to attempt to break up amounts in order to stay under any applicable CDD threshold, thereby avoiding reporting or record keeping;
  - Customer attempts a transaction, but cancels the transaction once subjected to CDD monitoring to avoid reporting or other requirements;
  - Customer makes unusual inquiries, threatens or tries to convince staff to avoid reporting;
  - Customer offers a bribe or a tip, or is willing to pay unusual fees to have transactions executed;
  - Customer appears to have no familial relationship with the receiver and no explanation is forthcoming in relation to the purpose of the transfer;
  - Customer is unclear about the amount of money involved in the transaction;
  - Based on information provided by the customer when conducting the transaction or during subsequent contact the number or value of transactions appears inconsistent with the financial standing or occupation, or is outside the normal course of business of the customer;

- Transactions are unnecessarily complex and have no apparent business or lawful purpose;
- Customer sends money internationally and then expects to receive an equal incoming transfer or vice versa;
- Customer wires money to higher-risk jurisdiction;
- Customer is transferring money to claim lottery or prize winnings to someone he or she met only online, towards a credit card or loan fee, or for employment opportunity or mystery shopping opportunity. These are all indicators of potential consumer fraud.

- MSBs should be able to detect the following activity during monitoring (either during the point-of-sale interaction or back-end transaction monitoring):
  - Where a customer uses aliases, nominees or a variety of different addresses to execute transactions;
  - Transfers are being made to the same person from different individuals or to different persons from the same individual with no reasonable explanation;
  - Where there are unusually large aggregate transfers, or high volume or frequency of transactions with no logical or apparent reason;
  - Customers whose number of transfers to a jurisdiction is notably higher than what is to be expected considering overall customer base;
  - Customer transfers/receives funds from persons involved in criminal activities as per the information available.
- Contact information, such as address, telephone or e-mail is shared between a network of customers where such sharing is not normal or reasonably explicable.

b) Transactions received:

- MSBs should pay special attention:
  - To transactions that are not accompanied by the required originator or beneficiary information; or
  - When additional customer or transactional information has been requested but has not been received.
- Large number of transactions received at once or over a certain period of time which do not seem to match the recipient's usual past pattern.

Customer Risk

An MSB is expected to determine the potential risk that a customer poses within the context of its own internal control system, and the potential impact of any mitigating factors relating to that assessment. In assessing risks that may be associated with a customer, MSBs should take the following into account:

- Customers conducting their business relationship or transactions in unusual circumstances, such as:
  - Travelling unexplained distances to locations to conduct transactions;
  - Establishing groups of individuals to conduct transactions at single or multiple outlet locations or across multiple services;
  - Customers who own or operate a cash-based business that appears to be a front or shell company or, based on a review of transactions that seem inconsistent with financial standing or occupation, appear to be intermingling illicit and licit proceeds;
- Customers who are PEPs or family members or close associates of PEPs, and where the beneficial owner of a customer is a PEP;

- Non face-to-face customers, where doubts exist about the identity of such customers;
- Customers who give inconsistent information (e.g. provide different names);
- Where the nature of the relationship or transaction(s) makes it difficult to identify the beneficial owner of the funds due to the use of agents or associates to carry out the transaction, or where the customer is acting on behalf of a third party but not disclosing that information or is being controlled by someone else (his or her handler). For example, someone else speaks for the customer, but puts the transaction in his or her name, or the customer picks up a money transfer and immediately hands it to someone else;
- Customers that appear to know little or are reluctant to disclose details about the payee (address, contact information, etc.);
- Customers who offer false or fraudulent identification, whether evident from the document alone, from the document's lack of connection to the customer, or from the document's context with other documents (e.g. use of identification cards or documents in different names without reasonable explanation);
- Customers that are involved in transactions that have no apparent ties to the destination country and with no reasonable explanations;
- Customers who are known to the MSB as having been the subject of law enforcement sanctions (in relation to proceeds generating crimes);
- Customers whose transactions and activities indicate connection with potential criminal involvement, typologies or red flags provided in reports produced by the FIA, RVIPF or the FATF or CFATF (or other FATF Style Regional Body (FSRB));
- Customers whose transaction patterns appear consistent with generation of criminal proceeds - *e.g.* drug trafficking, corruption, illegal immigration, human trafficking, people smuggling, etc. - based on information available to the MSB; and
- Where the customer or its counterpart is another MSB or financial institution which has been sanctioned by the FSC or FIA for its non-compliance with the current AML/CFT regime and is not engaging in remediation to improve its compliance.

