British Virgin Islands Financial Services Commission

ANTI-MONEY LAUNDERING & COMBATTING TERRORIST FINANCING GUIDELINES FOR THE BANKING SECTOR

Published: 1 July, 2020

Issued: 1 July, 2020

Approved by the Board of Commissioners: 23 June, 2020

Table of Contents

INTRODUCTION 1

1. Abbreviations and definitions 3

2. Understanding Money Laundering, Terrorist Financing and Proliferation Financing 5

Money Laundering **5**

Anti-money Laundering **6**

Terrorist Financing **6**

Combating the Financing of Terrorism **6**

Proliferation Financing **6**

3. Banking Business 7

The Legislative and Regulatory Framework **7**

Licensing of Banks **7**

4. AML/CFT Regulatory Regime 8

Proceeds of Criminal Conduct Act, 1997 (PCCA) **8**

Anti-Money Laundering Regulations, 2008 (AMLR) **9**

Anti-Money Laundering and Terrorist Financing Code of Practice 2008 (AMLTFCOP) **9**

Terrorism (United Nations Measures) (Overseas Territories) Order 2001 (TUNMOTO) **9**

Anti-Terrorism (Financial and Other Measures) (Overseas Territories) Order 2002 (ATFOMOTO) . **9**

Terrorist Asset-Freezing etc. Act 2010 (Overseas Territories) Order 2011 ..... **9**

Proliferation Financing (Prohibition) Act, 2009 (PFPA) **10**

5. Meeting International Standards 10

Financial Action Task Force (FATF) **10**

Caribbean Financial Action Task Force (CFATF) **10**

How is it determined whether international standards are met? **10**

6. Duty of the FSC and Banks 11

7. Financial Inclusion and AML/CFT 12

What is financial inclusion? **12**

Financial inclusion and AML/CFT **12**

8. Risk-based Approach 13

What is meant by a risk-based approach (RBA)? **13**

How should banks go about identifying and assessing risks? **13**

How can banks manage and mitigate identified risks? **14**
How do banks ensure their RBAs are effective? **15**
9. Internal Controls 16
What are internal controls? **16**
What should be included in a bank's internal controls? **16**
10. Governance 17
11. Money Laundering Reporting Officer (MLRO) 17
What is the role of an MLRO? **17**
12. Customer Due Diligence / Enhanced Customer Due Diligence 18
What is customer due diligence? **18**
Why should banks conduct CDD? **18**
When should a bank conduct CDD? **18**
Steps for conducting CDD **18**
What if the customer is a legal person or arrangement? **19**
What if a person is acting on behalf of another person? **19**
What methods can a bank use for verification? **20**
Timing of verification **20**
What happens if a bank cannot verify the customer's identity within 30 days? **21**
What should a bank do once it has obtained relevant CDD information? **21**
Application of CDD measures **21**
Ongoing CDD **22**
Ongoing monitoring **22**
What if a bank cannot apply appropriate CDD measures, including verification? **23**
Are there any relationships a bank is prohibited from establishing? **23**
13. Wire Transfers 24
Cross-border wire transfers **24**
Domestic wire transfers **25**
14. Correspondent Banking Relationships 26
15. Reporting a Suspicion 27
16. Indicators of Suspicious Activity 28
How can a bank tell if an activity is suspicious? **28**
17. Record Keeping 30
Transaction records **30**

CDD records **30**
SARs/STRs **30**
Period and format of retention **30**
18. Employee Screening and Training 32
Employee screening **32**
Employee training **32**
Employee Testing **33**
Training records **33**
19. Internal Audits 33
20. A Final Reminder 33

INTRODUCTION

Banks play an integral role in the global financial services landscape. Locally and internationally, banks offer legitimate individuals and businesses financial products and services that meet their needs. Criminals can however also use banks to launder the proceeds of crime by concealing the source and ownership of illegally derived money, and to fund terrorism, terrorist organisations or the production of weapons of mass destruction by concealing the intended purpose of their funds. Supervisory authorities around the world are therefore responsible for ensuring that banks under their remit have adequate and appropriate controls and procedures in place to prevent, deter and combat money laundering (ML), terrorist financing (TF) and proliferation financing (PF).

BACKGROUND

As an International Finance Centre, the Virgin Islands is committed to playing its role in the global fight against ML, TF, PF and other financial crimes by ensuring that all financial institutions are licensed and adequately supervised. Banks in the Virgin Islands are licensed under the Banks and Trust Companies Act, 1990 and are regulated and supervised by the Financial Services Commission (FSC).

Banking entities licensed by the FSC are required to put controls in place to prevent ML, TF and PF activities in accordance with the Territory's AML/CFT framework. This framework includes the Proceeds of Criminal Conduct Act, 1997 (PCCA), the Anti-Money Laundering Regulations, 2008 (AMLR) and the Anti-Money Laundering and Terrorist Financing Code of Practice, 2008 (AMLTFCOP).

PURPOSE

The guidelines are intended to supplement the explanatory notes to the AMLTFCOP, by providing user-friendly and practical AML/CFT guidance specifically geared towards banking institutions. Banks should use these guidelines as a tool to understand and navigate the requirements of the jurisdiction's AML/CFT legislative framework, as well as the 40 Recommendations of the Financial Action Task Force and to implement appropriate AML/CFT programmes within their institutions.

The guidelines present a fundamental understanding of ML, TF and PF along with the jurisdiction's legal and regulatory framework for combatting these crimes. They also set out the international standard-setting bodies leading the fight against ML, TF, PF and related threats and the role they play in assessing the Virgin Islands' AML/CFT framework.

Within the guidelines, banks are also provided with guidance on how they may implement a risk-based approach to AML/CFT that promotes financial inclusion. The guidelines also detail the expectations of a bank as an organisation, its staff and in particular, its Money Laundering Reporting Officer (MLRO), as it relates to AML/CFT matters.

The guidelines stress the importance of understanding individual customers and the risks they pose, undertaking simplified and enhanced due diligence and implementing ongoing monitoring measures to help banks identify suspicious transactions or activities relating to specific customers. Additionally, they detail banks' obligations relating to wire transfers and correspondent banking relationships, each of which present their own risks.

Finally, the guidelines underscore that an efficient AML/CFT regime relies on banks having a good system of governance, record keeping, employee screening, training and suspicious activity reporting.

In using the guidelines to implement an AML/CFT programme, each bank will need to take its unique circumstances into account. While they provide a useful compliance tool, the guidelines are not a

substitution for legislation, notably the AMLR and AMLTFCOP, including the latter's Explanatory Notes, and should be read in conjunction with the relevant legislation.

