BANK OF GUYANA

PAYMENT SERVICE PROVIDERS

GUIDELINE NO. 1

ISSUED UNDER THE AUTHORITY OF THE ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM ACT 2009

FOR NON-BANK PAYMENT SERVICE PROVIDERS

February 2026

TABLE OF CONTENTS

GLOSSARY

Term	Definition
AML/CFT/CPF	Anti-Money Laundering, Countering the Financing of Terrorism, and Countering the Proliferation of Weapons of Mass Destruction
Bank	Bank of Guyana
Board	Board of Directors
Beneficial Owner	Natural Person(s) who ultimately owns(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,
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force- an international policy-making body that sets standards and promotes policies to combat money laundering, terrorist financing, and the financing of proliferation of weapons of mass destruction.
KYC	Know Your Customer
PSP	Payment Service Provider
BOD	Board of Directors
ML	Money Laundering
ML/TF/PF	Money Laundering/Terrorist Financing/Proliferation Financing
STR	Suspicious Transaction Report including attempted transaction
FIU	Financial Intelligence Unit- An autonomous body responsible for requesting, receiving and analysing and dissemination of suspicious transaction reports and other information relating to money laundering, terrorist financing and proliferation financing. It was established under the ambit of the Anti-money Laundering and Countering the Financing of Terrorism Act 2009
PEP	Politically Exposed Person- Person holding prominent public office in a local or foreign country and includes spouse, close relative, or associate of such person. Example of politically exposed persons include Heads of States or of Governments, senior politicians, senior government/judiciary/military officers , senior executives of state –owned corporations, important political party officials, and their spouses, close relatives and associates or legal persons and arrangements controlled by such persons.
PF	Proliferation Financing- 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, transporting, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials, including technologies and dual use
UNSCR	United Nations Security Council Resolution

PART 1 – INTRODUCTION

1. This Payment Service Providers Guideline (PSP) No. 1 replaces Supervision Guideline No. 1 for Payment Services Providers which was issued under the under the authority of the AML/CFT Act 2009 and was gazetted on April 1, 2023.

2. This Guideline for PSPs is issued pursuant to the section 22(b) of the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Act 2009. It provides guidance on the requirements for the implementation of an adequate Anti- Money Laundering/Countering the Financing of Terrorism/Countering the Financing of Proliferation (AML/CFT/CPF) risk-based framework.

3. PSPs must establish internal programs to combat money laundering, terrorism financing and proliferation financing in order to ensure that their services are not used to launder unlawfully derived funds, finance terrorist, and to facilitate proliferation financing.

SCOPE

4. This Guideline covers the following:
   - obligations of PSPs with respect to the requirements under the AML/CFT Act
   - roles of the Board of Directors and Senior Management of PSPs in putting in place The relevant AML/CFT/CPF measures; and
   - Implementing a risk-based approach in identifying and managing ML/TF/PF risks.

APPLICABILITY

5. All non-bank PSPs licensed by the Bank of Guyana are required to ensure that this Guideline is implemented in furtherance of their compliance with the AML/CFT Act 2009 and the applicable regulations issued under this Act.

Money Laundering

6. Money laundering (ML) is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. Section 3 of the AML/CFT Act 2009 states that "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. The techniques for laundering funds may vary and can be very intricate, there are three stages in the process:
   - **Placement** - the placement of funds derived from illegal activity in the financial system;
   - **Layering** - separating illicit proceeds from their source, often by creating complex layers of financial transactions designed to disguise the source of money, to subvert the audit trail and provide anonymity; and
   - **Integration** - creating the impression of apparent legitimacy to criminally derived wealth.

8. These three stages may occur as separate and distinct phases or they may also occur simultaneously and in some instances may even overlap. How the basic steps used is dependent on the available laundering mechanisms and the requirements of the perpetrators of ML/TF/PF offenses.

9. If the layering process was successful, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal legitimate funds.

Terrorism Financing

10. Terrorism financing generally refers to raising money involving the provision or solicitation of funds with the intent of using those funds to support terrorist acts or terrorist organizations. The funds may be from legitimate or illegitimate sources whereas as money laundering involves funds or properties that are proceeds of crime. Terrorists need money to plan, train

for and execute terrorist attacks, therefore preventing and disrupting terrorism-related financial flows and transactions is one of the most effective ways of fighting against terrorism.

11. Terrorists are constantly changing how they raise funds and where they move them to, in order to avoid detection. Factors facilitating **t**errorist financing include the ease with which electronic payment mechanisms can be facilitated, the widespread use of new technologies/products, anonymity when making financial transfers, and access to a wide range and number of potential sponsors.

12. The challenge for jurisdictions is to identify terrorists due to the relatively low amounts of funding they require and the speed with which they can acquire it. The relevant authorities must therefore ensure that all Terrorist Financing are criminalised in accordance with the United Nations (UN) Convention for the Suppression of the Financing of Terrorism, adopted by the General Assembly in December 1999.

Proliferation Financing

13. Proliferation Financing (PF) is the act of providing funds and financial services which are used in whole and in part for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, stockpiling or use of nuclear, chemical or biological weapons and related materials[1] and their means of delivery, in contravention of national laws and where applicable international obligations.