Geographic/Country Risk

Country/geographic risk requires an entity to make a good assessment of the potential ML/TF risks associated with a particular jurisdiction or geographic region. Some of the factors that should be considered when making a determination as to whether a country poses a higher risk include:

- Countries or areas identified by credible institutions, such as the FATF, CFATF or other FSRB, IMF, WB or Egmont Group, as lacking appropriate AML/CFT laws, policies and compliance measures and for which special attention should be given to business relationships and transactions; providing funding or support for terrorist activities or that have designated terrorist organisations operating within them; or that have significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking and people smuggling and illegal gambling;
- Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations or the EU. These may relate to persons (natural and legal) and transactions, and are generally extended and apply to the Territory by Orders in Council; account may also be taken of individual sanctions and embargoes issued by other countries on the basis of ML/TF concerns.

Agent/Distribution Risk

MSBs that use agents to facilitate the delivery of their services should be aware of the risks posed by such relationships. MSBs must ensure that they understand who the agent is, and that they are not criminals or criminal associates. Analysis of such agent risk should take into consideration the following factors insofar as they are relevant to the MSBs' business model:

- Agents identified as PEPs;
- Agents conducting an unusually high number of transactions with another agent location, particularly with an agent in a high risk geographical location;
- Transaction volume of the agent is inconsistent with overall transaction volumes or is atypical of past transaction volumes;
- Agent transaction patterns that indicate the value of transactions is just beneath the CDD threshold;
- Agents serving high-risk customers or transactions;
- Agents who fail to provide required originator information upon request;
- Agents that have been the subject of negative attention from credible media houses or law enforcement sanctions;
- Agents that have failed to attend or complete required training programmes;
- Agents that operate sub-standard compliance programmes that do not effectively manage compliance with internal policies, monetary limits, external regulation, etc.;
- Agents with a history of regulatory non-compliance and that are unwilling to implement a corrective action plan, or have been subject to enforcement action by the Commission or any other regulator;
- Agents with a history of lax, sloppy or inconsistent data collection or record keeping practices;
- Agents who accept false identification or identification records that contain false information, addresses that are known to be non-existent, or bogus phone numbers that are used as fillers;
- Agents whose send-to-receive ratio is not balanced, consistent with other agents in the Territory, or whose transactions and activities indicate potential complicity in criminal activity;
- Agents whose seasonal business fluctuation is not consistent with their incomes or with other agents in the Territory, or is consistent with patterns of criminal proceeds; and
- Agents whose ratio of questionable or anomalous customers to customers who are not in such groups is out of the norm for comparable locations.

Senior Management Role in Risk Management

Risk management governance and controls mechanisms, driven by senior management and the MSB's board of directors, should reflect the company's established risk policy, and ensure that the MSB's AML/CFT function is adequately resourced. Additionally, these governance and control mechanisms should ensure that adequate internal communication processes, relevant to the actual or potential ML/TF risks faced by the MSB, are appropriately implemented.

Senior management should understand the ML/TF risks to which the MSB is exposed, as well as how its AML/CFT control framework operates to mitigate those risks. It is important, therefore, that senior management understands all regulatory and supervisory requirements of the environment in

which the MSB operates. That means having a good knowledge of the Financing and Money Services Act, the Regulatory Code and all AML/CFT legislation.

It is also important that senior management:

- receives sufficient, regular and objective information in order to get an accurate picture of the ML/TF risk the MSB may be exposed to based on its activities and individual business relationships;
- receives sufficient and objective information to understand whether the MSB's AML/CFT controls are effective;
- receives updates on government communications or enforcement actions related to the AML/CFT obligations of MSBs and ML/TF risks; and
- ensures that processes are in place to escalate important decisions that directly impact the ability of the MSB to address and control risks.

Ensuring Compliance

MSBs are subject to inspection by the Commission. During the monitoring and inspection process the Commission is required to review the MSBs' internal control procedures to ensure compliance with regulatory standards. MSBs should, therefore, ensure that their internal control frameworks address the following situations, to allow for compliance with such regulatory standards.