1. Abbreviations and definitions

Abbreviations

AML/CFT	Anti-money laundering and combating the financing of terrorism
CDD	Customer due diligence
ECDD	Enhanced customer due diligence
FATF	Financial Action Task Force
FSRB	FATF-style regional body
FIA	Financial Investigation Agency
ML	Money laundering
MLRO	Money Laundering Reporting Officer
PF	Proliferation financing
RBA	Risk-based approach
STR	Suspicious transaction report
SAR	Suspicious activity report
TF	Terrorist financing

Definitions

Business relationship	When two parties do business on a frequent or habitual basis.
Key staff	Employees who deal with customers or clients and their transactions.
MLRO	A person appointed to ensure that the bank complies with all AML/CFT legislation and internal reporting and compliance procedures. They liaise between the bank and the FIA around suspicious activities.
One-off transaction	A transaction carried out other than in the course of an established business relationship.
Politically exposed persons (PEPs)	Individuals who are or have been entrusted with prominent public functions and members of his or her immediate family, or persons who are known to be close associates of such individuals. PEPs may be domestic or foreign and include persons who are or have been entrusted with a prominent function by an international organisation. PEPs generally comprise persons who are Heads of State/Government, cabinet ministers/secretaries of state, judges (including magistrates where they exercise enormous jurisdiction), senior political party functionaries and lower political party functionaries with an influencing connection in high ranking government circles, military leaders and heads of police and national security services, senior public officials and heads of public utilities/corporations, members of ruling royal families, senior representatives of religious organisations where their functions are connected with political, judicial, security or administrative responsibilities and senior management of international

organisations in positions such as directors, deputy directors and members of the board and equivalent functions.

The AMLR, AMLTFCOP and Banks and Trust Companies Act, 1990 provide definitions for other terms in these guidelines. Users of these guidelines should also refer to these accordingly.

2. Understanding Money Laundering, Terrorist Financing and Proliferation Financing

Money Laundering

Money laundering (ML) is the process used to disguise the illicit origin and conceal the true ownership of illicit proceeds, by channeling these criminal proceeds via the financial system and economy. Money launderers seek to hide their actions through a series of steps that make it appear as if money that comes from illegal or unethical sources was earned legitimately. ML enables criminals to generate and maximize income, without jeopardising their illicit source. The three stages of ML described below may occur in sequence but often overlap.

(i) Placement

This introduces criminal proceeds into the financial system, usually as cash, and may include:

- Placing cash on deposit at a bank (often mixed in with a legitimate credit to obscure the audit trail)
- Physically moving cash between jurisdictions
- Wiring cash to various locations within and between jurisdictions
- Converting cash into debt by making loans in cash to businesses which seem to be legitimate or are connected with legitimate businesses
- Purchasing high-value goods for personal use (e.g. vehicles, furniture) or as presents (e.g. jewellery) to reward colleagues.

(ii) Layering

This separates criminal proceeds from their source by creating layers of transactions designed to disguise the audit trail and provide the appearance of legitimacy. It typically includes:

- Switching funds rapidly between banks and/or jurisdictions
- Using cash deposits as collateral security for legitimate transactions
- Switching cash across several jurisdictions through a network of legitimate businesses and companies not engaged in any known business activity
- Reselling goods/assets.

(iii) Integration

If layering has succeeded, integration places the criminal proceeds back into the economy so they appear to be legitimate funds or assets.

There are many ways of laundering criminal proceeds. Although this does not always directly involve the financial sector, hundreds of billions of dollars are laundered through banks annually. As their services and products make them especially vulnerable to abuse by money launderers, banks must be extra vigilant.

The Virgin Islands has put laws and guidelines in place to improve the understanding, detection and prevention of money laundering. These target activities that may include market manipulation, improper trading of goods, corruption of public funds and evasion of tax. All financial institutions, including banks, must play their role in understanding, detecting and preventing ML by putting proper internal procedures for knowing their customers, maintaining proper records and identifying and reporting suspicious activities, in place.

Anti-money Laundering

Anti-money laundering (AML) refers to a set of policies, procedures, laws and guidelines designed to forestall and prevent the practice of generating income through illegal activity.

Terrorist Financing

Terrorist financing (TF) means providing or collecting funds directly or indirectly with the aim or knowledge that these will be used for terrorism or by a terrorist or terrorist organisation. This may involve funds raised from legitimate sources, such as personal donations and profits from businesses and charities, or from criminal sources, such as the drugs trade, smuggling, fraud, kidnapping and extortion. TF also extends to the financing of travel of individuals for the purpose of penetrating, planning, or preparing or participating in, terrorist acts or providing or receiving terrorist training.

Terrorists use techniques similar to money launderers to evade attention and protect the identities of their sponsors and the ultimate beneficiaries of the funds.

Banks are attractive to terrorists who wish to move funds within and across jurisdictions. When the funds come from legitimate sources, detecting and tracking them becomes more difficult. It is therefore important to exercise vigilance in establishing the nature of business relationships when facilitating transactions, especially wire transfers.

Combating the Financing of Terrorism

Like AML, combating the financing of terrorism (CFT) refers to those policies, procedures, laws and guidelines designed to prohibit people from generating income for use in terrorism. This involves policies, procedures and laws regarding the criminalisation of terrorism and terrorist financing, transaction monitoring, and the gathering of intelligence and monitoring of suspected and confirmed terrorist cells. People involved in terrorist financing (TF) may often get money from legitimate sources (e.g. charitable fundraising) and use it to fund people or organisations who undertake terrorist activity. It is possible to contribute unknowingly to funds which end up being use for terrorism (e.g. charitable fundraising to build a school in a foreign country). This makes it all the more important that banks undertake active due diligence not only by collecting information from their customers but also by taking steps to ensure they know their customers and their source of funds and source of wealth.

Proliferation Financing

Proliferation financing (PF) is referred 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."[1]

The mechanics for PF are essentially the same as for TF.

PF could pose a significant threat to global stability if used to develop weapons of mass destruction. To stop these weapons from getting into terrorists' hands, international standards from the FATF require countries to identify and prevent any act tending towards the financing and development of such weapons.

[1] https://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf

3. Banking Business

The Legislative and Regulatory Framework

The Banks and Trust Companies Act, 1990 (BTCA) is the legislative framework for licensing, regulating and supervising banking business in the Virgin Islands.

Section 2 of the BTCA defines banking business as "the business of accepting deposits of money which may be withdrawn or repaid on demand or after a fixed period or after notice, by cheque or otherwise and the employment of such deposits, either in whole or in part (a) in making or giving loans, advances, overdrafts, guarantees or similar facilities, or (b) the making of investments, for the account and the risk of the person accepting such deposits".

Under the BTCA, a bank may obtain either a general, Class I or Class II banking licence. A general banking licence allows the bank to carry on banking business without any restrictions on service. A Class I banking licence prohibits the bank from taking deposits from persons resident in the Virgin Islands except for another licensee or companies registered under the BVI Business Companies Act, 2004. A Class II banking licence has the same restrictions and further prohibits the bank from receiving or soliciting funds from persons other than those listed on its licence.

Licensing of Banks

Under the BTCA and other legislation, the FSC is responsible for licensing and supervising persons that perform banking business in or from within the Territory. Any such person must have a valid licence from the FSC. To obtain such a licence, the applicant must satisfy the requirements of the BTCA, the Financial Services Commission Act, 2001 and the Regulatory Code, 2009.

For avoidance of doubt, a BVI Business Company that carries on any kind of banking business outside the Virgin Islands is considered to be carrying on banking business from within the Territory, and is therefore subject to the licensing requirements of the BTCA.

4. AML/CFT Regulatory Regime

The Virgin Islands' comprehensive AML/CFT regime comprises a number of legislation to which banks are subject. Banks are therefore required to implement measures to prevent, forestall and identify ML/TF activities. Failure to comply can lead to criminal investigation and prosecution.

