BANK OF GUYANA

SUPERVISION GUIDELINE NO. 1

ISSUED UNDER THE AUTHORITY OF THE ANTI- MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM (AML/CFT) ACT 2009

FOR
Payments Service Providers (PSP)

Bank of Guyana
Date: March 17, 2023

Table of Contents

GLOSSARY

Acronyms/Terms	Definition
AML/CFT	Anti-Money Laundering and Countering the Financing of Terrorism
BOD	Board of Directors
BOG	Bank of Guyana
Beneficial owner	Beneficial owner refers to the natural person(s) who ultimately own(s) or control(s) and/or the natural person on whose behalf a transaction is being conducted.It also includes those persons who exercise ultimate effective control over a legal person or arrangement.
Business relationship	Means any arrangement between the financial institution and the applicant for business whose purpose is to facilitate the carrying out of transactions between the parties on a 'frequent, habitual or regular' basis and where the monetary value of dealings in the course of the arrangement is not known or capable of being ascertained at the outset.
CAP	Customer Acceptance Policy
CDD	Customer Due Diligence
CIP	Customer Identification Procedures
CSR	Customer Service Representative
DFA	Dealers in Foreign Currency (Licensing) Act 1989, amended 1995
Designated Institution	Means any institution designated in terms of the Anti-Money Laundering Act 2009 for purposes of implementing statutory AML/CFT obligations prescribed therein and includes an individual or entity carrying on the business of a Money Transfer Agency or a PSP.
EDD	Enhanced Due Diligence
Egmont Group	The Egmont Group is a united body of FIUs. The Egmont Group provides a platform for the secure exchange of expertise and financial intelligence to combat ML/TF. This is especially relevant as FIUs are uniquely positioned to cooperate and support national and international efforts to counter terrorist financing and are the trusted gateway for sharing financial information domestically and internationally in accordance with global AML/CFT standards.
EU	European Union
FATF	Financial Action Task Force
FIU	The Financial Intelligence Unit (FIU) of Guyana is an autonomous body responsible for requesting, receiving, analyzing and dissemination of suspicious transaction reports and other information relating to money laundering, terrorist financing or the proceeds of crime. It was established and operates within the ambit of the AML/CFT Act 2009 and its Regulations.
FSRB	FATF Style Regional Body

Acronyms/Terms	Definition
HT	Human Trafficking is the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs.
HS	Human Smuggling (used interchangeably with People Smuggling)
IMF	International Monetary Fund
KYA	Know Your Agent
KYC	Know Your Customer
KYE	Know Your Employee
NPS	National Payments System
ML	Money Laundering
PSP	Payment Service Provider
PS	People Smuggling which is also referred to as Human Smuggling is the facilitation, transportation, attempted transportation or illegal entry of a person or persons across an international border, in violation of one or more countries' laws, either clandestinely or through deception, such as the use of fraudulent documents.
PEP	Politically Exposed Person. This refers to a person holding prominent public office and includes spouse, close relative or associate of such person. Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a local or foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc., including their spouses, close relatives and associates or legal persons and arrangements controlled by such persons.
PF	Proliferation Financing is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, 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.
Suspicious Transaction:	A transaction which is inconsistent with a customer's known, legitimate business or personal activities or normal business for that type of account or that lacks an obvious economic rationale. It is a transaction which is unusual because of its size, volume, type or pattern or otherwise suggestive of known money laundering methods or terrorism.

Acronyms/Terms	Definition
SOF	Source of Fund: Refers to the origin of the particular funds or assets which are the subject of the business relationship between the firm and its client and the transactions the firm is required to undertake on the client's behalf (e.g. the amounts being invested, deposited or remitted).
SOW	Source of Wealth: Refers to the origin of the entire body of wealth (i.e. total assets) of the client.
STR	Means Suspicious Transaction Report or includes an attempted transaction.
TF	Terrorist Financing – means willfully providing or collecting funds, by any means, directly or indirectly, with the unlawful intention that they should be used or in the knowledge that they are to be used in full or in part – (a) to carry out terrorist acts; (b) a terrorist organization; (c) by an individual terrorist.
TIN	Taxpayer Identification Number
UN	United Nations

PART 1 – INTRODUCTION

1. This Guideline is issued in accordance with section 22 (2) (b) of the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Act 2009. The Guideline provides guidance on what is required to implement an adequate AML/CFT compliance risk-based framework within each payments service provider (PSP).

2. Money laundering (ML) and the financing of terrorism prevention should not be viewed in isolation from a PSP's other business systems, but rather as an integral part of its overall risk management strategies. Consequently, it is essential that the Board of Directors (BOD) and senior management of a PSP ensure that policies, procedures and monitoring mechanisms are in place to prevent the PSP from being used as a conduit for ML and terrorist financing (TF).

3. Effective enforcement to deter ML and the financing of terrorism should therefore enhance the integrity of the financial system and reduce incentives for the commission of crime within a jurisdiction.

PURPOSE

4. This Guideline seeks to provide PSPs with the broad parameters to aid compliance with:

- ✓ the AML/CFT Act 2009 and its Amendments;
- ✓ AML/CFT Regulations 2010 and the Amendments; and
- ✓ the standards of the Financial Action Task Force (FATF) [1]

[1] The FATF was established by the G-7 Summit in Paris in July 1989. In 1990, it issued its Forty Recommendations setting out the basic framework for AML efforts. The Forty Recommendations were first revised in 1996 and most recently in 2012 to take into account changes in money laundering methods, techniques and trends that have developed as counter-measures to combat this crime and can be viewed at www.fatf-gafi.org.

5. It also sets out expectations of the Bank of Guyana (BOG) in relation to the minimum standards for AML/CFT practices by all PSPs.

WHAT IS MONEY LAUNDERING?

6. ML means conduct which constitutes an offence as described under section 3 of the AML/CFT Act 2009. "A person commits the offence of ML if he knowingly or having reasonable grounds to believe that any property in whole or in part directly or indirectly represents any person's proceeds of crime…"

7. There is no one single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g., properties, cars and jewelry), to passing money through a complex international web of legitimate businesses and "shell" companies. In the case of drug trafficking and other specified serious offences[2] cited under the AML/CFT Act 2009, the proceeds usually take the form of cash which needs to enter the financial system.