Internal control frameworks should:

- Prioritise MSBs' operations (products, services, customers and geographic locations) based on their vulnerability for abuse;
- Provide for an AML/CFT compliance function and review programme;
- Take into account the environment within which the MSB operates and the activity in its market place, and provide for regular reviews of its risk assessment and risk management processes based on such;
- Ensure that adequate risk assessment and controls are in place before new products are offered;
- Provide a mechanism to inform senior management of compliance initiatives, identified compliance deficiencies, corrective action taken, and suspicious activity reports filed;
- Enable the timely identification and filing of reportable transactions;
- Ensure all appropriate AML/CFT compliance, regulatory record keeping and reporting requirements are met and provide for timely updates in response to changes in laws and guidelines;
- Provide for programme continuity despite changes in management or employee composition or structure;
- Provide for adequate controls, such as transaction limits or management approvals, for higher risk customers, transactions and products, agents, etc., as necessary;
- Provide for adequate management and oversight of agents, including execution of initial agent due diligence, AML/CFT training, and ongoing risk-based monitoring;
- Provide for adequate supervision of employees who handle transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity that forms part of the MSBs' AML/CFT programme;
- Ensure job descriptions and performance evaluations of appropriate personnel include responsibility for AML/CFT compliance; and

- Provide for appropriate initial and refresher training for all relevant staff and agents, paying close attention to the training requirements under the Anti-money Laundering Regulations (regulation 16) and AMLTF Code of Practice (Part VII).

15. Reporting a Suspicious Activity

Suspicious activity is any observed behavior that could indicate money laundering and/or terrorism or terrorism-related crime. All entities that are subject to the requirements of the AMLTF Code of Practice must take steps to identify any activity suspected to be linked to money laundering or terrorist financing and report it to the FIA if they determine that the activity is a viable suspicion. Where reports are not made to the FIA, a record should be made of the activity and the reason for not filing a report (these may be the subject of review by the Commission during its onsite compliance inspections of MSBs).

Any person who voluntarily discloses information to the FIA arising out of a suspicion or belief that any money or other property represents the proceeds of criminal conduct is protected by law under sections 28(2) and 29(5) of the Proceeds of Criminal Conduct Act, from being liable for breach of any duty of confidentiality.

It is therefore important that MSBs appoint MLROs to serve as the point of contact for staff and the FIA in the handling of cases of suspicious customers and transactions. The MLRO should be a senior member of the *key staff* with the necessary authority to ensure compliance with these Guidelines, including the Explanatory Notes contained in the AMLTF Code of Practice.

16. Indicators of Suspicious Activity

New customers and occasional or 'one-off' transactions

MSBs must pay particular attention to the following indicators which may give rise to suspicious activity tending towards money laundering when dealing with new customers or with customers on an occasional or one-off transaction basis:

- Checking identity is proving difficult;
- The customer is reluctant to provide details of his or her identity or is in any other way uncooperative;
- A cash transaction is unusually large; the cash is in used notes and/or small denominations;
- The customer requests currency in large denomination notes;
- The customer will not disclose the source of cash;
- The explanation for the amounts involved are not credible;
- A series of transactions are structured just below the regulatory threshold for due diligence identity checks;
- The customer has made an unusual request for collection or delivery; and
- A customer engages in unnecessary routing of funds through third-parties.

Regular and established customers

In relation to customers that MSBs know and are accustomed to dealing with, attention must be paid to the following indicators which may give rise to suspicious activity of money laundering:

- The size or frequency of the transaction is not consistent with the normal activities of the customer;
- The pattern of transactions has changed since the business relationship was established; and
- There is a sudden increase in the frequency or value of transactions of a particular customer without reasonable explanation.

Examples where customer identification issues have potential to indicate suspicious activity

The following represent examples relative to customer identification that may raise suspicious activity:

- The customer refuses or appears reluctant to provide information requested;
- There appears to be inconsistencies in the information provided by the customer;
- An address appears vague or unusual or, in relation to a known customer, changes frequently;
- The supporting documentation does not add validity to the other information provided by the customer; and
- The customer is in a hurry to rush a transaction through, with promises to provide the information later.