The key legislation comprises the Proceeds of Criminal Conduct Act, 1997, the Anti-money Laundering Regulations, 2008, the Anti-money Laundering and Terrorist Financing Code of Practice, 2008, the Terrorism (United Nations Measures) (Overseas Territories) Order 2001, the Anti-Terrorism (Financial and Other Measures) (Overseas Territories) Order 2002, the Terrorist Asset-Freezing etc. 2010 (Overseas Territories) Order 2011, and the Proliferation Financing (Prohibition) Act, 2009, which are outlined below.

Banks should be aware of other enactments, such as the Financial Services Commission Act, 2001 (FSCA) and the Regulatory Code, 2009 which create AML/CFT supervisory responsibilities for banks and other financial institutions.

Proceeds of Criminal Conduct Act, 1997 (PCCA)

The PCCA establishes the five primary ML offences below. It also contains provisions for making and enforcing confiscation orders and establishes certain investigatory and co-operative powers to enhance enforcement.

(i) Acquiring, possessing or using the proceeds of criminal conduct

It is an offence to acquire, take possession of, transfer or use any property which wholly, partly, directly or indirectly represents the proceeds of criminal conduct. It is also an offence to do any of this if you know or suspect the property to be the proceeds of criminal conduct.

(ii) Assisting another to retain the benefit of criminal conduct

It is an offence to be in any way involved in an arrangement which you know or suspect will facilitate the acquisition, retention, use or control of a property which represents the proceeds of criminal conduct, whether by concealment, removal from the Virgin Islands, transfer to nominees or other means.

(iii) Concealing or transferring proceeds of criminal conduct

It is an offence to conceal, disguise, convert or transfer a property or to remove it from the Territory if you know or have reasonable grounds to suspect that it represents the proceeds of criminal conduct.

(iv) Tipping off

If you know or suspect that an ML investigation is happening or about to take place, it is an offence to disclose information to anyone else which is likely to prejudice that investigation. Equally, if you know or suspect that a disclosure of suspicion has been or is being made, it is an offence to leak information that could prejudice any investigation conducted as a consequence. This extends beyond ML investigations to disclosures which would prejudice a confiscation investigation. Interfering with documents and other materials relevant to an investigation are also offences.

(v) Failure to disclose a suspicion

If in the course of your trade, profession, business or employment you know or suspect (or have reasonable grounds for knowing or suspecting) that someone is laundering money, it is an offence

not to disclose your suspicion as soon as reasonably practicable. You will be protected from liability if you comply with the law by making a disclosure.

Anti-Money Laundering Regulations, 2008 (AMLR)

The AMLR are promulgated under section 41 of the PCCA and apply to "relevant persons", which includes banks. Relevant persons must comply with the AMLR's requirements to:

- Establish proper identification procedures
- Maintain verification procedures
- Maintain records of transactions and reports and verifications of these
- Retain records for a period
- Train staff
- Maintain records of SARs/STRs (register of reports and inquiries)
- Appoint an MLRO
- Establish written internal reporting procedures in relation to suspicious activities.

Every business covered by the AMLR has a supervisory authority. For banks, this is the FSC.

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

The Code, established under section 27A of the PCCA, provides the detailed legal framework for effectively combating money laundering and terrorist financing. In addition to the legal framework it also provides guidelines in the form of Explanatory Notes with regards to the interpretation of the Code and how the Commission expects its provisions to be implemented. It outlines the systems and controls that relevant entities need to have in place to detect and prevent and identify ML/TF, and promotes the use of a risk-based approach to implementing appropriate AML/CFT programmes. It must always be read in conjunction with the AMLR.

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

The TUNMOTO prohibits making any funds or financial services available directly or indirectly for committing or facilitating an act of terrorism. It is an offence to fail to disclose knowledge or suspicion of the commission of an offence relating to a prohibition under the TUNMOTO.

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

The ATFOMOTO prohibits raising funds to be used for terrorism. It also prohibits using and possessing money or other property for terrorism or engaging in funding arrangements to advance terrorism. This extends to helping to retain or control terrorist property by concealment, removal from the Virgin Islands, or in any other way.

It is an offence if you become aware of any failure of these prohibitions and do not disclose this to law enforcement. You will be protected from liability if you comply with the law by making a disclosure.

Terrorist Asset-Freezing etc. Act 2010 (Overseas Territories) Order 2011

The TAFAOTO extends Part 1 (including Part 1 of Schedule 2) of the United Kingdom's Terrorist Asset-Freezing etc. Act 2010 to the Territory and replaces the existing power that the Territory has to freeze the assets of those suspected of being involved in terrorism under the TUNMOTO.

Proliferation Financing (Prohibition) Act, 2009 (PFPA)

The PFPA empowers the FIA to issue directions to any person in relation to any country where the FIA reasonably believes that the development, production or facilitation of nuclear, radiological, biological or chemical weapons in that country poses a significant risk to the Virgin Islands or United Kingdom. The FIA can impose restrictions and conditions on any dealings with that country's persons or government. The FIA's extensive powers include investigative and civil penalty powers.

As the techniques used by money launderers and other criminals consistently evolve, so must the regulatory framework and environment. Banks are expected to keep up to date on amendments to legislation, new legislation and new guidance.

5. Meeting International Standards

As a key international financial centre, the Virgin Islands operates an AML/CFT regime that aims to meet international standard-setting bodies' requirements for protecting the international financial system from misuse by criminals.

Financial Action Task Force (FATF)

The key standard-setting body for AML/CFT is the Financial Action Task Force (FATF). Its objectives are to set standards and to promote the effective implementation of legal, regulatory and operational measures for combating ML, TF, PF and related threats to the integrity of the international financial system.

Jurisdictions must adhere to the FATF's International Standards on Combatting Money Laundering and the Financing of Terrorism and Proliferation, known as the FATF Recommendations. These specify the requirements outlined in these guidelines and determine how they should be applied.

Caribbean Financial Action Task Force (CFATF)

Another inter-governmental body, the CFATF has responsibility for monitoring Caribbean Basin countries' compliance with the Kingston Declaration on ML, including assessing members' compliance with the FATF Recommendations. The CFATF is an Associate Member of the FATF and is one of 9 FATF-Style Regional Bodies (FSRB). The Virgin Islands is a founding member of the CFATF and has twice served as chair.

How is it determined whether international standards are met?

The Territory is subject to a mutual evaluation (a peer review by other CFATF, FATF or FSRB members) of how it meets the FATF recommendations. This review assesses the Virgin Islands' AML/CFT legislative framework and whether the Territory is effectively implementing measures to mitigate its ML/TF risks. The FATF's Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT systems guides this peer review process.

6. Duty of the FSC and Banks

The FSC has a duty to monitor the compliance of its licensed entities, including banks, with the AMLR, AMLTFCOP and any other AML/CTF measures. This can entail both onsite and offsite inspections.

Banks need to maintain and make available to the FSC upon request evidence of the policies, procedures and documentation prescribed within the AMLTFCOP, the AMLR and other relevant AML/CFT legislation.

Where compliance failures are identified, the FSC may take enforcement action. As it is an offence for a bank not to comply with AML/CFT regulatory requirements, directors, members and employees, including managers and other senior officers, may be liable to criminal prosecution under the PCCA.

Duty of vigilance

All bank employees – in particular, all customer facing employees and managers – are at risk of becoming involved in criminal activity if they are negligent in their vigilance. Systems should be in place to enable staff to react effectively to suspicious behaviour or transactions by reporting them to the relevant in-house personnel.