8. Despite the variety of methods employed, ML is generally accomplished in three stages, which may comprise numerous transactions by the launderers that could alert a financial institution to criminal activity. These stages are placement, layering and integration:-

   (i) **Placement**: refers to the placing of "dirty money" or unlawful cash proceeds into the financial system without arousing suspicion for example via deposits and purchases of monetary instruments such as cheques, or bank drafts.

   (ii) **Layering**: refers to the movement of the money, often in a series of complex transactions crossing multiple jurisdictions designed to disguise the audit trail and provide the appearance of legitimacy. These transactions may include purchasing investment instruments, insurance contracts, wire transfers, money orders, travellers' cheques and letters of credit.

---

2 See Second Schedule – AML/CFT Act 2009

(iii) **Integration**: refers to the attempt to legitimize wealth derived from criminal activity. The illicit funds re-enter the legitimate economy by way of investments in real estate, luxury assets and business ventures, until the laundered funds are eventually disbursed back to the criminal.

APPLICABILITY OF THE GUIDELINE

9. This Guideline applies to entities licensed under the:-

- National Payments System Act 13 of 2018 and Regulations:
  - Agents (9 of 2019
  - Electronic Money (8 of 2019
  - Electronic Funds Transfer (7 of 2019)
  - Oversight (10 of 2019)

10. All PSPs should ensure that, at a minimum, this Guideline is also implemented in their branches/subsidiaries.

11. PSPs are required to assess the AML/CFT regime existing in any jurisdiction in which its branches and/or subsidiaries operate. Where the branch operates in an overseas jurisdiction and the AML/CFT laws and requirements in that jurisdiction exceed the standards required by Guyana laws, the branch should adhere to the requirements in the overseas jurisdiction.

12. Where Guyana's AML/CFT requirements exceed those in the host jurisdiction, subsidiaries and branches of PSPs in those jurisdictions should apply the higher standard to the extent that the host jurisdiction laws and regulations permit.

13. PSPs with non-deposit-taking subsidiaries, must take steps to ensure that there is access to information regarding the operations, and activities of these subsidiaries locally in order to ensure that such subsidiaries are compliant with the AML/CFT laws, regulations, and Guidelines.

14. PSPs are required to pay particular attention that the principle stated in section 22 (2) of the AML/CFT Act 2009 is observed with respect to branches and subsidiaries in countries which do not or insufficiently apply the FATF recommendations.

Payments Service Providers (PSPs)

15. Payment services refer to the whole of services that are associated with cash deposits and withdrawals, execution of payment transactions, issuing or acquisition of payment instruments, the provision of money transfer services or any other service functional to the transfer of money and includes the issuance of electronic money and electronic funds transfers but does not include the provision of solely online or telecommunication services or network access.

16. PSPs can easily be used by criminals to launder proceeds of crime or to channel funds destined to fund terrorist activities.

17. PSPs provide a conduit for dirty funds to be cleansed and to be moved away from their source of origin. In some cases, PSPs maintain accounts or ongoing business relationships with certain customers while in many cases PSPs also transact with walk-in clients on occasional or once-off basis.

18. The AML/CFT Act of2009 and this guideline seek to ensure that PSPs put measures in place to deter as well as detect transactions that involve or are suspected to involve money laundering and financing of terrorism. PSPs should develop suitable mechanisms for enhanced monitoring of transactions suspected of having terrorist and/or ML links.

19. PSPs refer to entities that provide a payment service licensed under the National Payments System Act 2018.

20. All PSPs are required to implement an AML/CFT compliance program which must be commensurate with the risks presented by the PSPs location, size, and the nature and volume of the services it provides. The purpose of the AML compliance program is to prevent money laundering issues. It is the responsibility of each PSP to have policies in place to prevent ML and TF in line with the FATF Forty Recommendations.

PART 2 - LEGISLATIVE AND REGULATORY FRAMEWORK

LEGISLATIVE

21. The AML/CFT Act 2009 and its Amendments provide the legal framework for detecting and preventing ML and TF.

- ✓ Section 22 (1) (a) of the AML/CFT Act 2009 mandates the Governor of the BOG as the Supervisory Authority of PSPs.

- ✓ Section 9 of the AML/CFT Act 2009 speaks to the establishment and functions of the Financial Intelligence Unit (FIU).

- ✓ Sections 15 (2) to (6) and (8), 16, 18, 19 and 20 of the AML/CFT Act 2009 refers to the following:-

  - o identifying and verification of a customer's identity;
  - o reporting obligations;
  - o appointment and duties of a Compliance Officer;
  - o attention to and reporting, if suspicious, large business transactions which are unusual and complex, as well as transactions which have no apparent economic or visible lawful purpose and are inconsistent with the profiles of the persons carrying out such transactions;
  - o making a suspicious transaction or a suspicious activity report to the FIU;
  - o record keeping; and
  - o training of employees in AML/CFT.

- ✓ Section 23 (1) outlines the sanctions available to the Supervisory Authority.

- ✓ Section 5 of the AML/CFT Act 2009 which speak to tipping off.

REGULATORY FRAMEWORK

22. The primary responsibilities of the BOG as a Supervisory Authority include:-

- ✓ reviewing the AML/CFT compliance programme of all PSPs to determine its adequacy and assess its compliance with applicable laws and Guidelines and AML/CFT measures consistent with FATF Recommendations to the extent that host countries laws and Regulations permit;
- ✓ issuing Guidelines,[3] circulars or recommendations as appropriate to aid compliance with AML/ CFT requirements;
- ✓ cooperating and sharing information promptly with the FIU, by providing assistance in investigations, prosecutions or proceedings relating to proceeds of crime, money laundering and terrorist financing. Sharing of information with the FIU as required for the purposes of AML/CFT; includes disclosing information to the FIU as soon as is reasonably practicable but no later than three working days after acquiring any information concerning suspicious transactions or activities that could be related to money laundering, terrorist financing or the proceeds of crime;
- ✓ taking regulatory action as stipulated in section 23 of the AML/CFT Act 2009, against those institutions regulated by it which fail to adequately comply with statutory AML/CFT obligations and Guidelines issued by the BOG;
- ✓ maintaining statistics concerning measures adopted and sanctions imposed under the AML/CFT Act 2009;
- ✓ developing standards and criteria applicable to the communication of suspicious activities that reflect other existing and future pertinent national and internationally accepted standards;
- ✓ ensuring that PSPs as it relates to their foreign branches/subsidiaries implement and enforce standards consistent with the AML/CFT Act 2009, Regulations 2010, guidelines or directives.