Examples of activity that might suggest there could be potential terrorist activity

The following represent examples of possible links to terrorist activity:

- The customer is unable to satisfactorily explain the source of income or provides contradictory statements that raises doubt about his or her integrity;
- The customer's address changes frequently; and
- Media reports on suspected or arrested terrorists or groups.

17. Record Keeping

It is imperative for MSBs to keep a record of all customer verification measures, all transactions executed, and all suspicious transaction reports filed with the FIA. Maintenance of such comprehensive records enables MSBs to show their compliance with the Anti-Money Laundering Regulations and AMLTF Code of Practice. Such records may also prove crucial if there is an investigation into a customer or suspicious business transaction. The types of records kept may include:

- daily records of transactions;
- receipts;

- cheques;
- customer correspondence; and
- customer information, such as name and address and, in the case of a legal person, controller and beneficial ownership information.

Records may be kept in the following formats:

- original documents;
- certified copies of original documents, including scanned documents;
- microform or microfiche; and
- computerized or electronic format.

All records are required to be maintained for a period of at least 5 years from the date the one-off transaction was completed or the business relationship was terminated.

18. Staffing

Vetting and Recruitment

When recruiting staff MSBs should conduct thorough background checks and assess the competency and probity of applicants to satisfy themselves that the staff they employ have integrity, are adequately skilled and possess the knowledge and expertise necessary to carry out their function. This is particularly important where staff are responsible for implementing AML/CFT controls, whether in compliance or in front-line function.

Such assessment should be done on a continuing basis during a staff member's employment with the MSB and particularly where there is a change in the role or function of the employee.

The level of vetting procedures of staff should reflect the ML/TF risks to which individual staff are exposed and not focus merely on senior management roles. Steps should be taken to manage potential conflicts of interest for staff with AML/CFT responsibilities.

MSBs are obligated to inform the FSC and the FIA of any instance in which an employee is terminated based on the employee's lack of competence with respect to compliance with AML/CFT requirements or on account of the employee's probity.

Employee Training

Employees are required to receive training from time to time, whether internally or externally, to adequately equip them to meet their AML/CFT responsibilities. Effective application of AML/CFT policies and procedures depends on staff within MSBs understanding not only the processes they are required to follow, but also the risks these processes are designed to mitigate, as well as the possible consequences of those risks.

MSBs should ensure that all employees receive appropriate training in relation to money laundering and terrorist financing at least once a year. Training should be relevant to the MSBs' ML/TF risks, business activities, and should be up to date with the latest legal and regulatory obligations, and internal controls.

Employees should be tested appropriately in relation to the training provided to ensure the training has the desired effect. Additionally, levels of compliance should be monitored with the MSBs' AML/CFT controls and appropriate measures applied where staff are unable to demonstrate the level of knowledge expected.

Any training provided should be appropriately tailored to the responsibilities of the employees receiving the training thereby equipping staff with a sound understanding of specialised ML/TF risks they are likely to face and their obligations in relation to those risks and be complemented by AML/CFT information and updates that are disseminated to relevant staff as appropriate.

In addition, the MSBs are required to maintain a record of the training they provide to their staff; these become particularly relevant during an inspection by the Commission to establish the extent to which the MSBs are adhering to their AML/CFT obligations.

19. Obligations in Relation to Agents of MSBs

MSBs that wish to appoint an agent to carry on MSB services on their behalf must seek prior approval from the Commission. In appointing an agent, an MSB must ensure that the agent is 'fit and proper' (see Schedule 1A of the Regulatory Code for the criteria for fitness and propriety), and where the agent is a legal person, that the MSB knows and understands the agent's legal and ownership structure to ensure that the MSB will be forming a business relationship with a legitimate and viable agent. When appointing an agent, the MSB should:

- Identify the agent and perform the necessary background checks and due diligence, such as any recent change from current relationship with other product/service providers, whether the agent is representing another MSB, has been previously licensed, length of time in business, ownership structure, creditworthiness, financial viability, and other regulatory, licensing or registration requirement to which the agent may be subject;
- Obtain information that will allow the MSB to understand the agent's business, the agent's past record of legal and regulatory compliance, expected nature and level of transactions and customer base, and geographical exposure;
- Upon approval, conduct new agent AML/CFT training encompassing applicable AML/CFT requirements, AML compliance programme responsibilities, and MSB internal policies and procedures;
- Provide AML/CFT compliance materials, tools, and training to agents on an ongoing and regular basis;
- Provide guidelines and assistance to the agent to assess the agent's own compliance programme regime and to develop its own risk assessment based upon its unique risk profile for its products and services, customers, geography, and sub-agents or outlets (if applicable);
- Through periodic AML compliance programme reviews, ensure the agent adheres to internal policies and external regulation, including reporting suspicious or attempted suspicious activities, large transactions, monitoring identified risk behaviours, reporting and record keeping; and
- Ensure that any adverse behaviour is promptly addressed by way of further training, probation, suspension or termination of the agent; this includes making a report to the Commission.

Training and Awareness of Agents

Putting in place and maintaining effective controls relies on both training and awareness. MSBs should ensure that agents receive appropriate AML/CFT training either independently, or by providing such training themselves. Training programmes should be implemented that provide appropriate AML/CFT information that is at the appropriate level of detail. All relevant employees and agents should, therefore, be provided with appropriate information on AML/CFT laws, guidelines and internal policies.

The training of agents should be documented and should include the frequency, delivery mechanisms and focus of such training. Training records should be maintained in accordance with the Anti-money Laundering Regulations and AMLTF Code of Practice. MSBs should also conduct periodic assessments of the agent's compliance with internal and external AML/CFT regulatory requirements.

Monitoring of Agents

It is important for MSBs to effectively monitor the activities of their agents to assess and address any potential systemic risks which may arise from issues such as inadequate training, lax internal control procedures, or poor individual judgment or performance.

The degree and nature of such monitoring may depend on:

- the transaction volume of the agent;
- the destination countries of outgoing transactions;
- the origination countries of incoming transactions;
- the monitoring method being utilised (manual, automated or some combination);
- outcomes of previous monitoring mechanisms (where relevant); and
- the type of activity under scrutiny.

Any risk-based approach to monitoring should be based on perceived risks, both external and internal, associated with the agent and should allow the MSB to create monetary or other thresholds or specific red flags to determine which agent activities will be reviewed. Risks include the products or services being provided by the agent, the location of the agent and the nature of the activity being carried out. Situations or thresholds used to define these risks should be reviewed on a regular basis to determine their adequacy for the risk levels established.

MSBs should address any identified risk behaviours promptly and appropriately by carrying out enhanced examination of the agent's transaction history and data integrity, evaluating the agent's explanation of these behaviours, and/or testing the areas of the agent's services that are being questioned. The outcome of such monitoring may result in further training, or probation, suspension or termination of the agent depending on the extent of the deficiencies identified.

19. Combatting Money Laundering and Terrorist Financing

Information Exchange

Information exchange between MSBs and other financial institutions, as well as regulatory and law enforcement authorities, is an important part of a country's strategy for combating ML/TF. Where authorities are armed with suspicion or evidence of a person's link or suspected link to ML or TF,

they should be able to share that information with the MSBs so that the latter can better engage its processes in dealing with such a person. Conversely, MSBs should also be able to share information on suspicions of activities that may be linked to ML or TF with other financial institutions and government agencies, including the regulator. This can only help to strengthen the MSB sector and insulate it from abuse and misuse for ML and TF purposes.

There are various types of information that can be shared between regulatory and law enforcement agencies and MSBs. Such information may include:

- ML/TF risk assessments;
- General feedback on suspicious transaction reports and other relevant reports;
- Typologies of how money launderers or terrorist financiers have misused MSBs;
- Targeted unclassified intelligence which, subject to appropriate safeguards such as confidentiality agreements, may be shared with MSBs, either collectively or individually; and
- Sanctions lists issued through the Governor's Office and published by the FSC and FIA, that include countries, persons or organisations whose assets or transactions should be frozen pursuant to targeted financial sanctions.

Domestic cooperation and information exchange between MSBs and the FSC (as the supervisor of the MSB sector for monitoring and feedback of the remittance flows), among law enforcement and intelligence agencies, and between the FIA and FSC, is extremely important in the effective monitoring and/or supervision of the MSB sector.