Consequences of failure

(i) First consequence

The first consequence of failure in vigilance is likely to be commercial, as banks which become involved in ML/TF, however unwittingly, risk the loss of their good market name and market position and may incur additional unnecessary costs and expenses. This may also affect business relationships with other financial institutions, including correspondent banks and those with whom wire transfers are made.

(ii) Loss of Fit And Proper Standing Consequence

Next the bank may suffer the loss of its fit and proper standing. This may result in an increased level of supervision by the FSC and ultimately suspension or revocation of the bank's licence.

(iii) Criminal Prosecution Consequence

Finally, as mentioned, there is a real risk of criminal prosecution for any employee who fails to adhere to requirements set out in the AMLTFCOP and AMLR and the POCCA. At a minimum, as with the bank itself, the employee's good name is likely to suffer.

(iv) Cumulative effect

Taken together, these consequences will lead to a loss of confidence in the bank and damage its reputation.

7. Financial Inclusion and AML/CFT

What is financial inclusion?

Financial inclusion means the provision of access to an adequate range of safe, convenient and affordable financial services to disadvantaged and other vulnerable groups, including low income, rural, elderly and undocumented people who have been underserved by, or excluded from, the regulated financial sector.

The FATF also sets out that financial inclusion is about making a broader range of financial services available to individuals who currently only have access to basic financial products.

Financial inclusion and AML/CFT

Banks play an important role in supporting financial inclusion. It is essential that essential products and services are offered through regulated banks that are subject to adequate AML/CFT supervision, as opposed to unregulated, underground facilities which may take advantage of people and expose them to fraud, and which may be conduits for illicit activities and transactions.

It is also important that banks implement a risk-based approach, with the flexibility to use simplified measures for underserved and excluded persons who may pose relatively low levels of ML/TF risks. For example, a bank that normally requires two forms of identification could require a senior citizen who intends to conduct limited business to only provide a national health insurance card, as this person may not possess any other form of identification.

8. Risk-based Approach

What is meant by a risk-based approach (RBA)?

Taking a RBA towards AML/CFT requires banks to identify and assess the ML/TF risks to which they are exposed and take commensurate measures to prevent and mitigate the identified risks effectively.

A RBA offers banks some flexibility in implementing AML/CFT measures by allowing banks to place greater focus on organising internal controls and allocating resources (including compliance resources) in the areas which are most vulnerable to, and pose the greatest levels of ML/TF risk. This approach enhances the efficacy of the bank's AML/CFT programme.

How should banks go about identifying and assessing risks?

In identifying and assessing risks, a bank must first identify the ML/TF threats posed to the Virgin Islands as a jurisdiction, as well as the jurisdictions to which it is exposed, the banking sector, the products and services being offered by the bank and its customers. A bank will next need to determine and understand how and the extent to which its organisation is vulnerable to ML/TF, based on the threats identified. Assessment of risks should be informed by internal sources such as customer profiles and transactions, internal audit reports, analysis of logged STR/SARs and the bank's own knowledge of its business. Banks should also use information and data from credible external sources such as reports and guidance from the FSC, FIA and international bodies, national risk assessments, typology reports, mutual evaluation reports, sanctions lists and reliable media reports.

The assessment should consider the risk factors below.

(i) Product/service or delivery channels risk

Banks should consider the characteristics of the products and services that they offer, along with the delivery channels used, and the extent to which they can be abused for ML/TF. Special attention should be given to new or innovative products that the banks do not offer but which their services help to deliver. An assessment here might consider:

- the nature, size and complexity of the bank's business (including the volume and size of transactions)
- products or services offered that require higher monetary values
- geographical reach of the products or services
- the complexity of products or services being offered
- the extent to which non face-to-face customer transactions are conducted
- products or services that allow for third party payments
- products or services that permit the exchange of cash for a negotiable instrument, such as a stored value card or money order
- products or services that seek to provide anonymity or layers of opacity, or that can readily transcend international borders, such as cash, online payment systems, stored value cards, money orders, mobile payments, prepaid cards and international wire transfers.

(ii) Customer risk

This is the potential risk posed by a customer, category of customers or the bank's overall customer base. Assessment should take into consideration the potential impact of mitigating such risk. Customers may pose higher levels of risk if they:

- engage in cash or equivalent intensive business
- work in high-risk industries such as mineral extraction, pharmaceuticals or oil and gas
- are PEPs, or family members or close associates of PEPs where the beneficial owner of a customer is a PEP
- are based in, or conduct business in or through a high risk jurisdiction, or a jurisdiction with known corruption, organized crime or drug production/distribution
- appear to know little, or are reluctant to disclose details (address, contact information, etc.), about the payee or beneficiary of a wire transfer
- are known to the bank as having been the subject of law enforcement sanctions
- are suspected of illegal activity
- have been, or have a counterpart who has been, sanctioned by the FSC or FIA for non-compliance with the AML/CFT regime and are not trying to improve compliance.

(iii) Geographic/country risk

Banks should assess the potential ML/TF risks associated with a particular jurisdiction or geographic region to which the institution is exposed. These include the countries and regions; where its applicants for business and customers are nationals, resident and/or conduct business, where financial institutions within its group operate and provide services and where financial counterparts operate and conduct business (e.g. respondent banks). Factors to consider include those below.

- Countries or areas which:
  - have been identified by credible institutions (such as the FATF, CFATF or other FSRBs, IMF, World Bank or Egmont Group) as lacking appropriate AML/CFT laws, policies and compliance measures and where special attention should be given to business relationships and transactions
  - fund or support terrorist activities or have designated terrorist organisations operating within them
  - have significant levels of organized crime, corruption, or other criminal activity, including being source or transit countries for illegal drugs, arms dealing, human trafficking, people smuggling and illegal gambling.
- Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations or European Union. These may relate to persons (natural and legal) and transactions emanating from a particular jurisdiction, and are generally extended to the Virgin Islands 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 with a particular country.
- Countries or areas identified by credible sources such as the OECD as lacking transparency or having excessive secrecy laws.

How can banks manage and mitigate identified risks?

Banks should mitigate and manage risks by introducing suitable procedures, systems and controls for customer acceptance, due diligence and ongoing monitoring. These must be approved by senior managers, who are responsible for reviewing and monitoring implementation and enhancing measures as needed.

Banks may rank their ML/TF risks in various categories (e.g. high, medium and low; or high, medium high, medium, medium low and low). This will help them allocate compliance resources, organise internal controls and internal structures, and implement policies and procedures to deter and detect ML/TF.

Higher risk areas should be subject to enhanced procedures, which may include:

- Requiring additional customer due diligence information for customers engaging in high-risk transactions or dealing with higher risk jurisdictions
- Requiring real time monitoring for higher risk customers
- Updating CDD information more frequently
- Requiring senior management approvals when engaging with higher risk transactions or high-risk customers such as PEPs
- Setting transaction limits (amounts and/or frequency of transactions) for higher risk transactions and customers.

Although an RBA enables a focus on areas that pose the highest AML/CFT risk, this should not stop banks addressing medium and lower risk areas. For these, banks may implement standard or simplified controls.

It is imperative that banks document their risk assessments to demonstrate their allocation of compliance resources and focus of internal controls to higher risk areas, as well as to substantiate their decision that simplified, standard or enhanced measures are appropriate.

How do banks ensure their RBAs are effective?