---

[3] Refer to Section 22 (1) of the AML/CFT Act 2009 and Section 13 of the AML/CFT Regulations 2010

SANCTIONS

23. Pursuant to section 23 of the AML/CFT Act 2009, regulatory actions[4] that could be taken by the BOG include:

the issuance of written warnings;

- ✓ compliance orders with specific instructions;
- ✓ suspension, restriction or revocation of licence;
- ✓ prohibiting convicted persons from gaining employment within the sector;
- ✓ requesting regular reporting from the PSP on the measures it is taking to comply with the law.

The BOG is required to inform the FIU as to the sanctions imposed and may publish its decision.

TIPPING-OFF

24. In accordance with section 5 of the AML/CFT Act 2009, it is an offence for employees, directors, officers or agents of a PSP to disclose that a suspicious transaction report (STR) or related information on a specific transaction has been reported to the FIU; or that an investigation into money laundering, terrorist financing or the proceeds of crime is impending/pending, and to divulge that fact or other information to another whereby the investigation is likely to be prejudiced.

25. In the event that a person is found guilty of tipping off he/she may, on summary conviction, be liable to a fine not exceeding one million dollars and to imprisonment for a term not exceeding 3 years.

---

4 Refer to AML/CFT Act 2009 –Section 23 (1)

LEGAL PROTECTION AND INDEMNIFICATION

26. Pursuant to section 11 of the AML/CFT Act 2009, when a suspicious transaction or suspicious activity report is made to the FIU, PSPs, their employees, officers, directors, owners or other representatives as authorized by law, are exempted from criminal, civil or professional liability action as the case may be, or for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, regardless of the result of the communication.

ENFORCEMENT OF THE GUIDELINE

27. Section 19 of the AML/CFT Regulations 2010 makes the failure to comply with the requirements of this Guideline a summary conviction offence. The Courts by Regulation 19 may also take account of the provisions of the Guideline in determining whether there has been compliance with the requirements of the AML/CFT Regulations 2010. PSPs are therefore advised to adopt the provisions of this Guideline and to implement the requisite internal systems and procedures.

PART 3 - KNOW YOUR CUSTOMER (KYC) AND CUSTOMER DUE DILIGENCE (CDD)

GENERAL

28. KYC and CDD are key elements in the fight against ML and TF. CDD procedures enable designated institutions to know /understand their customers and their financial dealings better, which in turn helps to identify unusual or suspicious transactions and to manage risks prudently.

Who is a Participant and who is a Customer?

29. In relation to PSP, a 'Participant' is defined as:

A party who is recognized in the rules of the system as eligible to exchange, clear and settle through the system with other participants as a direct participant or through the services of a directive participant,

A customer is any natural or legal person who uses the services or facilities of a payment service provider to execute a payment service."

KYC

30. PSPs should put in place KYC policies and procedures which incorporate the following key elements:

- Consumer Acceptance Policy;
- Consumer Identification Procedures; and
- Monitoring of Transactions

CUSTOMER ACCEPTANCE POLICY (CAP)

31. PSPs shall develop a clear CAP outlining explicit criteria for acceptance of customers. The CAP shall ensure that explicit guidelines are in place on the following aspects of customers relationships:

- No transaction shall be conducted in anonymous or fictitious name(s).
- PSPs shall not conduct any transaction where it is unable to apply appropriate CDD measures i.e. the PSP is unable to verify the identity and/ or obtain documents required due to non-cooperation of the customer or non- reliability of the data/information furnished.

32. In the event a customer is permitted to act on behalf of another person/entity, it must be clearly spelt out and supporting documents shall be furnished, showing that the person is duly authorized. The **beneficial owner** shall be identified and all reasonable steps taken to verify his/her identity.

33. PSPs shall prepare a profile for each new customer, where regular transactions or a continuing business relationship is expected, based on risk categorization. The customer profile may include information relating to customer's identity, address, occupation, nationality, etc. The nature and extent of due diligence will depend on the risk perceived.

CUSTOMER IDENTIFICATION PROCEDURES (CIP)

34. Customer identification means verifying his/her identity by using reliable, independent source documents, data or information. PSPs shall obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional. PSPs must be able to satisfy the BOG that due diligence was observed.

35. For customers who are natural persons, the PSPs shall obtain sufficient identification document/s to verify the identity of the customer, such as a valid national identification card, passport or the 'new' driver's licence.

For those customers who are legal persons, e.g., companies, clubs, societies and charities and legal arrangements, PSPs shall:

- ✓ verify the legal status (of the legal person) through proper and relevant official documents;
- ✓ obtain a letter of authorization, resolution or other acceptable and legally valid document from the entity showing that the person acting on behalf of the legal person or entity is properly authorized to so act;
- ✓ understand the ownership and control structure of the customer and determine who are the natural persons, who ultimately control the legal person/ beneficial owner(s).

36. Any natural person conducting the transaction on behalf of a legal person or entity shall be subjected to the same identification requirements as applied to a customer who is a natural person, i.e., identification documents of that person shall be obtained and verified.

37. In the case of a continuing business relationship, the PSP shall introduce a system of periodical updating of customer identification data.

38. When there is suspicion of ML or TF, or where there are reasonable grounds to doubt the accuracy or veracity of previously obtained information, the PSP shall apply EDD measures including verifying again the identity of the customer and obtaining information on the purpose and intended nature of the business relationship.

CUSTOMER EDUCATION

39. Implementation of KYC procedures requires PSPs to demand certain information from a customer which may be of a personal nature or which has hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. There is, therefore, a need for PSPs to prepare specific literature/ pamphlets, etc. which shall educate the customer of the objectives and necessity of the KYC policies. The front desk staff need to be specially trained to handle such situations while dealing with customers.

CDD REQUIREMENTS FOR PSPS

40. PSPs shall be required to undertake CDD measures when:

- ✓ establishing continuing business relations;
- ✓ carrying out occasional transactions above the applicable designated threshold limits;
- ✓ the PSP has doubts about the veracity or adequacy of previously obtained customer identification data;
- ✓ the transaction involves a PEP; or
- ✓ where the PSP has identified a particular customer or transaction as representing a high ML or TF risk, or where there is suspicion of ML or TF.