14. PSPs must therefore have adequate systems in place to understand, identify, assess and manage the ML/TF/PF risk to which they are exposed in order to disrupt the financial flows available to and used by launderers, terrorists and proliferation financiers.

15. In addition, PSPs have a statutory duty to ensure that a Suspicious Transaction Report (STR) is filed with the Financial Intelligence Unit (FIU) when knowing or suspecting that any funds

[1] *Including both technologies and dual use goods for non-legitimate purpose*

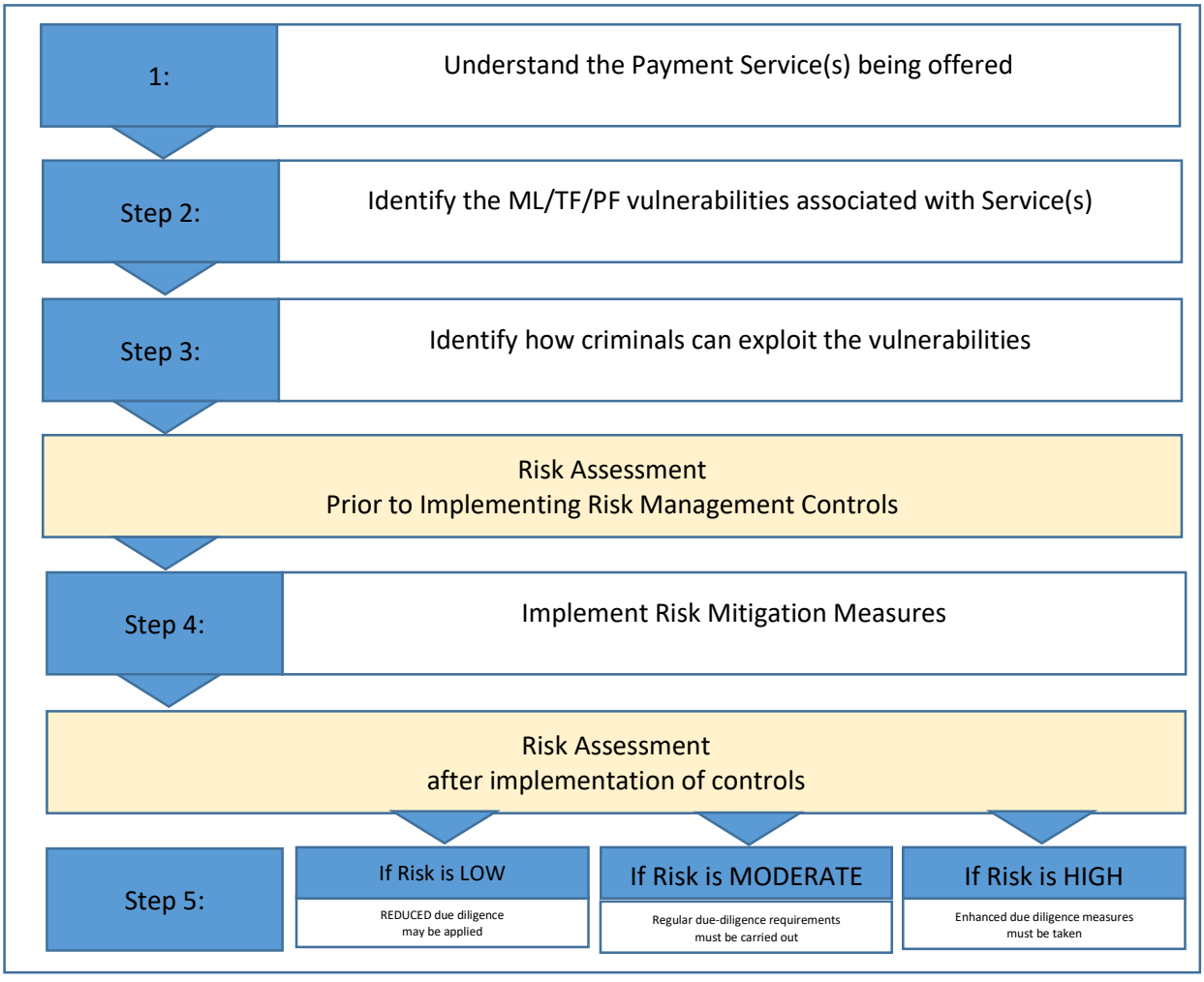
connected to proceeds of crime, money laundering, terrorism and proliferation financing, is or was intended to be used in that connection.

Risk-Based Approach

16. The "Risk-Based Approach" prescribes that the intensity and extensiveness of risk management function must be proportionate to the nature, size and complexity of the PSP's activities and its ML/TF/PF risk profile.

17. The risk-based approach adopted by the PSP must identify the high, medium and low risk areas and assist the institution to better allocate limited resources in its effort to combat ML/TF/PF. In addition, the approach must also include an assessment and identification of the level ML/TF/PF risk posed by the institution's customers, product, services, transactions, delivery channels and geographic locations used when providing payment services.

18. The diagram below provides a summary of a risk assessment methodology which may be used by PSPs to assess the level of risk inherent in their operations:



19. Once the risks are identified and assessed, the PSP must implement the appropriate control measures to mitigate the identified risks to ensure its systems are not exploited to launder funds and facilitate acts of TF/PF. The institutions risk management function should also be aligned with its overall risk control function.