Risk assessments are not one-offs. Changes in risk factors such as customer conduct, development of new technologies, new embargoes or changes in the volume of transactions being undertaken may impact the ML/TF risks of the institution. It is therefore vital for banks to undertake and document risk assessments regularly to determine whether the risks identified remain relevant and if new potential risks have emerged.

Banks should also maintain an ongoing understanding of the overall ML/TF risk for their sector, as well as the risks specific to their products, services and customer base. A mechanism for consistently assessing the effectiveness of internal controls should be implemented by banks.

An effective RBA requires clear communication of policies and procedures across the bank, along with robust mechanisms for implementation, identifying weaknesses and making improvements.

Where banks lack the experience or capacity to conduct proper ML/TF risk assessments, they should notify the FSC immediately. The FSC will take measures to prevent any abuse or misuse of the banks it regulates, such as providing enhanced training and enabling law enforcement agencies to share available risk information.

9. Internal Controls

What are internal controls?
Internal controls are the written, risk-based policies, processes and procedures that banks need to have in place as the basis of a programme to identify and prevent ML/TF.

What should be included in a bank's internal controls?
The internal controls should comply with the AMLR and the AMLTCOP, as well as other relevant legislation. They must include, at minimum, the following (see section 11(3) of the AMLTFCOP):

- Greater focus on the products, services, customers and geographic locations that are more vulnerable to ML/TF abuse
- Regular reviews of risk assessments and management policies, processes and procedures
- Designation of a Compliance Officer responsible for managing AML/CFT compliance
- An AML/CFT compliance function and review programme
- Processes for expediting any inspection report's recommendations on regulatory breaches and AML/CFT compliance
- Measures to meet record keeping and reporting requirements
- Timely updates in response to changes in regulations, policies and other AML/CFT initiatives
- Risk-based customer due diligence policies, processes and procedures
- Additional controls for higher risk customers, transactions and products as necessary
- Mechanisms for the timely identification and accurate filing of reportable transactions
- Adequate supervision of employees who handle applicable currency transactions, complete reports, monitor for suspicious activity or engage in any other activity that forms part of the bank's AML/CFT programme
- Incorporation of AML/CFT compliance into job descriptions and performance evaluations of key staff
- Appropriate and periodic training for all key staff
- Means for senior management to test and validate independently the development and operation of suitable risk and management processes and related internal controls
- Measures for identifying complex or unusually large patterns of transactions which do not demonstrate any apparent economic or lawful purpose or which are unusual with regard to business patterns or known customer resources
- Policies, processes and procedures for communicating to employees the bank's written system of internal controls
- Policies, processes, procedures and conditions for entering into business relationships prior to effecting any required verifications.

Processes should also be developed for:

- Determining a bank's risk tolerance level
- Ensuring that the risks can be managed before entering into, or maintaining, business relationships or offering products or services associated with excessive ML/TF risks
- Ensuring that business relationships are not established when the ML/TF risks cannot be managed.

10. Governance

Banks should embed the framework for preventing and forestalling ML/TF in their system of governance, ensuring full commitment from their senior management and board of directors. A culture of AML/CFT compliance should be promoted as a core value, with mechanisms in place to communicate any actual or potential ML/TF risks speedily throughout the bank.

Senior management is responsible for overseeing the AML/CFT regime, identifying deficiencies and taking swift corrective action. Senior management must, therefore, put mechanisms in place for ML/TF issues to be brought to their attention in a timely and complete manner. They should also allocate responsibilities for establishing and maintaining AML/CFT controls and monitoring the effectiveness of these. They must further ensure that MLROs are adequately resourced to execute their responsibilities.

Senior management is also required to have a means of independently verifying that risk management processes are developed which reflect the bank's risk profile. They should ensure that the staff who undertake this verification have sufficient independence, seniority, knowledge and expertise to assess:

- The adequacy of the bank's AML/CFT's controls for addressing identified risks
- The effectiveness of the bank's staff in implementing controls
- The effectiveness of the bank's compliance oversight functions.

11. Money Laundering Reporting Officer (MLRO)

What is the role of an MLRO?

A money laundering reporting officer (MLRO) is a senior manager responsible for ensuring that the bank complies with key AML/CFT legislation and adheres to established policies, procedures and processes. An MLRO should serve as the liaison between the bank and the FIA with respect to AML/CFT compliance, in particular reporting suspicious activities.

The MLRO is responsible for receiving and analysing internal suspicious activity/transaction reports (SARs/STRs) and for filing these with the FIA where applicable (see section 0 below).

To be effective, the MLRO should:

- Have adequate knowledge of the relevant AML/CFT legislation
- Function independently and be given full access to the bank's records
- Intricately understand the bank's operations and business lines, as well as its products and services.

A bank's Compliance Officer may also act as its MLRO. However, the FSC's approval must first be sought for this.

12. Customer Due Diligence / Enhanced Customer Due Diligence

What is customer due diligence?

Customer due diligence (CDD) and enhanced CDD (ECDD) refer to the set of procedures a bank must undertake in order to:

- understand who its customers are
- ensure that customers are who they say they are
- determine the level of ML/TF risks that customers pose.

Why should banks conduct CDD?

CDD is a key measure in preventing customers from misusing banks for ML/TF purposes. Good CDD should provide enough knowledge of their customers for banks to establish the types of transactions their customers may engage in. It also enables banks to ascertain who owns or controls an account or the funds associated with a transaction. This helps identify where a transaction or activity deviates from the customer's norm and whether there are legitimate grounds to suspect the customer of ML/TF activities.

When should a bank conduct CDD?

- When setting up business relationships with a customer
- When effecting an occasional or one-off transaction which involves funds of or above $15,000 (although banks can impose their own lower thresholds depending on the risks involved)
- When ML/TF is suspected (irrespective of any threshold amount)
- When the relationship or transaction presents a higher than normal risk
- When there is any doubt about any information provided by the customer for identification or verification purposes
- On a periodic, ongoing basis.

Steps for conducting CDD

(i) Identify the customer

This entails gathering and recording information about the customer, such as name, date of birth, gender, nationality, address and place of employment.

(ii) Verify the customer's identity

This entails gathering evidence (reliable and independent information, data and/or documentation) to prove that customers are who they say they are and have provided true and accurate information.

(iii) Obtain details of the purpose or intended nature of the business relationship or transaction

This entails gathering information on the reasons why a customer wishes to carry out a specific transaction, or the type of business transactions the customer intends to engage in. For example, are they establishing a bank account to facilitate international business transactions or initiating a wire transfer to purchase a home?

(iv) Understand the customer and their circumstances

This entails gathering information on the source of the customer's wealth and funds, the size and volume of their business and the nature and level of their transactions. This may include details of any assets the customer owns, the proceeds of assets sold and family inheritances. It will also look

at the types of transactions that the customer intends to undertake and the jurisdictions the customer intends to engage with using banking services. For example, where a customer intends to conduct international business transactions, the bank may request information on the types of transactions, the types of people the company does business with, the expected value of the transactions and the frequency with which the customer intends to engage in these. Banks should also seek to ascertain whether the customer is a Politically Exposed Person or may have links to illegal activities.

What if the customer is a legal person or arrangement?
Where the customer is, say, a company, partnership or trust, the identification and verification process is more extensive.