PSPs shall:

- ✓ verify the customer's identity and occupation using reliable, independent source documents, data or information;
- ✓ identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner. For legal persons and arrangements, PSP should understand the ownership and control structure of the customer; and
- ✓ obtain information on the purpose and intended nature of the business relationship; and conduct ongoing due diligence for customers that the PSP has an account with or has established a business relationship with.

41. A PSP is allowed to apply reduced or simplified identification measures where the risk of ML or TF is lower.

42. Where the simplified CDD measures are subject to certain conditions, it is necessary to verify that these conditions are satisfied, and where the exemption applies under a certain threshold, measures should be in place to prevent transactions from being split artificially to avoid the threshold. In addition, information beyond customer identity, such as customer location and purpose of the transaction, may be needed to adequately assess the risk. This will be an iterative process: the preliminary information obtained about a customer should be sufficient to determine whether to go further, and in many cases customer monitoring will provide additional information.

KNOW YOUR EMPLOYEE (KYE)

43. When recruiting staff, PSPs should conduct thorough background checks and assess the competency and probity of applicants to satisfy themselves that the staff they employ have integrity, and possesses 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.

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

45. Where a PSP has reasonable grounds to suspect that any of its employees may be involved in any form of illicit activity/transaction which are connected to the proceeds of crime it shall take the necessary action as stipulated by section 18(4) of the AML/CFT Act 2009.

46. The level of vetting procedures of staff should reflect the AML/CFT risks to which individual staff are exposed a n d not focus me rely on senior management roles. Steps should be taken to manage potential conflicts of interest for staff with AML/CFT responsibilities.

KNOW YOUR AGENT (KYA)

47. PSPs that use agents to facilitate the delivery of their services should be aware of the risks posed by such relationships. PSPs must ensure that they understand who the agent is, and that they are not criminals or criminal associates.

48. PSPs must ensure that due diligence is performed for each prospective agent as well as continuous monitoring of current agents to establish and maintain integrity in line with the NPS Regulation on Agents (9 of 2019), Part III, section 8 (1), .

MANAGEMENT OF AGENTS

49. It is important for PSPs to effectively monitor the activities of their agents to assess and address any potential risks which may arise from issues such as inadequate training, lack of internal control procedures, or poor individual judgment or performance as guided by NPS Regulation on Agents (9 of 2019), Part V section 17.

50. The degree and nature of such monitoring may depend on:

- ✓ the transaction volume of the agent;
- ✓ the monitoring method being utilized (manual, automated or a combination);
- ✓ outcomes of previous monitoring mechanisms (where relevant); and
- ✓ the type of activity under scrutiny.

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

52. PSPs should address any identified risk behaviors promptly and appropriately by carrying out enhanced examination of the agent's transaction history and data integrity, evaluating the agent's explanation of these behaviors, and/or testing the areas of the agent's services that are being questioned.

53. The outcome of such monitoring may result in further training, probation, suspension or termination of the agent depending on the nature and extent of the deficiencies identified.

PART 4 - ENHANCED DUE DILIGENCE (EDD)

54. PSPs are required to perform EDD for high risk customers. Such measures shall be on a risk sensitive basis for categories of customers, business relations or transactions as the PSP may assess to present a higher risk for ML or TF.

55. EDD shall be applied based on risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the source of funds (SOF)/wealth are not clear. Examples of customers requiring EDD include:

- Non-resident customers;
- Customers from countries that do not or insufficiently apply the FATF standards;
- High net worth individuals;
- Politically exposed persons (PEPs);
- Non-face to face customers; and
- Those with dubious reputation as per public information available, etc.

56. A PSP shall, when conducting a transaction, carry out EDD whenever there is suspicion of ML or TF, or when other factors give rise to a belief that the customer or particular transaction poses a high risk.

POLITICALLY EXPOSED PERSONS (PEPs)

57. The decision to undertake a transaction with a PEP, a family member or close relative of a PEP, and transactions in which a PEP is the beneficial owner shall be taken at a senior level and the guidelines for making such decisions shall be clearly spelt out in writing in the CAP. All transactions involving a PEP shall be subject to enhance monitoring on an ongoing basis.

58. PSPs shall gather sufficient information on any prospective customer falling under this category including checking all the information available on the person in the public domain, verify the identity of the person and seek information about the SOF/wealth before accepting the PEP as a customer.

59. The EDD requirements may also be applied to customers who become PEPs subsequent to the establishment of the business relationship.

SPECIAL IDENTIFICATION REQUIREMENTS APPLICABLE TO PSPs

60. PSPs are required to obtain and maintain accurate and meaningful information of:

- ✓ the name of the originator;
- ✓ the originator's reference number where such an account is used to process the transaction;
- ✓ the originator's address, national identification card or passport number and date of birth;
- ✓ the name of the beneficiary; and
- ✓ the beneficiary's account number where such an account is used to process the transaction.

61. The ordering of PSP may include full originator information or only the originator's account number or unique reference number, provided full originator information is available to the recipient PSP and competent authorities.

MONITORING OF TRANSACTIONS

EDD

62. PSPs may set limits for any category of transactions and pay particular attention to the transactions which exceed these limits. High-risk transactions have to be subjected to EDD. Key indicators shall be established for such transactions, taking note of the background of the customer, e.g., SOF, the type of transactions involved and other risk factors. A system of periodical review of risk categorization of customers shall be put in place and the need for applying EDD measures. PSPs shall examine the background and purpose of transactions with persons (including legal persons and other financial institutions) classified by the FATF as uncooperative or high-risk countries that do not sufficiently apply the FATF Standards.

Suspicious Transaction Report (STR)

63. Further, if the transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions should, as far as possible, be examined and written findings together with all the documents should be retained and made available to the FIU. PSPs are unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, they shall not undertake the transaction. Under these circumstances, the PSP shall file a STR with the FIU even if the transaction was not processed.

PART 5 - RESPONSIBILITIES OF PSPS

RISK MANAGEMENT

64. Risk analysis must be performed, and kept up to date, to determine where ML and TF risks are greatest. PSPs need to identify the main vulnerabilities and address them accordingly. Higher risk customers, products and services, including delivery channels, and geographical locations should be identified and commensurate AML/CFT measures must be applied.