20. The risk control and mitigation measures implemented by PSPs must be commensurate with the risk profile of a particular customer/type of customer. After the initial acceptance of the customer to establish a business relationship, PSPs may regularly review and update the customer's risk profile based on their level of ML/TF/PF risks.

21. It is also important for PSPs to conduct independent control testing of their policies, controls and procedures for the purpose of monitoring the implementation of their risk control and mitigation policies.

22. PSPs may be vulnerable to criminals due to the following factors:

(i) Anonymity/customer identity is unknown

Vulnerabilities:

- where identification processes are weak/absent, criminals may operate with a degree of anonymity and open/operate multiple accounts, and
- if identification processes exist but verification processes are weak e.g. lack of reliable national identification, criminals may be able to commit identity fraud.

Mitigating Factors:

- transactions are linked to a unique mobile number,
- the SIM card and customer are identified and located through the mobile station international subscriber directory number and international mobile subscriber identity,
- transactions are recorded including sender's mobile number, amount, receiver's mobile number and date,
- transactions can be traced,
- SIM card registration records make critical information available to identify the customer, and
- If law enforcement officials wish to identify a particular unidentified client, the service provider can furnish identifying data including voice recordings.

(ii) Evasiveness/ability to conceal amount, origin, and destination

Vulnerabilities:

- sharing a single device, SIM, and/or mobile money account makes it harder to ensure the person conducting a transaction is the registered user,
- criminals can use smurfing to hide larger sums being transferred, and
- The prevalence of mobile phones eliminates requirement for sender and recipient to be in the same place at the same time.

Mitigating Factors:

- mobile money transactions are traceable in a mobile operator's system as part of standard business practice, and
- Telephone number, both sending and receiving, time, and the value of the transaction are known to the mobile operator.

(iii) Rapidity of Transfer

Vulnerabilities:

- transactions occur in real time,
- Allow for rapid transaction layering - transferring funds among multiple accounts to conceal their origin.

Mitigating Factors

- mobile money transactions are traceable in a mobile operator's system as part of standard business practice, and
- telephone number, both sending and receiving, time, and the value of the transaction are known to the mobile operator.

23. The vulnerabilities in relation to the abovementioned risk factors can be exploited by criminals to abuse the mobile payment systems for ML/TF/PF. Below are some examples of how criminals may exploit the vulnerabilities:

RISK FACTORS	Example of Exploitation of Vulnerability		
	Depositing	**Transferring Payments**	**Withdrawing**
Anonymity	Multiple accounts can be opened by criminals to hide the true value of deposits	Suspicious names cannot be flagged by system, making it a safe zone for criminals and terrorists	Allows for cashing out of illicit or terrorist linked funds
Evasiveness	Criminals can smurf proceeds of criminal activity into multiple accounts.	Criminals can perform multiple transactions to confuse the money trail and true origin of funds	Smurfed funds from multiple accounts can be withdrawn at the same time
Rapidity	Illegal monies can be quickly deposited and transferred out to another account.	Transactions occur in real time, making little time to stop it if there is a suspicion of terrorist financing or laundering	Criminal money can be moved through the system rapidly and withdrawn from another account.

24. Below are some risk mitigation controls which may be implemented in relation to the risk factors identified above:

Risk Factor	Controls
Anonymity	• Creating and updating periodically customer profiles, registration information including name, unique ID and phone number etc. • Requiring recipients to register to receive funds.
Elusiveness	• Limits on amount, balance, frequency and number of transactions for both originators and recipients. • Real-time monitoring
Rapidity	• Real time monitoring • Frequency restrictions on transactions • Restrictions on transaction amount and total account turnover in a given period

PART II – AML/CFT/CPF PROGRAM

25. In order to discharge their statutory responsibility to deter and prevent AML/FT/CPF, PSPs must implement an AML/CFT/CFP program which must include at a minimum:

- duties and responsibilities of the Board of Directors and Senior Management
- internal policies, procedures, and controls;
- designation of a Compliance Officer;
- training of its employees and agents; and
- Audit of AML/CFT/CPF policies, procedures and controls.

26. The AML/CFT/CPF program must be endorsed by the Board of Directors (where applicable) and Senior Management, and must be applicable and appropriate to all branches and agents.

Duties of Board of Directors and Senior Management

Board of Directors

27. Members of Board must be aware of their roles and responsibilities in managing ML/TF/PF risks faced by the PSP, as well as the ML/TF/PF risks associated with business strategies, delivery channels, geographical coverage of its business products and services and its customers.

28. The Board must understand the AML/CFT/CPF measures required by the law including the AML/CFT Act and its amendments, Regulations and AML/CFT/CPF Guidelines, and best practices as well as the importance of implementing measures to prevent the product and services offered by the PSP from being abused by money launders and financiers of terrorism.

29. The responsibilities of the Board include:

(i) Ensuring the establishment of AML/CFT/CPF risk management systems that are reflective of the nature of the PSP's operations, size of business, complexity of business operations, structure, and risk profiles of products and services offered and geographic locations.