Steps for conducting CDD

(i) Identify and verify the legal person or arrangement as a customer

This entails gathering and recording information on the legal person or arrangement, including;

- Name, legal type, place and date of incorporation/formation and relevant registration numbers
- Name, date and country of establishment of a legal arrangement
- Mailing and physical address of the customer's registered agent or trustee
- Nature and types of business activities and the place where these activities are carried out
- Nature and purpose of a legal arrangement
- Whether the legal person/arrangement is subject to regulation
- Ownership of the legal person
- Details of any group the legal person is a part of, including ownership of the group (specific to a legal person)
- Details of the structure, including any underlying companies, as well as beneficiaries, charitable objects and related matters (specific to legal arrangements).

(ii) Identify and verify the ultimate beneficial owners of the legal person

This entails gathering information on the beneficial owners of the company or partnership. CDD should be conducted on the beneficial owners as if they were individual customers of the bank.

(iii) Identify and verify the controllers of the legal person or arrangement

This entails gathering information on persons responsible for managing the business activities of the legal person (such as directors, managers and general partners) or persons that may have influence or voting rights as regards the board of directors or the activities of the legal person. This extends to persons that establish and act in relation to legal arrangements, such as trustees, settlors or protectors. CDD should be conducted on these as if they were individual customers of the banks.

What if a person is acting on behalf of another person?
In this case, irrespective of whether the ultimate customer is an individual or a legal person/arrangement, the bank is responsible for undertaking CDD both on the customer and the person purporting to act on their behalf.

The bank must also verify that the person purporting to act on behalf of the customer is authorised to do so. They may ask for evidence that the person has been given power of attorney or, where the customer is a legal person, documentation that the person has the authority to act on its behalf.

What methods can a bank use for verification?

Banks may use documentation or other methods to verify customers' identities and the purpose of a transaction. The suggestions below are not an exhaustive list. Banks should apply verification according to the risks posed and must not use it to stifle business relationships by asking for too much.

(i) Individuals

- Government-issued photo identification (e.g. passport, driver's licence, national identity card, work permit card, voter's registration card, student identification card and national insurance card)
- Copies of utility bills and bank statements
- Searches against voter registration lists and telephone directories
- Verification of employment through calls to employers or job references
- Consultation engagement letters
- Checks on public registers or private databases
- Electronic verification databases.

(ii) Legal persons

- Certificate of incorporation
- Constitutional document (e.g. Memorandum and Articles of Association)
- Partnership agreements
- Register of directors/members
- Trade/regulatory licence
- Ownership structure chart
- Organisational structure chart
- Business plan/director statement of business activities
- Financial statements (for legal persons already in existence)
- Public searches, including searches of independent databases
- Partner statement of business activities
- Business brochure.

(iii) Legal arrangements

- Trust or foundation documents
- Documentation confirming settlors and trustees
- Regulatory status of trustee (where applicable).

Timing of verification

Banks must verify a customer prior to, or at the time of, establishing a business relationship or engaging in a one-off transaction. However, there may be extraordinary circumstances where verification will have to be conducted after the establishment of a relationship and where it is essential not to interrupt normal business. In such an instance, the bank must verify the customer's identity within 30 days of establishing the business relationship and must ensure that ML/TF risks are effectively managed.

Banks may manage ML/TF risks by, for example, limiting the value or number of transactions in which the customer may engage or restricting the types of banking services which the customer may utilise. Banks may also give a senior officer responsibility over the account, or exercise enhanced scrutiny of transactions during the period where verification has not been completed.

Banks should exercise caution when establishing a relationship without completing verification, ensuring that there is no suspicion of ML/TF and the customer is not seeking to circumvent CDD.

What happens if a bank cannot verify the customer's identity within 30 days?
In this case, the bank should notify the FIA at least seven days before the end of the 30 days describing the circumstances that were essential not to interrupt the normal conduct of business, and saying why it cannot verify the identity within 30 days. The FIA may within its discretion grant the bank an extension of no more than 30 days. Where a bank is unable to complete the verification process of a customer it should a) terminate the business relationship; b) submit a suspicious transaction report to the FIA; c) submit a report to the FIA indicating the customer's non-cooperation in the provision of the required CDD or ECDD.[2]

What should a bank do once it has obtained relevant CDD information?
Banks should use the CDD information to assess the ML/TF risks associated with a proposed business relationship or transaction, develop a customer risk profile and determine the level of risk mitigation measures to be applied. The risk profile should establish characteristics that would be the norm for a customer or category of customers.

Application of CDD measures
Once an appropriate risk profile has been established, the bank should implement CDD measures based on the level of risk.

(i) What kind of CDD measures can be implemented where a customer is low risk?
In this case, the bank may use simplified CDD measures, as below.

- Fewer elements of customer identification data (e.g. one means of verification where the bank may normally require two)
- Simplified identity verification procedures, e.g. verification after the business relationship is established
- Not requiring specific information or measures to understand the purpose and intended nature of the business relationship (these may be inferred from the type of transactions or business relationship)
- In the case of an existing business relationship, less frequent customer identification updates (e.g. every four years as per the AMLTFCOP)
- Reduction in the degree and extent of ongoing monitoring and scrutiny of transactions, based on a reasonable monetary threshold.

(ii) What are enhanced customer due diligence (ECDD) measures and when should they be applied?
Where a customer poses a greater level of ML/TF risk, enhanced customer due diligence (ECDD) refers to the additional steps required to limit or manage the risk. High-risk customers include politically exposed persons (PEP), persons from jurisdictions considered to pose significant ML/TF risk, persons associated with high risk activities or those who engage in frequent complex transactions.

For these persons, the bank must gather sufficient information to gain amplified knowledge of the customer and their transactions. Senior management should be responsible for deciding whether

[2] AMLTFCOP Section 23(2)(2C)

to enter into, continue business relationships with, or conduct transactions on behalf of, these customers.

ECDD includes the following:

- Obtaining and corroborating additional identifying information from a wider variety of sources or from more robust sources
- Carrying out additional searches (e.g. verifiable adverse internet searches)
- Verifying the sources of the customer's funds and wealth
- Seeking and verifying additional information about the purpose and intended nature of the business relationship or transaction
- Further verification where appropriate.

Ongoing CDD

Once a business relationship is established, banks have an obligation to ensure CDD is carried out on an ongoing basis. This should allow banks to identify and update changes in customer profiles (e.g. behaviour, use of products, frequency of transactions, amount of money involved, sources of deposits and jurisdictions involved). It may lead to new or enhanced CDD measures.

Banks are required to update CDD information for high risk customers at least once a year and for all other customers at least once every four years. Beyond this, banks should seek to screen their customers periodically to detect PEPs and those associated with illegal activities, and to check names against known or suspected terrorist and sanctions lists whenever these change.

Ongoing monitoring

An essential way of identifying potentially suspicious transactions (executed or proposed) is transaction monitoring. Following CDD and the development of customer profiles, banks should have an understanding of customers' normal and reasonable activities. They must implement systems that monitor transactions to identify potentially suspicious activity that does not fit expected behaviour, e.g. deviates from the usual pattern of transactions or varies greatly from activity that occurs with customers with similar profiles.

While this might indicate suspicious activity, it may also signal that the customer's purpose for the banking relationship has changed. This would warrant updating the customer's profile.

Monitoring should be carried out continuously, either in real time (i.e. when transactions are about to take place or as they are taking place) or post-event (i.e. through a retrospective review of transactions).