65. Risk assessment must include a variety of factors, depending upon particular circumstances, including but not limited to:

- ✓ The nature, scale and complexity of the PSPs operations, including geographic locations.
- ✓ The initial and ongoing due diligence or monitoring conducted on the PSP agent locations.
- ✓ The customer, product, and activity profile.

- ✓ The nature of the business relationship (i.e., Occasional vs. Ongoing relationship).
- ✓ The distribution channels used.
- ✓ The volume and size of transactions.
- ✓ The extent to which PSPs are dealing directly with customers or is dealing through intermediaries, third parties or in a non- face-to-face setting.

66. To conduct a proper risk-based approach, PSPs need to collect relevant information. The effectiveness of the risk-based approach would increase significantly if designated institutions are able to share information with other relevant institutions, including foreign counterparts.

CONTROLS FOR HIGH RISK SITUATIONS

67. PSPs are required to implement appropriate measures and controls to mitigate the potential ML or TF risks for situations that are considered to be of higher risk as determined from the designated institution's risk assessment.

68. These measures and controls may include:

- ✓ Increased levels of KYC or EDD, such as proactive contact with the customer to determine the reason for the transactions, the customer's relationship to the sender or receiver, and the SOF.
- ✓ Increased levels of controls and frequency of reviews of customer relationships.
- ✓ Increased transaction monitoring of higher -risk and channels.
- ✓ Enhanced systematic controls and data integrity at the points of payment, particularly at a higher risk agent location.
- ✓ Aggregation of activity by a known or a new customer.

69. PSPs should pay special attention to any ML threats that may arise from new or developing technologies, including internet-based transactions which might favour anonymity; and take measures to prevent their use for ML or financing of terrorism.

IMPLEMENTATION OF RISK-BASED APPROACH

70. PSPs should formulate and implement a risk-based approach in their AML/CFT programmes. This approach requires an assessment of the risk posed by the nature of the business and the implementation of appropriate mitigation measures, while maintaining an overall effective programme.

71. There should be evidence by categorization of the customer base, products and services by risk-rating (e.g., low, medium, and high) and identification of assigned actions by risk types. While each PSP will determine the number and name of risk categories, the fundamental issue is for the adoption of reasonable criteria for assessing risks.

72. The review of high-risk customers may be undertaken more frequently than for other customers and a determination should be made by senior management as to whether the relationship should be continued. All decisions regarding high-risk relationships and the basis for these decisions shall be documented.

73. The framework should take into account customer acceptance and on-going monitoring policies and procedures that assist the PSPs in identifying the types of customers that are likely to pose higher than average ML and TF risk. A more extensive EDD process should be adopted for high risk customers.

74. There should also be clear internal guidelines which require management's approval for business relationships with such customers. The framework should provide for documentation of any changes in a customer's risk rating and the reason for such a change.

75. PSPs shall therefore design an AML/CFT framework that is tailored to satisfy the needs of their institution, but should include at a minimum:

- Differentiation of client relationships by risk categories (such as high, moderate or low);
- Differentiation of client relationships by risk factors (such as products, client type/profession, complexity of ownership and legal structure, source of business, type of assets, size, volume and type of transactions, cash transactions, adherence to client activity profile).
- KYC documentation and due diligence information requirements appropriate for each risk category and risk factor; and
- Requirements for the approval of upgrading and downgrading of customer risk ratings.

76. Typologies of ML and TF schemes are available at websites such as www.fatf-gafi.org to assist in risk categorization. A PSP shall ensure that systems are in place to periodically test the accuracy of the assignment of the customer base to risk categories and that the requisite due diligence is being followed. A PSP shall periodically review its risk categories as typologies evolve on practices by money launderers and terrorists. These reviews shall be undertaken at intervals no longer than one year.

77. PSPs shall establish a customer's profile taking into account, at a minimum:

- the nature of the customer's business (whether cash intensive, etc.);
- the nature and frequency of the activity;
- the complexity, volume and pattern of transactions;
- type of customer, based on specific risk factors (e.g. whether ownership of a corporate customer is highly complex for no apparent reason, whether the customer is a PEP, whether the customer's employment income supports transaction patterns, whether customer is known to other members of the financial group, whether delegated authority such as power of attorney is in place);
- delivery channels (e.g., whether mobile/internet banking, remote cash withdrawals);
- geographical origin of the customer;
- geographical area (e.g., whether business is conducted in or through jurisdictions with high levels of drug trafficking, corruption or lacking proper standards in the prevention of ML/TF, whether the customer is subject to regulatory or public disclosure requirements);
- whether the SOF/wealth can be easily verified and whether the audit trail has been deliberately broken and/or unnecessarily layered;
- unwillingness of the customer to cooperate with the PSPs' CDD process for no apparent reason; and
- any other information that raises suspicion of the customer's connection to ML or TF.

78. AML/CFT risks may be measured in various ways. Developing proper risk categories allow PSPs to ensure that 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 a PSP 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 Factors

79. This is the risk associated with the products or services offered by the PSPs. PSPs should pay special attention to new or innovative products or services that it does not offer but makes 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 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, such as cash, online money transfers, stored value cards, money orders and money transfers by mobile phone.

Transaction Risk Factors

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

a) *Transactions sent or attempted:*

- ✓ PSPs 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 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 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.

PSPs should be able to detect the following activities 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; and
- ✓ 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:

- ✓ PSPs should pay special attention:
- ✓ to transactions that are not accompanied by the required originator or beneficiary information;
- ✓ when additional customer or transactional information has been requested but has not been received; or
- ✓ 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 Factors

81. A PSP 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, PSPs 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 who are known to the PSP 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 FIU, 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 (HT), people smuggling (PS), etc. - based on information available to the PSPs; and
- ✓ where the customer or its counterpart is another PSP or financial institution which has been sanctioned by the FIU for its non-compliance with the current AML/CFT regime and is not engaging in remediation to improve its compliance.

Geographic Risk Factors

82. Geographic risk requires an entity to make a good assessment of the potential AML/CFT risks associated with a particular geographic region.