Cross border information sharing between authorities and the MSB sector with their international counterparts is also vitally important given the multi-jurisdictional reach of many MSBs.

In situations where MSBs do not have the experience, or have limited capacity to effectively conduct proper ML/TF risk assessments, it is important that they notify the Commission immediately so that appropriate measures can be adopted to prevent any abuse or misuse of the MSBs. This process may include enhanced training and putting in place necessary mechanisms whereby law enforcement agencies are able to share available risk information. Sharing of such information will help MSBs with their assessments of ML/TF risk and should not be impeded in any way once it is done within the ambit of the law.

20. Meeting International Standards

Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) is an inter-governmental body established in 1989. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing, proliferation financing and other related threats to the integrity of the international financial system.

Jurisdictions are required to adhere to the FATF's *International Standards on Combatting Money Laundering and the Financing of Terrorism and Proliferation – The FATF Recommendations.* These Recommendations specify, amongst other things, the requirements outlined in these Guidelines, and determine how they should be applied and adhered to by financial and non-financial institutions.

Caribbean Financial Action Task force (CFATF)

The CFATF, like the FATF, is an inter-governmental body of Caribbean Basin countries established in 1990 and has the responsibility of monitoring its members for compliance with the Kingston Declaration on Money Laundering, including the assessment of its members to establish their level of compliance with the FATF Recommendations. It is an Associate Member of the FATF with which it works closely in ensuring compliance by CFATF Members of their AML/CFT obligations. The Virgin Islands is a founding member of the CFATF and has twice (1999/2000 and 2012/2013) served as chair of the organisation. This membership of the CFATF effectively obligates the Virgin Islands to ensure that appropriate steps are taken to bring all relevant financial and non-financial entities and/or institutions into compliance with AML/CFT obligations. That includes all MSBs, and hence these Guidelines to better steer MSBs into compliance with the AML/CFT legislation.

21. Relevant Legislation

Financing and Money Services Act, 2009 (FSMA)

The Financing and Money Services Act of 2009 provides the legislative framework for the licensing, registration and supervision of persons carrying on financing and money services business.

Additionally, specific legislation have been enacted which, taken together as a package, form a comprehensive anti-money laundering and anti-terrorist financing regime. The most significant of these are the Proceeds of Criminal Conduct Act, 1997, the Anti-money Laundering Regulations, the AMLTF Code of Practice, The Terrorism (United Nations Measures) (Overseas Territories) Order 2001 and the Anti-Terrorism (Financial and Other Measures) (Overseas Territories) Order 2002.

Proceeds of Criminal Conduct Act 1997 (PCCA)

All MSBs should be aware of the laws relating to ML/TF and ensure that they adopt appropriate measures to ensure compliance with their legal obligations and steer clear of becoming the subject of criminal investigation and prosecution. The key legislation are outlined below, but MSBs should be aware of other enactments, such as the Financial Services Commission Act, which create AML/CFT supervisory responsibilities in relation to MSBs and other financial institutions.

The PCCA established the core money laundering offences in the Virgin Islands. It also contains provisions for the making and enforcement of confiscation orders and establishes certain investigatory and co-operative powers to enhance enforcement efforts.

Under the PCCA, five primary money laundering offences are established: (i) acquisition, possession or use of proceeds of criminal conduct; (ii) assisting another to retain the benefit of criminal conduct; (iii) concealing or transferring proceeds of criminal conduct; (iv) tipping-off; and (v) failing to disclose a suspicion.

- **Acquisition, possession or use of proceeds of criminal conduct**

It is an offence to acquire, transfer or use any property, or take possession of property which, in whole or in part, directly or indirectly represents the proceeds of criminal conduct. It is also an offence for a person who, knowing or suspecting that any property is the proceeds of someone else's criminal conduct, acquires, transfers or uses that property or have possession of it.

- **Assisting**

A person commits an offence if he or she enters into or is otherwise concerned in an arrangement which he or she knows or suspects facilitates, whether by concealment, removal from the virgin Islands, transfer to nominees or other means, the acquiring, retention, use or control of proceeds of criminal conduct.