Banks' systems must be able to flag transactions and/or activity that do not fit a customer's profile (e.g. spanning jurisdictions with which the customer has no connections). They should allow for senior management to review the transactions promptly and take appropriate action.

A flagged transaction does not in itself mean suspicious activity. In reviewing it, senior management should gather information, including from the customer or other reliable sources, and consider other factors (e.g. a commercial customer may increase cash deposits because they cannot use electronic payments after a natural disaster).

Transaction monitoring systems may be manual or automated depending on banks' business activities, size, number of customers and volume of transactions. Where automated systems are used, banks should

understand their operating rules, verify their integrity on a regular basis and check that they take into account the identified ML/TF risks.

The level of transaction monitoring should be relative and proportionate to the level of risk identified, with enhanced measures in higher risk situations and reduced frequency and intensity for lower risk customers.

The systems and criteria used to determine the level of monitoring should be reviewed regularly to ensure they are in line with the banks' AML/CFT risk programme. As criminals find new ways to misuse banking facilities, banks must expand their systems to include new indicators of suspicious activities and illegal trends, which may be identified in typologies reports or from other reliable sources.

What if a bank cannot apply appropriate CDD measures, including verification?
In this case, the bank should not enter into the business relationship (in the case of a new customer) or carry out the transaction (in the case of one-off transactions). Where a business relationship already exists, the bank should seek to terminate that relationship. Consideration should also be given to filing a SAR.

Are there any relationships a bank is prohibited from establishing?
If in carrying out CDD a bank determines that an entity is a shell bank, in the case of a new customer the bank should not enter into a relationship with the shell, or should terminate its relationship with the shell where the relationship already exists.

A bank should not enter into a relationship with a customer that requests anonymity or maintains anonymous or fictitiously named accounts.

13. Wire Transfers

Wire transfers can move large funds and payments quickly around the world, making them attractive to terrorists and criminals who want to move illicit funds or funding for illicit activities across jurisdictions. To prevent and detect their misuse, banks must ensure that wire transfers are traceable by collecting and maintaining all originator and beneficiary information.

Cross-border wire transfers
Whether acting as payment service provider for the payer, payee or an intermediary, banks should accompany cross-border wire transfers with the required information.

(i) Payer's payment service provider

A bank transferring funds from a customer should accompany each transfer with the below.

- Full originator information, which includes:
  - The name of the customer
  - The account number of the customer or, if the customer does not have an account, a unique identifier that allows the transaction to be traced back to the customer
  - The customer's address
  - The customer's date and place of birth or customer identification number or national identity number.
- Full beneficiary information, which includes:
  - The name of the payee
  - The account number of the payee or, if the payee does not have an account, a unique identifier that allows the transaction to be traced back to the payee.

Where a single payer makes several cross-border transactions which are bundled in a batch file for transmission, the bank does not have to include full originator and beneficiary information for each transfer as long as the batch file contains this and each transfer contains the payer's account number or a unique identifier that allows the transaction to be traced back to the customer.

Banks must ensure that full originator information is verified. Where the transfer is from an established customer's account, verification is deemed to have taken place if the customer's identity was verified at the time of account opening. For one-off transactions, originator information is deemed to have been verified if the transaction does not exceed $1,000 or is not connected to several bunched transactions not exceeding $1,000 and if the customer is not suspected of ML/TF or other financial crime.

(ii) Payee's payment service provider

Where a bank is receiving funds where its customer is the payee, the bank should:

- Verify the identity of the payee, if not previously identified
- Verify that the transfer is accompanied by full originator information and beneficiary details
- Ensure it has systems in place (including post-event or real-time monitoring) to detect missing or incomplete originator information and/or beneficiary details.

When it becomes aware that the full originator information and/or beneficiary details are missing or incomplete, a bank should already have risk-based processes and procedures for determining

whether it should request the full originator and/or beneficiary information, reject the transfer or take follow-up action as directed by the FIA or the FSC.

Missing or incomplete information is a factor in assessing whether the transfer of funds or any related transactions should be reported to the FIA as suspicious for ML/TF.

(iii) Intermediary payment service provider

Where a bank's customer is neither the payee nor the payer, the bank must ensure that the relevant originator and beneficiary information are retained with the transfer unless prevented by technical limitations. Where technical limitations exist, the intermediary bank must keep a record of all the information that accompanied the transfer.

An intermediary bank should have risk-based procedures in place to identify where originator or beneficiary information are missing or incomplete and to determine its next steps.

Domestic wire transfers

For domestic wire transfers, banks acting as the payer's service provider should ensure the transfers are accompanied by complete originator information.

14. Correspondent Banking Relationships

Banks may engage in correspondent banking relationships and provide respondent banks with products and services to offer their own customers (where the respondent banks do not provide these themselves). These may include cash management (e.g. interest-bearing accounts in various currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.

Given the nature of the relationship, the correspondent bank must ensure it is not facilitating ML/TF by first confirming that the respondent bank has appropriate measures in place to prevent and forestall this. Banks should not have correspondent banking relationships with shell banks and should ensure that respondent banks do not permit their accounts to be used by shell banks.

Essentially, a respondent bank should be treated as a correspondent bank's customer. As such, correspondent banks should do the following:

- undertake CDD/ECDD of a respondent bank to understand its business fully (including its activities, customer base and products and services), its ownership, the jurisdiction(s) to which it is exposed, its reputation, whether it is subject to a regulatory regime, and whether it has been the subject of any ML/TF or financial crime investigation or enforcement action
- understand the purpose of the services to be provided to the respondent bank
- be satisfied that the respondent bank has adequate and appropriate AML/CFT controls
- obtain senior management approval prior to establishing the new relationship
- undertake senior management reviews of the relationship at least every year to ensure continued compliance
- ensure that each bank's ML/TF measures are fully understood and properly recorded
- undertake ongoing monitoring to identify any changes in activities.

Where it gives a respondent bank's customers direct access to its services via payable-through accounts, a correspondent bank should ensure the respondent bank has undertaken appropriate CDD/ECDD of the customers and is able to provide this documentation on request.

15. Reporting a Suspicion

Banks have an obligation to report any ML/TF suspicions to the FIA. This means they must have processes and procedures which allow employees, including senior management, to promptly report their knowledge or suspicion of ML/TF to the bank's MLRO. This also applies to any attempted activity, transaction or customer relationship that the bank has refused.

Banks' internal controls must say how an employee should report a suspicious activity and to whom. An internal SAR log should be maintained and should indicate the date the suspicious activity took place, the date the report was made, the circumstances surrounding the activity and the outcome of the investigation.

Bank MLROs are responsible for investigating internal SARs/STRs, determining whether there is sufficient information to support the suspicion and whether the suspicion should be reported to the FIA, and if so, filing the report with the FIA. If a report to the FIA is not filed, a record should be made of the suspicious activity along with the reason for not filing.

Detailed guidance on filing SARS/STRs can be found within the Guidance Note on Suspicious Transaction and Suspicious Activity Reports[3] on the FIA's website.

Once a SAR/STR has been filed with the FIA, banks should take swift action to mitigate the risk of being abused by that customer for criminal purposes. This may mean reassessing the risk entailed in the business relationship and escalating the relationship to management.