Agent/Distribution Risk Factors

83. PSPs that use agents to facilitate the delivery of their services should be aware of the risks posed by such relationships. They 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 as they are relevant to the PSP's 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;
- ✓ 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 consistent with other agents, or whose transactions and activities indicate potential complicity in criminal activity; and whose 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.

INTERNAL CONTROLS General

84. The PSPs shall ensure that effective AML/CFT internal controls are put in place by establishing appropriate procedures and ensuring effective implementation. The internal controls shall cover proper management oversight systems and controls, segregation of duties, training and other related matters. Responsibility shall be explicitly allocated within the PSP so as to ensure that the policies and procedures are implemented effectively.

85. The PSP's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the AML/CFT policies and procedures. As a general rule, the compliance function should provide an independent evaluation of the PSP own policies and procedures , including legal and regulatory requirements. A PSP shall ensure that its audit machinery is staffed adequately with individuals who are well-versed with such policies and procedures.

86. Effective internal control measures should allow PSPs to perform a risk assessment of their business relationships or one-off transactions and allow for the management and mitigation of such risks. Established internal controls should be appropriate given the nature of the business relationship or one-off transaction and should ensure compliance with the requirements of the AML/CFT Act of 2009.

87. It is important that the BOD/senior management should be aware that subsidiaries and branches of PSPs are expected to, at a minimum, comply with the requirements of the AML/CFT Act of 2009, Regulations 2010, and this Guideline; and where some PSPs' operational AML/CFT functions may be outsourced, it retains full responsibility for compliance with local laws, Regulations and Guidelines.

88. Directors should therefore demonstrate their commitment to an effective AML/CFT programme by:

- ✓ understanding the statutory duties placed upon them, their staff and the entity itself;
- ✓ approving AML/CFT policies and procedures that are appropriate for the risks faced by the licensee;
- ✓ ensuring that the institution appoints a Compliance Officer in accordance with section 19 (1) of the AML/CFT Act 2009 and section 14 (1) of the Regulations 2010;
- ✓ ensuring that the institution is in compliance with its statutory responsibilities as it relates to AML/CFT. This includes reviewing the reports from the Compliance Officer, internal audit, external auditors and supervisory authority on the operations and effectiveness of compliance systems.

89. Senior management in collaboration with the Compliance Officer is responsible for the development of sound risk management programmes and for keeping directors adequately informed about these programmes and their effectiveness.

90. PSPs should formally document policies and procedures which at a minimum, should provide for:

- ✓ the development of internal policies, procedures and controls for, inter alia:
  - o the processing of a transaction and verification of customer identity;
  - o establishing business relations with third parties (correspondent banks, etc.);
  - o determining business relationships that is not accepted by PSP;
  - o the timely detection of unusual and suspicious transactions, and reporting to the FIU;
  - o internal reporting; and
  - o record retention.

- ✓ the recruitment of staff, appropriate to the nature and size of the business, to carry out the AML/CFT compliance function;

- ✓ an on-going training programme designed to ensure adherence by employees to the legal and internal procedures, and familiarity with the dangers the PSPs face and on how their job responsibilities can encounter specified ML and TF;

- ✓ the appointment of a Compliance Officer at an appropriate level of authority and independence to, inter alia, coordinate and monitor the compliance programme, receive internal reports, and issue STRs to the FIU;

- ✓ establishment of management information/reporting systems to facilitate aggregate and group/branch wide monitoring;

- ✓ an effective independent risk-based oversight function to test and evaluate the compliance programme; and

- ✓ screening procedures for hiring, and on-going systems to promote high ethical and professional standards to prevent the PSP from being used for criminal activity.

91. Policies should be periodically reviewed for consistency with the business model, and changes and developments in the PSP's products and services. Special attention should be paid to emerging technologies and new payment products as well as trends in ML and TF.

Ensuring Compliance

92. PSPs are subject to inspection by the BOG. During the monitoring and inspection process the BOG is required to review the PSPs' internal control procedures to ensure compliance with regulatory standards.

93. PSPs shall not put any restrictions on payment to beneficiaries where an STR has been made. Moreover, a PSP shall ensure that employees keep the fact of furnishing such information as strictly confidential, and **tipping-off** to the customer is strictly prohibited.

APPOINTMENT/ROLE OF A COMPLIANCE OFFICER

94. A PSP shall appoint a senior management officer as a Compliance Officer.

The Compliance Officer shall, among other things, be responsible for:

- Monitoring and reporting of all suspicious transactions and sharing of information as required under the AML/CFT Act 2009.
- Overseeing and ensuring overall compliance with the relevant laws on AML/CFT issues inclusive of the AML/CFT Act 2009 and AML/CFT Regulations 2010 .
- Developing appropriate compliance management arrangements across the full range of AML/CFT areas (e.g., CDD, record-keeping, etc.).
- Maintaining close liaison with law enforcement agencies, and any other institutions that are involved in the fight against ML and TF.

Training

95. It is important and imperative that the Compliance Officer appointed by the PSP has the necessary knowledge, expertise and required authority to effectively discharge assigned responsibilities, including knowledge on AML/CFT obligations required under the relevant laws and regulations, and the latest developments in ML and financing of terrorism techniques. The Compliance Officer should be appointed at a management level; BOG shall be immediately informed in writing; and a Personal Declaration Sheet (PDS) be submitted within thirty (30) days.

96. The Compliance Officer should be independent of the receipt, transfer or payment of funds or management of customer assets and should have timely and uninhibited access to customer identification, transaction records and other relevant information. The powers and reporting structure of the Compliance Officer should be conducive to the effective and independent exercise of his/her duties.

97. At a minimum, the Compliance Officer must be appointed and perform the functions and duties in accordance with section 19 of the AML/CFT Act 2009 and section 14 of the AML/CFT Regulations 2010. The Compliance Officer is required to consider any report submitted to him/her on a transaction which is believed or known to be proceeds of a specified offence and where necessary submit a STR to the FIU.

98. The Compliance Officer should have the authority and the resources necessary to effectively discharge his/her responsibilities. To ensure consistent and ongoing attention to the compliance regime, the appointed officer may choose to delegate certain duties to other employees. For example, the officer may delegate an individual in a branch to ensure that compliance procedures are properly implemented at that location. However, the appointed compliance officer remains responsible for the PSP's overall compliance programme and its effectiveness. It is also recommended that a Deputy be identified, who should be a staff member of similar status and experience to the Compliance Officer, and who must be able to conduct all functions of the Compliance Officer in his/her absence.