(ii) Maintaining accountability and oversight for establishing AML/CFT/CPF policies and procedures and minimum standards.

(iii) approving AML/CFT/CPF policies, procedures measures including those required for risk assessment, mitigation and profiling, know your customer (KYC), customer due diligence (CDD), enhanced due diligence (EDD) record keeping, on-going due diligence, identifying, detecting and reporting of suspicious transactions and combating the financing of terrorism and proliferation financing.

(iv) Ensuring the establishment of lines of authority and responsibility for implementing the AML/CFT/CPF measures and ensuring that there is a separation of duty between those implementing the policies and procedures and those enforcing the controls.

(v) ensuring the implementation of the appropriate mechanisms to ensure the AML/CFT/CPF policies are periodically reviewed, assessed and updated in line with changes in legislation and regulations and developments in the PSP's products and services, technology and trends in ML/TF/PF.

(vi) Ensuring the establishment and maintenance of an effective internal control system for AML/CFT/CPF and maintain adequate oversight of the overall AML/CFT/CPF measures undertaken by the PSP.

(vii) Ensuring effective internal audit function to assess and evaluate the robustness and adequacy of controls implemented to prevent ML/TF/PF.

(viii) Assessing the implementation of the approved AML/CFT/CPF policies through regular reporting, and updates by the Senior Management and Audit Committee.

Senior Management

30. The Senior Management is responsible for the implementation and management of AML/CFT/CPF compliance program in accordance with policies and procedures established by the Board, requirements of the law, regulations, guidelines and the industry's standards and best practices.

31. Senior Management has the following key roles and responsibilities:

(i) be aware of and understand the ML/TF/PF risks associated with new and existing business strategies, delivery channels and geographical coverage of its business products and services offered,

(ii) formulate AML/CFT/CPF policies to ensure that they are in line with the risk profiles, nature of business, complexity, geographic locations, volume of the transactions undertaken by the PSP,

(iii) establish appropriate mechanisms and formulate procedures to effectively implement AML/CFT/CPF policies and internal controls approved by the Board, including the mechanism and procedures to monitor and detect complex and unusual transactions,

(iv) undertake review and propose to the Board the necessary enhancements to the AML/CFT/CPF policies to reflect changes in the PSP's risk profiles, institutional and group business structure, delivery channels and geographical coverage,

(v) provide timely periodic reporting to the Board on the level of ML/TF/PF risks facing the PSP,

(vi) periodically review and strengthen the risk management and internal controls to manage the risks and new AML/CFT/CPF developments which may have an impact on the operations of the PSP,

(vii) allocate adequate resources to effectively implement and administer the AML/CFT/CPF compliance program which must be reflective of the size and complexity of the PSP's operations and risk profile,

(viii) ensure all the necessary remedial actions proposed by regulatory bodies and the Financial Intelligence Unit (FIU) in relation to AML/CFT/CPF compliance issues are properly addressed in a timely manner,

(ix) appoint a compliance officer at management level at Head Office and establish effective compliance mechanisms at each branch/agent/ or subsidiary,

(x) provide appropriate levels of AML/CFT/CPF training for employees at all levels throughout the institution,

(xi) ensure that there is a proper channel of communication in place to effectively communicate AML/CFT/CPF policies and procedures to employees at all levels,

(ix) Establishing appropriate employee assessment system in order to ensure the integrity of its employees.

Internal Policies, Procedures, and Controls

32. Each PSP must establish and implement policies, procedures, and internal controls, which should also be integrated into its agents' AML/CFT/CFT program. These policies, procedures, and internal controls shall be in writing and must be approved by the Board or the Senior Management, and subject to continuous or periodic review and must be implemented using the risk-based approach.

33. At minimum, the following shall be included in the policies, procedures, and internal controls:

- KYC/CDD/EDD and Customer Acceptance,
- monitoring and Reporting,
- record-keeping, and
- Training and Awareness.

34. These policies, procedures, and internal controls must be readily accessible to the relevant employees.

Compliance Officer

35. The Board or the Senior Management must designate a compliance officer who shall be responsible for ensuring implementation of the PSP's AML/CFT/CPF compliance program.

36. The Compliance Officer must be independent and at a senior level, have sufficient knowledge, resources, and authority to participate and be able to effectively implement decisions of the Board or the Senior Management relating to AML/CFT/CPF.

37. The Compliance Officer must also possess the necessary knowledge and expertise to effectively discharge his/her roles and responsibilities, including being informed of the latest developments in ML/TF/PF and techniques and the AML/CFT/CPF measures undertaken by the industry.

38. PSPs must ensure that the roles and responsibilities of the Compliance Officer are clearly defined and documented.

39. The Compliance Officer has a duty to ensure, at minimum, the following:

(i) the PSP's compliance with the AML/CFT/CPF requirements;

(ii) proper implementation of the AML/CFT/CPF policies; and procedures, including KYC/CDD/EDD, record keeping, on-going

(iii) system for identifying monitoring and reporting of suspicious transactions, are implemented effectively;

(iv) the AML/CFT/CPF mechanism is regularly assessed to ensure that it is effective and adequate to address any change in ML/TF/PF trends;

(v) the channel of communication from the respective employees to the branch/agent and subsequently to the Compliance Officer is secured and that information is kept confidential;

(vi) all employees are trained and are aware of the PSP's AML/CFT/CPF measures, including policies, control mechanism and the channel of reporting;

(vii) all internally generated suspicious transaction reports submitted to the compliance officer are appropriately evaluated before submission to the FIU;

(viii) the identification of ML/TF/PF risks associated with new products or services or those arising operational changes, including the introduction of new technologies and processes;

(ix) act as the main contact person for the FIU on behalf of the PSPs on AML/CFT/CPF compliance issues.