[3] https://www.fiabvi.vg/Portals/0/Guidance%20Note_20190913104802.pdf?ver=2019-09-13-145053-917

16. Indicators of Suspicious Activity

How can a bank tell if an activity is suspicious?
Below is a list of indicative activities. These examples are not comprehensive. Each bank must consider its own operations, ML/TF risks and customer profiles in determining what activities to consider suspicious and communicate these to employees, including through training.

- Customers are reluctant to provide identity details, disclose source of funds or cooperate in any way
- Transaction sizes and frequencies are inconsistent with customers' normal activities or profile
- A series of transactions is structured just below the regulatory threshold for due diligence identity checks
- Payments are made to or from jurisdictions with which customers do not appear to have any connections, without any reasonable explanation
- Customers engage in transactions and business relationships with insufficient commercial rationale
- Large withdrawals are made from a previously inactive bank account or an account that recently received a large, unexpected deposit or transfer of funds
- The pattern of transactions since the business relationship was established changes
- There are inconsistencies in the information provided by customers
- Customers try to rush through a transaction without providing the requested information
- Customers are unable to explain the source of income satisfactorily or provide contradictory statements
- There are frequent and unexplained movements of funds to and between different persons in different jurisdictions
- There are transfers of large sums to, or numerous transactions with, people in high risk jurisdictions or those with known corruption, organized crime or drug production/distribution
- Customers who offer false or fraudulent identification, whether evident from the document alone, from its lack of connection to the customer or from its context with other documents (e.g. use of identification cards or documents in different names without reasonable explanation)
- Transactions are not consistent with the customer's business activities
- A person is unable to demonstrate their authority to act on behalf of another person
- Customers consistently pay in or deposit cash to cover requests for money transfers, bankers drafts or other negotiable instruments
- Large numbers of individual deposits or transfers to one bank account are made with no apparent explanation
- There is an unexpected and sudden full loan repayment by a customer with credit issues
- Large cash payments for outstanding credit card balances
- Transaction patterns appear consistent with the generation of criminal proceeds, e.g. drug trafficking, corruption, illegal immigration, human trafficking and people smuggling

- 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).

Banks must conduct a review to confirm whether the transaction constitutes a suspicious activity to be reported or requires an update of the customer's profile.

17. Record Keeping

Maintaining legible, accessible records about its business dealings is key to any bank's AML/CFT programme. Record keeping minimises ML/TF risks by ensuring that a transaction's history can be traced if needed. It also enables banks to show compliance with AML/CFT requirements and legislation.

Banks should maintain all transaction records in sufficient detail to allow for later reconstruction. They should also maintain any records obtained through the CDD process, and all SARs filed internally and externally.

Transaction records
For each transaction, the details below should be recorded:

- Customer name and address
- Currency and amounts involved
- Name and address of the beneficiary of the transaction
- Account number, account holder's name or other identifier if the transaction involves a customer's account
- Transaction date
- Nature of the transaction, including the form in which funds were offered and paid out, where applicable
- Account files and business correspondence
- Any other documentation or details that would allow the transaction to be properly understood.

CDD records
The information and documentation below obtained during the CDD process should be retained.

- Customer information, such as name, address and, in the case of a legal person, controller and beneficial ownership information
- Copies or records of official identification documentation
- Account files and business correspondence (including any communication used to establish the nature of the customer's business or transaction)
- The results of any analysis to understand the nature and purpose of any complex or unusual transaction
- The results of any risk assessments.

SARs/STRs
The information and documentation below in relation to SARs/STRs made should be retained:

- Any internal SARs/STRs made within the bank, along with supporting documentation
- The MLRO's decisions, along with the basis of these, with respect to any SARs/STRs
- Records of any SARs/STRs filed with the FIA, along with any feedback from the FIA.

Period and format of retention
Banks are required to maintain all records for at least five years from the date a one-off transaction was completed or a business relationship was terminated. Records may be:

- Original documents

- Certified copies of original documents, including scanned documents
- Microform or microfiche
- In computerised or electronic format.

A bank's record keeping obligations also extend to any records required by the BTCA, FSCA, Regulatory Code, AMLR and AMLTFCOP, to its internal control policies and procedures and to any AML/CFT staff training as highlighted in section 18 of these guidelines.

18. Employee Screening and Training

Employee screening

To ensure high standards, banks should have screening programmes in place when hiring. This means conducting thorough background checks and assessing 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 functions.

This is particularly important where staff are responsible for implementing AML/CFT controls, whether in compliance or in front-line functions. Staff vetting should reflect the ML/TF risks to which individual staff are exposed and not focus only on senior management.

Potential conflicts should be minimised as far as possible by ensuring staff that have been assigned AML/CFT responsibilities only perform AML/CFT compliance functions. Where this is not viable and employees have both line and compliance functions, compensation should not be based solely on business performance but should also consider AML/CFT performance, to minimise the risks of employees negating AML/CFT responsibilities.

Banks must inform the FSC and the FIA if an employee's contract is terminated for lack of AML/CFT compliance or lack of probity.

Employee training

Banks' duty of vigilance means their employees must be trained in the ML/TF risks relating to the bank's business activities and in their obligation to protect the bank from ML/TF, and must be kept up to date with the latest legal and regulatory obligations and internal controls.

AML/CFT training should not be a one-time event but should be continuous, occurring at least once a year. Temporary and contracted employees should also receive training, as should third parties to whom AML/CFT responsibilities have been outsourced.

Training should be tailored to employees' responsibilities and be complemented by AML/CFT information and updates for relevant staff.

An efficient training programme should ensure that staff understand the following:

- their compliance obligations under relevant AML/CFT legislation and international standards
- the consequences of non-compliance (including tipping off and its consequences)
- the vulnerabilities of the bank's products and services
- the bank's ML/TF risks
- the importance of CDD, risk assessments and record keeping
- how to recognise, handle and report suspicious transactions and activities
- the bank's AML/CFT policies and procedures
- identification of the MLRO and his or her roles and responsibilities.

Employee Testing
Banks should assess employees' learning from the training via appropriate testing. Where staff cannot demonstrate the expected knowledge, banks should monitor their compliance with AML/CFT controls and take appropriate steps.

Training records
Banks are required to maintain a record of all staff training, indicating the date, nature, topics and duration and the names of trainees.

19. Internal Audits

To ensure that their AML/CFT programmes function as intended, banks should undertake internal audits. An internal audit checks whether a bank has put AML/CFT processes and procedures in place and how effectively these are being applied.

The audit entails sample testing of the bank's records and conducting staff interviews. It may verify whether CDD measures are being implemented, risk ratings applied, relevant factors considered in risk assessments and flagged transactions reviewed. An audit should also assess compliance with relevant laws, best practices and international standards.

Banks must ensure the independence of the audits. While this does not necessarily require an internal audit to be conducted by a third party, any staff undertaking it must not have been involved in the areas that are being audited. A bank must determine whether the nature, size and complexity of its business and risks mean the audit would be better conducted in-house or by a third party.

Following an internal audit, a report should be provided to the bank's Board of Directors, identifying any deficiencies. Appropriate measures should be put in place to address these.

20. A Final Reminder

Banks must play their full part in helping the Virgin Islands to detect, prevent and combat ML/TF activities by implementing the policies and procedures required by the Territory's AML/CFT regime.

While not a substitute for the Territory's AML/CFT laws, these guidelines should aid banks in effectively assessing their ML/TF risks, mitigating those risks and preventing the misuse of their facilities for criminal purposes.

The FSC expects banks to have read them and to apply them appropriately.