The Compliance Officer of a PSP should:

- undertake responsibility for developing internal policies, procedures, controls and systems for an effective AML/CFT compliance programme within the institution;
- develop and maintain AML/CFT guidelines for the institution in relation to the business of the institution;
- implement the customer identification requirements;
- implement record keeping and retention requirements;
- monitor compliance with the institution's internal AML/CFT programme;
- receive internal reports and consider all such reports;
- prepare and submit written STRs to the FIU as soon as practicable after determining that a transaction warrants reporting. Such forms should be prepared in the specified format as the FIU may determine;
- monitor the accounts of persons for whom a suspicious report has been made;
- establish and maintain an on-going awareness programme for the officers and employees of the financial institution's AML/CFT internal policies and procedures and conduct training programmes for staff at all levels to recognize suspicious transactions;
- establish standards for the frequency and means of training;
- conduct a self-assessment and report to the BOD (or relevant oversight body in the case of branch operations) on the operations and effectiveness of the systems and controls to combat ML and TF;
- review compliance policies and procedures to reflect changes in legislation or international developments, non-compliance and new services or products. It is essential that the scope and the results of the review be documented. Deficiencies should be identified and reported to senior management and the BOD, and corrective actions taken to address these deficiencies in a timely manner;

- participate in the approval process for high-risk business lines and new products, including those involving new technologies;
- screen persons before employing them in the compliance department;
- act as the Liaison between the institution and the BOG and/or FIU on matters pertaining to compliance with the AML/CFT function.

Training of Agents

99. Training should also be conducted for the specific categories of staff, for example, agents, customer service representatives, regular employees, senior management and the BOD.

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

101. 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 AML/CFT Act 2009.

Customer Service Representatives and Other Employees

102. 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 PSPs 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.

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

104. 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 PSPs' AML/CFT controls and appropriate measures applied where staff are unable to demonstrate the level of knowledge expected.

105. Any training provided should be appropriately tailored to the responsibilities of the employees receiving the training thereby equipping staff with a sound understanding of specialized 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.

106. In addition, the PSPs is required to maintain a record of the training they provide to their staff; these become particularly relevant during an examination by the BOG to establish the extent to which the PSPs is adhering to their AML/CFT obligations.

107. It is important that all staff members fully understand the rationale behind the AML/CFT policies, and the need for them to implement such policies consistently. The steps to be taken when staff members come across any suspicious transaction (such as asking questions about the SOF, checking the identification documents carefully, reporting immediately to the Compliance Officer) should be carefully and clearly formulated by the designated institution, and the respective procedures laid down in writing.

108. Senior management and the BOD must also undergo annual AML/CFT training relevant to their rank within a PSP. This will enhance the policies and procedures formulated by them after being updated on the changes for AML/CFT requirements and form the basis for PSPs to put measures in place to mitigate the likely risks arising from ML/TF.

REPORTS

(1) Suspicious Transactions

109. Suspicious activity is any observed behavior that could indicate ML and/or terrorism or terrorism-related crime. All entities that are subject to the requirements of the AML/CFT must take steps to identify any activity suspected to be linked to ML or TF and report it to the FIU if they determine that the activity appears suspicious. Where reports are not made to the FIU, a record should be made of the activity and the reason for not filing are port.

110. PSPs must ensure that, in the event of a suspicious activity being discovered, all staff are aware of the reporting chain and the procedures to follow. Staff at all levels should also be aware of the identity of the Compliance Officer and the steps to be followed when making a STR.

111. Where a suspicious report has been filed with the FIU, and further unusual or suspicious activity pertaining to the same customer arises, PSPs should file additional reports with the FIU.

112. Pursuant to section 18 (4) of the AML/CFT Act 2009, PSPs are required to report as soon as possible but not later than **three** working days to the FIU, where the identity of the person involved, the transaction, proposed transaction or attempted transaction or any other circumstance concerning that transaction lead the institution to have reasonable grounds to suspect that a transaction:

- involves proceeds of crime to which the AML/CFT Act 2009 applies;
- involves or is linked or related to or to be used for terrorism, terrorist acts or by terrorist organizations or for the financing of terrorism; or
- is of a suspicious or an unusual nature.

113. The STR should be in the format prescribed in the Guideline No.1 – 2013 issued by the FIU or in accordance with section 18 (4) (b) of the AML/CFT 2009. All reports must be accompanied by a letter signed by the institution's Compliance Officer.

114. An institution which has reported a suspicious transaction shall, if requested by the FIU, provide further information as required on the said transaction.

Indicators of Suspicious Activity

New customers and occasional or 'one-off' transactions

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

- checking the 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 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

116. In relation to customers that PSPs know and are accustomed to dealing with, attention must be paid to the following indicators which may give rise to suspicious activity of ML:

- 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

117. 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.

(2) Threshold Reports

118. **PSPs**

In addition, regardless of whether or not a transaction is viewed as suspicious, all purchases over G$200,000 (two hundred thousand dollars) and all sales over G$200,000 (two hundred thousand dollars) should be promptly reported to the FIU by PSPs.

Establishment of Registers

119. PSPs are required to maintain a register of all STRs made to the Compliance Officer and should contain details of the date on which the report is made, the person who made the report and information sufficient to identify the relevant documents.[5]

120. Additionally, PSPs are required to maintain a register of all enquiries made by the FIU and other law enforcement authorities acting under powers provided by the AML/CFT Act 2009 or any other law relating to ML, TF and proceeds of crime. The register should be kept separate from other records and contain at a minimum the date and nature of the enquiry, the name and agency of the enquiring officer, the powers being exercised, and details of the accounts or transactions involved.

121. PSPs are also required to maintain records of staff training which at a minimum should include:-

- details of the content of the training programmes provided;
- the names of staff who have received the training;
- the date on which the training was delivered;
- the results of any testing carried out to measure staff understanding of the AML requirements; and
- an on-going training plan.

Reporting Declined Business

122. It is normal practice for financial institutions to turn away business that they suspect might be criminal in intent or origin. Where an applicant for business or a customer fails to provide adequate documentation, including the identity of any beneficial owners or controllers, consideration should be given to filing a STR. (Please refer to Section 18 of the AML/CFT Act 2009).