41. In order to ensure the necessary communication PSPs shall inform the FIU, and the Regulator on the appointment or change of the Compliance Officer.

42. PSPs must designate a Deputy Compliance officer who is authorized to act as the Compliance Officer when the principal compliance officer is absent for any reason.

Know Your Employee (KYE)/Employee Due Diligence Procedures

43. The employee due diligence procedures shall apply upon hiring the employee and throughout the course of employment. PSPs shall establish an employee assessment system that is commensurate with the size of operations and risk exposure of PSPs to ML/TF/PF. The employee assessment system shall include an evaluation of an employee's personal information, including criminal records, employment history, and where available, the financial history.

44. Under an effective employee due diligence program, PSPs should also screen prospective employee who, if employed, may be in a position to facilitate the commission of fraud, a ML/TF/PF offence and rescreen an employee, where the employee is transferred or promoted and may be in a position to facilitate the commission of fraud, a ML/TF/PF offence.

45. PSPs shall determine employees who are in high-risk positions and conduct on-going due diligence and monitoring of such employees. The employees must be made aware that they may be held personally liable for any failure to observe the AML/CFT/CPF requirements and PSPs must have proper remedial and administrative actions applicable for the employees

who violate the PSP's AML/CFT/CPF policies and procedures, and shall keep record of the actions taken.

Employee Training and Awareness Programs

46. PSPs must conduct awareness and training programs on AML/CFT/CPF practices and measures for their employees. Such training must be conducted regularly and supplemented with refresher trainings.

47. In addition, PSPs may distribute awareness materials periodically or on case-by-case basis to the employees, branches and agents.

48. The training conducted for employees must be appropriate to their level of responsibilities for detecting ML/TF/PF activities and the risks of ML/TF/PF faced by PSPs. In addition, training for all relevant employees may be provided with a general background on ML/TF/PF, the requirements and obligations to monitor and report suspicious transactions to the Compliance Officer and the importance of KYC and CDD.

49. Front-Line employees must be trained to conduct effective KYC at the time of on-boarding, on-going CDD, detecting suspicious transactions and on the measures that need to be taken upon determining that a transaction is suspicious. Training should also be provided on factors that may give rise to suspicion and the circumstances where enhanced CDD is required.

50. *Employees Responsible for Establishing Business Relationships* - the training for employees who establish business relationship must focus on customer identification, verification and

CDD procedures, including when to conduct enhanced CDD and circumstances where there is a need to defer establishing business relationship with a new customer until CDD is completed satisfactorily.

51. *Board/Officials/Senior Officers* - training provided to Board and the relevant Officials/Senior Officers shall include all aspects of AML/CFT/CPF procedures, in particular, the risk-based approach to CDD, risk profiling of customers, enforcement actions that can be taken for instances of non-compliance with the requirements pursuant to the relevant laws and regulations.

55. In addition to the AML/CFT/CPF trainings provided to the relevant staff, general awareness must be created for staff members on:

    (a) The relevant laws and regulations and guidelines,

    (b) The institution's internal AML/CFT/CPF policies and procedures.

    (c) The relevant documents on the enforcement of AML/CFT/CPF issued by other statutory bodies including the FIU;

    (d) Recent or emerging trends on money laundering and terrorism financing.

Independent Audit Function

56. The Board must ensure regular independent audits of the AML/CFT/CPF measures implemented by the institution in order to determine their effectiveness and compliance with the AML/CFT Act 2009, its amendments, implementing regulations, AML/CFT/CPF guidelines issued by the Bank and the FIU as well as other relevant laws and regulations of other supervisory authorities where applicable.

57. The Board shall also ensure that the roles and responsibilities of the auditor are clearly defined and documented. The roles and responsibilities of the auditor shall include, at a minimum:

(a) checking and testing the compliance with, and effectiveness of the AML/CFT/CPF policies, procedures and controls;

(b) Assessing whether current measures are in line with the latest developments and changes to the relevant AML/CFT/CPF requirements.

58. The scope of independent audit shall include, at a minimum:

(a) compliance with AML/CFT Act 2009, its amendments, regulations, guidelines and other legal and prudential requirements;

(b) Compliance with the institution's internal AML/CFT/CPF policies and procedures;

(c) Adequacy and effectiveness of the AML/CFT/CPF compliance program; and

(d) Reliability, integrity and timeliness of the internal and regulatory reporting and management of information systems.

59. The PSP must ensure that the auditor submit a written audit report to the Board to highlight an assessment of the effectiveness of AML/CFT/CPF measures and any inadequacy in internal controls and procedures.

60. The records of such audit findings and necessary corrective measures undertaken are maintained and must be made available to the regulator and other statutory bodies upon request.