- **Concealing**

A person commits an offence if, knowing or having reasonable grounds to suspect that any property, in whole or in part, directly or indirectly, represents another person's proceeds of criminal conduct, he or she conceals or disguises that property or converts or transfers that property or removes it from the Virgin Islands.

- **Tipping Off**

A person commits an offence if he or she knows or suspects that an investigation is being or is about to be conducted into money laundering, and he or she discloses information to any other person which is likely to prejudice that investigation.

It is also an offence if a person knows or suspects that a disclosure of suspicion has been made or is being made and he or she leaks information that is likely to prejudice any investigation which might be conducted as a consequence of the disclosure. This offence extends to disclosures which would prejudice a confiscation investigation as well as a money laundering investigation.

Separate offences exist for interfering with documents and other materials relevant to an investigation.

- **Failure to Disclose**

A person commits an offence if he or she knows, suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering, if the information on which the suspicion is based came to his or her attention in the course of his or her trade, profession, business or employment, and he or she does not disclose his or her suspicion as required by the law as soon as it is reasonably practicable after it comes to his or her attention. It should be noted that any person complying with the law by making a disclosure is protected from any liability.

Anti-Money Laundering Regulations, 2008 (AMLR)

The AMLR are promulgated under section 41 of the PCCA and apply to persons described as "relevant persons" under regulation 2 (1) of the AMLR. The term includes remittance service providers and money transmission services.

The AMLR outline the requirements of a relevant person in relation to:

- the establishment of proper identification procedures;
- maintenance of verification procedures;
- maintenance of records of transactions and reports and verifications thereof (nature of evidence, copy of evidence and other relevant information);
- retention period of records;
- staff training;
- maintenance of records of SARs/STRs (register of reports and inquiries);
- the duty to appoint an MLRO; and

- establishing written internal reporting procedures in relation to suspicious activities.

Every business covered by the AMLR must be supervised by a supervisory authority and must comply with the provisions of the AMLR. That supervisory authority in the case of MSBs is the Commission.

The Anti-Money Laundering and Terrorist Financing Code of Practice 2008 (AMLTF Code of Practice)

The AMLTF Code of Practice was issued by the Commission in 2008 pursuant to section 27(1) of the PCCA. It provides guidance on interpreting, understanding and applying the requirements of the AMLR and the Code. It ensures that appropriate systems and controls are in place to detect and prevent ML/TF, and promotes the use of an appropriate risk-based approach to the detection and prevention of money laundering and terrorist financing.

The Terrorism (United Nations Measures) (Overseas Territories) Order 2001 (TUNMOTO)

The TUNMOTO is an Order in Council which makes provision prohibiting a person from making any funds or financial services available, whether directly or indirectly, to another person for purposes of committing an act of terrorism. The prohibition extends to facilitating the commission of an act of terrorism. In addition, a financial institution commits an offence if it fails to disclose knowledge or suspicion of the commission of an offence in relation to a prohibition under the TUNMOTO.

Anti-Terrorism (Financial and Other Measures) (Overseas Territories) Order 2002 (ATFOMOTO)

The ATFOMOTO prohibits a person from engaging in fund-raising activities for such funds to be used for purposes of terrorism. In addition, it prohibits the use and possession of money or other property for purposes of terrorism or engaging in funding arrangements to advance terrorism purposes. The prohibition is extended to being concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property by concealment, removal from the Virgin Islands or in any other way. Accordingly, any person who becomes aware of any failure on these prohibitions and fails to make a disclosure to law enforcement commits an offence. Any person making a disclosure in compliance with the law is protected from any liability.

24. Conclusion

These Guidelines are designed to assist MSBs in their compliance with their AML/CFT obligations under the laws of the Virgin Islands. If closely followed, they should enable MSBs to properly and effectively assess their ML/TF risks and take appropriate measures to mitigate those risks.

However, it should be noted that these Guidelines are not a substitute to the AML/CFT laws. They are only meant to guide MSBs in managing their business relationships and business transactions to prevent any person abusing or misusing them for ML/TF or other nefarious purposes. It is therefore important that MSBs seek to understand the AML/CFT laws as they adhere to and apply the provisions of these Guidelines.

Issued by the Financial Services Commission this 17th day of November, 2016.

Signed:

Robert Mathavious
Managing Director/CEO