5 Refer to Section 11 (2) (3) of the AML/CFT Regulations 2010

MAINTENANCE OF RECORDS OF TRANSACTIONS

123. It is imperative for PSPs to keep a record of all customer verification measures, all transactions executed, and all STRs filed with the FIU. Maintenance of s u c h comprehensive records enables PSPs to show their compliance with the AML /CFT Act 2009 and AML/CFT Regulations 2010. 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.

Back-up and Recovery

124. Information on transactions processed must be maintained in a remote area from the place of operation in order to safeguard such data should an adverse event occur.

125. Part III section 16 (1) – (5) of the AML/CFT Act 2009 and 6-10 of the AML/CFT Regulations 2010 stipulates the minimum requirements for PSPs with regard to record keeping. All records are required to be maintained for a period of at least 7 years from the date the one-off transaction was completed or the business relationship was terminated. Records should be retained in a format, including electronic, scanned or original, that would facilitate retrieval in legible form without undue delay.

126. PSPs should develop clear standards on what records must be kept on customer identification and individual transactions and their retention period. Such a practice is essential to permit the institution to monitor its relationship with the customer, to understand the customer's on-going business and, if necessary, to provide evidence in the event of disputes, legal action, or a financial investigation that could lead to criminal prosecution.

127. To facilitate compliance with the above and to facilitate investigations undertaken by the FIU, PSPs should establish a document retention policy that provides for the maintenance of a broad spectrum of records, including those related to customer identification, business transactions, internal and external reporting and training. Once a business relationship has been formed, the institution should maintain records of client identification and transactions performed.

128. The document retention policy should incorporate the requirement that a PSP is required to keep records of all transactions as well as identification data on a customer for a minimum period of 7 years, from the date the relevant transaction or series of linked transactions was completed or when the business relationship was

terminated, whichever is the later. It is an offence to knowingly destroy, falsify or conceal any document or material which would aid in an investigation into ML, TF or the proceeds of crime[6].

129. It may also be necessary for PSPs to retain records for a longer time period as required by other statutory requirements or mandated by the BOG or until such time as advised by the FIU or High Court, for a period exceeding the date of termination of the last business transaction where there:

- has been a report of a suspicious activity; or
- is an on-going investigation relating to a transaction or customer.

6 Refer to AML/CFT Act 2009 –Section (6) (1) (2)

130. In addition, transaction records should contain sufficient details[7] to permit reconstruction of individual transactions (including the amounts and types of currency involved) so as to provide, if necessary, an audit trail and evidence for prosecution of criminal activity and to enable PSPs to comply swiftly with information requests from the FIU. This applies whether or not records are stored off the premises of the institution.

131. PSP should ensure that records held by a subsidiary or affiliate at a minimum, comply with the requirements of Guyana's law and this guideline. Where the institution has outsourced any or all of the foregoing functions to another company then it must be satisfied that the relevant records will be maintained in accordance with Guyana's law and will be available to the BOG, FIU or law enforcement on request.

132. When a PSP merges with or takes over a financial entity, it should ensure that the records such as CDD, transactions, external audit and training can be readily retrieved. Where the records are kept in a contractual relationship by an entity other than a PSP, the institution is responsible for retrieving those records before the end of the contractual arrangement.

133. To ensure that records remain up-to-date and relevant, there is a need for PSPs to undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, or at least upon occurrence of a material change to the business relationship (e.g., change of employment, marital status, address, etc.), or when there is a material change in the way that the account is operated. In addition, it is recommended that records for high-risk customers are updated annually.

---

[7] Such details are specified in Section 16 of the AML/CFT Act 2009.

134. If during the course of the updating exercise or any time after the business relationship has commenced and it is discovered that the information on file is inaccurate, insufficient or is no longer applicable it should take steps to ensure that all relevant and updated information is obtained as quickly as possible. Where the correct information is not available or cannot be obtained for any reason, then steps must be taken to terminate the relationship and consideration should be given to referring the matter to the FIU.

PART 6 - OTHERS

TERRORIST FINANCING

135. ML and TF are often mentioned together but the two are separate crimes. The key distinction between ML and TF involves the origin of the funds. TF uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds while ML always involves the proceeds of illegal activities.

DETECTING TERRORIST FINANCING

136. The following key considerations should be taken into account when making a determination whether funds are linked to TF:

- ✓ Motivation – is ideological.
- ✓ SOF – internally from self-funding groups and externally from benefactors and fundraisers.
- ✓ Conduits – favours cash couriers or informal financial system.[8]
- ✓ Detection Focus – suspicious relationships, such as wire transfer between seemingly unrelated parties.
- ✓ Transaction Amounts – small amounts below reporting threshold.
- ✓ Financial Activity – no workable financial profile of terrorist exists.

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

137. The following represent examples of possible links to terrorist activity:

- ✓ parties to the transaction are from countries known to support terrorist activities;
- ✓ use of false identity documentation;
- ✓ abuse of non-profit organisations;
- ✓ beneficial owner not properly identified;
- ✓ 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.

PROLIFERATION FINANCING (PF)

138. PF is the act of providing funds or financial services which are used as part, for the manufacture, acquisition, possession, development, export, transshipment, 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.

Some indicators of PF include:

- ✓ the customer is vague and resistant to providing additional information when asked;
- ✓ the customer's activity does not match its business profile or the end-user information does not match the end-user's business profile;
- ✓ the transaction involves designated persons;
- ✓ the transaction involves higher risk jurisdictions which are known to be involved in proliferation of weapons of mass destruction or PF activities; and
- ✓ the transaction involves possible shell companies.

139. **HUMAN TRAFFICKING (HT)**

HT is the act of recruiting, harboring, transporting, providing or obtaining a person for forced labor or commercial sex acts through the use of force coercion, or exploitation of victims. Anyone can be a victim regardless of origin, sex, age or legal status and there is no need for persons to cross a border, individuals can be trafficked within the borders of a country. It includes but is not limited to servitude, forced labor, debt bondage and sexual exploitation.

- ✓ Frequent transactions, inconsistent with expected activity and/or line of business in apparent efforts to provide subsistence to individuals (e.g., payment for housing, lodging, regular vehicle rentals, and purchases of large amounts of food).