PART III – COMPLIANCE MEASURES

KYC and CDD

61. PSPs must have clear customer acceptance policy that outlines the necessary steps to identify and verify the true identity of customers registering for a payment service.

62. Satisfactory evidence must be maintained of the identity and legal existence of the customer and beneficial owner at the point of establishing the business relationship.

63. PSPs shall not maintain anonymous mobile payment wallets or wallets in fictitious names.

Requirements for Conducting KYC and CDD

64. PSPs are required to conduct KYC/CDD on the customer and the person conducting the transaction, when:
    - a customer registers a mobile payment account;
    - there is any suspicion of ML/TF/PF, regardless of amount;
    - There is any doubt about the validity, veracity or adequacy of previously obtained information.

Customer Identification Procedures

For Natural Persons

65. The PSP must obtain sufficient information to establish to it's satisfaction, the identity of each new customer using reliable independent reliable source documents including, government issued national identification card/passport/drivers' license, and proof of income.

For Legal Persons

66. For customers who are legal persons and legal arrangements e.g. companies, societies and charities the PSP must:
    - Verify the legal status of the entity through proper and relevant official document

- Obtain from the legal person a letter of authorization, resolution or other acceptable and legal documents indicating that the person(s) purporting to act on their behalf are authorized to do so.
- Understand the ownership and control structure of the customer to determine the ultimate beneficial owner(s).

CDD Related to Combating the Financing of Terrorism

67. For cross-border transactions, PSPs are required to keep up to date with the various resolutions passed by the United Nations Security Council (UNSC) under the authority of Chapter VII of the United Nations' Charter on counter terrorism measures in particular the UNSC Resolutions 1267 which require sanctions against individuals and entities belonging or associated with Terrorists.

68. Institutions are required to ensure they do not open mobile payment accounts or conduct transactions with or involving the individuals and entities the UNSC designates as per the 1267 Resolution. In addition to sanction lists, PSPs must also take all the necessary steps to ensure other applicable UN sanctions on some of the nations are taken into consideration when opening mobile payment accounts and processing transactions.

69. The PSP must implement adequate automated systems to screen the names of new customers, as well as to conduct regular checks on the names of existing customers and potential customers, against the names of designated individuals on the UN Sanctions list.

70. Where a match is found after screening, the PSP must immediately:
    - freeze the customer's funds or block the transaction, where it is an existing customer
    - reject the potential customer if the transaction has not commenced,
    - submit a suspicious transaction report to the FIU

71. PSPs shall also file with the FIU a suspicious transaction report when there is an attempted transaction involving any of the persons listed in the UN consolidated lists.

72. PSPs must also consolidate their database with the other recognised lists of designated persons or entities issued by the Government of Guyana and, where applicable, other jurisdictions.

Measures to Mitigate Proliferation Financing

73. Proliferation financing risk can be mitigated by implementing strong controls, conducting risk assessment of customers and products, and the application of customer due diligence measures, including enhanced due diligence on high-risk customers and transactions.

74. PSPs must adopt a risk-based approach to managing their PF risk exposure. In order to apply this approach, they must understand the PF risks based on the risk factors discussed at paragraph 22 of this guideline.

75. The CDD measures for PF include identifying and understanding the ultimate beneficial owners of customers, assessing proliferation financing risks associated with customers and transactions, and implementing risk-based controls like continuous monitoring, transaction screening, and staff training to mitigate these risks.

76. **Key CDD measures for Proliferation Financing include:**

- *Customer Risk Assessment* - PSPs must implement robust processes to identify customers who pose a higher level of proliferation financing risk,
- *Conduct due diligence on beneficial owners* - Understand the ultimate beneficial owners of customers, especially those involved in high-risked regions and industries related to proliferation,
- *Transaction Monitoring* - PSPs must pay close attention to the pattern of transactions conducted by customers which could be used to acquire or transfer sensitive good, service,
- *Assess geographic risk* - Evaluate the geographic risks associated with customers and their transactions, as some regions may pose a higher risk for proliferation financing.

- *Implement Automated Sanctions Screening* - Use automated systems to screen transactions and customers against sanctions and other watch lists to detect suspicious patterns of transactions for potential links to proliferation
- *Conduct ongoing due diligence* - apply ongoing due diligence measures throughout the life cycle of the customer.
- Conduct regular staff *training*.

77. **Freezing of Mobile Wallets**

PSPs must place a hold on any account meeting the following criteria when implementing targeted financial sanctions:

- the wallet represents funds that are owned or controlled by designated person or entity, beyond those that can be tied to a particular act, plot or threat of proliferation,
- the wallet represents funds that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities,
- the wallet represents funds derived or generated from funds derived funds or other assets owned or controlled directly or indirectly by designated persons or entities, and
- The wallet represents funds or other assets of persons and entities acting on behalf of or at the direction of designated persons or entities.

78. All transactions must be screened in real time and monitoring must be done to detect any transactions that must be stopped to take further action where necessary. If a customer attempts to make a transfer to an individual or entity subject to UN sanctions, the PSP must take the following steps immediately if a match is found:

- hold the funds that would have been the subject of the transaction,
- File an STR with the FIU. and
- Inform the relevant supervisory authorities.

79. The funds shall remain with the PSP until the competent authorities have carried out full investigations into the purpose of the payment and the nature of the customer's relationship with the designated person. The PSP must comply with the directions of the supervisory authority or other relevant body regarding the ultimate disposition of the funds.

Reporting

80. PSPs must immediately implement a designated order, and report any actions taken in accordance with the designation to the relevant supervisory authorities within 48 hours of issuance of the designation order. This include:
    - any accounts frozen,
    - any transactions stopped, on hold, or blocked,
    - all screening performed, and
    - any other efforts to comply with sanctions.

81. PSPs must report to the relevant supervisory authorities within 30 days after issuance of the designation order whether or not they have taken any additional actions.

82. Once the above reports have been made, the PSP is required to report if they have frozen any additional wallets/funds or blocked any transactions and the accounts involved should be subject to enhanced monitoring.

On-Going Due Diligence

73. PSPs are required to conduct on-going due diligence on all its customers. Such measures shall include:
    - scrutinising transactions undertaken throughout the course of that account to ensure that the transactions conducted are consistent with the PSP's knowledge of the customer, their business and risk profile, including where necessary, the source of funds;
    - ensuring that documents, data/information collected under the CDD process is kept current, up-to-date and relevant, by undertaking reviews of existing records particularly for higher risk customers.

74. When conducting on-going due diligence, PSPs may take into consideration the economic background and purpose of all transactions or the account which:
    - appears unusual;
    - is inconsistent with the expected type of activity and business model when compared to the volume of transaction;

- does not have any apparent economic purpose;
- casts doubt on the legality of such transactions, especially with regard to complex and structured transactions or involving higher risk customers; or
- casts doubt about the veracity of previously provided information.

75. The frequency of the on-going due diligence or enhanced on-going due diligence, as the case may be, shall be commensurate with the level of ML/TF/PF risks posed by the customer based on the risk profiles and nature of transactions.

76. When conducting enhanced due-diligence PSPs may increase the intensity, frequency, and timing of controls to select patterns of transactions that need further examination.

Politically Exposed Persons (PEP)

77. PSPs are required to take reasonable measures to determine whether the beneficiaries and/or, where required, the beneficial owner of the beneficiary, are politically exposed persons. PEPs are defined as any person (foreign or domestic) who is or has been entrusted with prominent public functions in Guyana or any foreign country as well as members of such person's family and their close associates.

78. These include:
    - heads of states (example: presidents, vice presidents and prime ministers)
    - cabinet members and state ministers
    - members of parliament
    - judges and magistrates
    - elected members
    - senior officials of a state agency or institution
    - senior military officials
    - board members of state owned enterprises
    - senior officials appointed as per the provisions of a specific law
    - senior political appointees of a government
    - foreign and local diplomats
    - senior political party members

79. If the customer, a beneficial owner or the beneficiary is a PEP, the PSP shall assess the level of ML/TF/PF risks posed by the business relationship with the PEP; risk assessment shall take into account the profile of the customer. Generally, all PEPs, whether shall be categorized as high, medium or low- risk.

80. The PSPs may conduct enhanced due diligence on PEPs, whether previous or current, depending on the level of risk posed by the PEP and their capacity to influence public functions.

New Products/Services

81. PSPs shall identify and assess the ML/TF/PF risks that may arise in relation to the development of new products and services, including new delivery mechanisms, change in wallet size, transaction limits, and the use of new or developing technologies for both new and pre-existing products offered on mobile payment accounts. PSPs must:
    - undertake the risk assessment prior to the launch of such products, services and technologies;
    - take appropriate measures to manage and mitigate the risks.

Reliance on Third Parties

82. PSPs may rely on third parties, such as agents to conduct CDD or to introduce business. However, the ultimate responsibility and accountability for CDD measures shall remain with the PSP. PSPs are also responsible for providing training to those third parties on applicable AML/CFT/CPF compliance issues.

83. PSPs must have in place internal policies and procedures as well as controls to mitigate risks when relying on third parties. The relationship between PSPs and the third parties relied upon to conduct CDD shall be governed by an arrangement that clearly specifies the rights, responsibilities and expectations of all parties.

84. At the minimum, the PSP must be satisfied that the third party:

- can obtain immediately the necessary information concerning CDD as required under applicable laws and regulations;
- has an adequate CDD process;
- has measures in place to meet record keeping requirements;
- can provide the CDD information and provide copies of the relevant documentation immediately upon request;
- is properly regulated and supervised by the relevant supervisory authorities.

High Risk Countries

85. PSPs are required to conduct enhanced CDD for payment accounts and transactions with any person from countries identified by the Financial Action Task Force (FATF), other competent bodies, such as the FIU as having a substantial level of ML/TF/PF risks.

86. Where there is higher ML/TF/PF risks, PSPs are required to conduct enhanced CDD for accounts and transactions with any person from countries identified by the FATF, as having strategic AML/CFT/CPF deficiencies and have not made sufficient progress in addressing those deficiencies.

87. If the institutions are unable to comply with the CDD measures they shall not open the account or conduct any transaction in relation to the potential customer, or shall terminate the payment account in the case of an existing customer, if the MPSP is unable to comply with the prescribed CDD requirements.

88. Similar steps must be taken where the person acting on behalf of the beneficiary is unable to or refuses to provide the information on the identity of the beneficiaries, where applicable. In addition, based on the ML/TF/PF risk, the PSPs must also consider filing a suspicious transactions report in such circumstances.

Resource Allocation

89. PSPs must allocate adequate resources, to complement its CDD process in order to ensure timely information is available on a regular basis to enable the detection of irregularity/suspicious activity. The allocated resources must be commensurate with the nature, scale and complexity of the PSP's activities and ML/TF/PF risk profile.

Monitoring and Reporting

90. PSPs are required to establish proper customer and transactions monitoring systems to ensure that all the customers and transactions are monitored to detect any unusual activity. The system shall also include a reporting mechanism for the submission of suspicious activity reports and other reports which the service provider is legally required to submit.

91. Institutions must also establish internal criteria, such red flags to detect suspicious transactions, and to monitor customers and transactions against those red flags.

92. The institutions may be guided by case studies and examples of suspicious transactions and red flags provided by the FIU or international organisations from time to time and may incorporate those red flags in their monitoring and reporting system.

93. PSPs shall investigate transactions that are unusually large/complex, that have an unusual pattern, and which do not have an apparent lawful economic purpose. As part of transaction monitoring and reporting function, PSPs must ensure that transactions or series of transactions will not facilitate the transfer of the proceeds of crime or property connected to financing of terrorism, and, where applicable, all payment accounts and transactions must be screened for involvement with any person designated by the UNSCRs.

94. In addition, PSPs shall pay special attention to mobile payment accounts and transactions with persons, including legal persons from countries that do not apply the relevant international standards to combat ML/TF/PF.

95. The following are examples of potentially suspicious activities, or "red flags" for money laundering and terrorist financing:

- Frequent cash-ins and cash-outs by customers and third parties
- Unusual frequent person to person transfers, especially to unrelated parties.
- Transactions deviating from normal transactional pattern/behavior
- One unregistered or registered person doing cash-ins to many mobile wallets
- One person withdrawing from many mobile wallets

96. Although these red flags are not exhaustive, they may assist the institution to recognize possible money laundering and terrorist financing activities. PSPs are required to have specific red flags incorporated in their systems for monitoring suspicious transactions and for risk mitigation purposes.

97. The presence of a red flag may not necessarily mean that the transaction is suspicious. However, it may warrant further investigation prior to submitting a suspicious transaction report to the FIU.

Suspicious Transaction Reporting

98. PSPs are mandated to submit suspicious transactions report to the FIU under the following circumstances, as soon as practicable, but not later than 3 working days:

- where the PSP suspects or have grounds to suspect that funds or property are proceeds of crime, or are related to ML/TF/PF.
- where a person or an entity designated pursuant to UNSCRs attempted to establish a business relationship with the institution or is party to a transaction conducted or attempted transactions.
- where the PSP is about to conduct a transaction or series of transactions which facilitated or is likely to facilitate the transfer of the proceeds of crime or property connected to financing of terrorism.
- any other suspicious activity the PSP deems important to be reported.
- PSPs may also consider submitting a suspicious transaction report when any of its customer's transactions/attempted transactions fits the PSP's list of "red flags". The manner and form for submitting reports will be as prescribed by the FIU.

99. The Compliance Officer shall have the sole discretion and independence to report suspicious transactions. It is the duty of the Compliance Officer to maintain complete records on all internally generated STRs and any supporting documentary evidence regardless of whether such reports have been submitted to the FIU.

100. The Compliance Officer must ensure that all suspicious transaction reports are submitted to the FIU within three working days, from the date the Compliance Officer establishes the suspicion.

101. PSPs must provide additional information and documentation requested by the FIU and to respond promptly to any further enquiries made. In addition, institutions must also must ensure that in the course of submitting the suspicious transaction report, utmost care is undertaken to ensure that such reports are treated with the highest level of confidentiality.

102. PSPs must also ensure that the suspicious transaction reporting mechanism is operated in a secure environment to maintain confidentiality and preserve secrecy. Where a suspicious transaction report has been lodged, PSPs are not precluded from making a new suspicious transaction report as and when further suspicion arises. It is recommended that PSPs should continue monitoring the activities of the customer after filing a suspicious transaction report with the FIU.

Tipping Off

103. A PSP, its directors, officers and employees, shall not disclose to its customers or a third party that a STR, and/or information on a customer is being, was or will be provided to the FIU or that a ML/TF/PF investigation is being carried will be carried out. Stringent policies, procedures and internal controls must be in place to ensure that there is no breach in confidentiality. However, no proceeding shall be brought against the PSPs or their directors, officers or employees who provided information in good faith.

Record Keeping

104. PSPs should develop clear standards for maintaining records and their retention period. Records must be maintained of the following and must remain current up-to-date and relevant:

a) KYC and CDD information of customers including the copies of information verification documents;

b) information on suspicious transaction reports submitted to the FIU including information and records on internal investigations conducted on matters considered suspicious;

c) employee due diligence information and reports and training and awareness records;

f) risk assessment reports;

g) AML/CFT/CPF review reports; and

h) internal and external audit reports.

Institutions shall be guided by the record retention period requirements stipulated in the AML/CFT Act 2009.