Reserve Bank of Fiji
Payment Service Provider Supervision Policy
Statement No: 2

MINIMUM REQUIREMENTS FOR THE MANAGEMENT OF MONEY LAUNDERING AND TERRORIST FINANCING RISK

NOTICE TO LICENSED PAYMENT SERVICE PROVIDERS

Reserve Bank of Fiji
January 2026

PART 1: PRELIMINARY

1.0 Introduction

1.1 This Policy is issued under section 6(1)(a) of the National Payment System Act 2021, section 36 of the Financial Transactions Reporting Act 2004 ("FTR Act 2004" or the "FTR Act") and sections 35, 36 and 37 of the Financial Transactions Reporting Regulations 2007 ("FTR Regulations") and is applicable to all licensed Payment Service Providers ("PSPs").

1.2 The Policy is also issued in line with the Financial Action Task Force ("FATF") 40 Recommendations.

2.0 Objective of the Policy

2.1 The objective of this Policy is to ensure that licensed PSPs have in place a Money Laundering/Terrorist Financing ("ML/TF") Risk Management Framework that is aligned to their strategy and business plans, and commensurate with the size, complexity and nature of their operations.

2.2 The Policy, therefore, sets out the minimum requirements on establishing a risk management framework, comprising of systems, structures, processes and people within which the institution identifies, assesses, mitigates and monitors money laundering and terrorist financing risk.

3.0 Background

3.1 The increasing sophistication of Money Laundering (ML) and Terrorism Financing (TF) activities, coupled with the growing internationalisation of financial services, has heightened the need for robust regulatory frameworks to safeguard the financial system. This has the potential to adversely affect the country's reputation, investment climate, and may have economic and social consequences. The globalisation of financial services and advancements in technology has posed challenges to regulators and law enforcement agencies as criminals have become more sophisticated in laundering illicit funds and using financial service providers as conduits for ML/TF activities.

3.2 The globalisation of financial markets and the development of information technology have made the movement of funds across borders easier and has further spurred the growth of mobile money transfers.

3.3 In drafting this policy, reference has been made to FATF guidance for a risk-based approach.

4.0 Applicability to Foreign Branches, Subsidiaries, and Agents

4.1 Licensed PSPs are required to ensure that their agents or network of agents meet the requirements of this Policy[1], and the Policy applies to the licensed PSP's agents as if the agent were the entity itself.

4.2 Licensed PSPs are required to closely monitor foreign branches or their subsidiaries in other countries, which may be operating in jurisdictions with inadequate anti-money laundering/combating the financing of terrorism (AML/CFT) laws.

4.3 Licensed PSPs are required to ensure that their foreign branches, subsidiaries and agents apply AML/CFT measures in a manner that is consistent with the AML/CFT requirements in Fiji. Where the minimum AML/CFT requirements of the host or the home country are less stringent than those of Fiji, licensed PSPs must apply Fiji's AML/CFT requirements, to the extent that host country laws and regulations permit.

4.4 If the host or home country does not permit the proper implementation of AML/CFT measures in a manner that is consistent with the AML/CFT requirements in Fiji, licensed PSPs are required to apply appropriate additional measures to manage the ML/TF risks, and adequately report to the Reserve Bank of Fiji on the AML/CFT gaps and additional measures implemented to manage the ML/TF risks arising.

PART 2: MINIMUM REQUIREMENTS

5.0 Risk-Based Approach

5.1 In meeting their obligations under this Policy, licensed PSPs must undertake a risk-based approach. Licensed PSPs must identify, assess and understand the ML/TF risks which they are exposed to, and implement AML/CFT measures commensurate to their risk profile, proportionately based on their size and complexity of operations, in order to mitigate them effectively and efficiently.

5.2 Licensed PSPs must utilise the Customer Due Diligence (CDD) and other guidelines, policy advisories issued by Financial Intelligence Unit in Fiji ("FIU"), from time to time. Refer to Advisory on Risk Based Approach[2] and Identification and Verification of Occasional Customers[3] as well as Enforceable Guideline on Higher Risk Countries[4] and Politically Exposed Persons (PEPs)[5].

5.3 At a minimum, each licensed entity before providing a product or service, must identify, assess and understand its ML/TF risk with regard to the following:

a) customer types;
b) the source of funds and source of wealth of customers;
c) the business or occupation of customers;
d) the types of products and services that it provides;
e) the methods by which it delivers designated products and services; and
f) the foreign jurisdictions it has dealings with, and the ML/TF risk controls of that country.

[1] Section 25(2) of the National Payment System Act 2021
[2] Advisory 5/2007, Date: 22/06/07, Risk Based Approach
[3] Advisory 4/2007, Date: 22/06/07, Identification and Verification of occasional customers
[4] Guideline 6 - Higher Risk Countries
[5] Guideline 7 - Politically Exposed Persons (PEPs)

5.4 Licensed PSPs must document the measurement techniques that they apply, the reasons for the use of this measurement technique and the associated procedures that will enable the assessment and quantification of ML/TF risk, and its impact on their operations.

6.0 Money Laundering/Terrorist Financing Risk Management Framework

6.1 Licensed PSPs are required to establish and implement an effective ML/TF Risk Management Framework. At a minimum, a licensed entity's risk management framework must establish procedures to comply with the requirements of the FTR Act, FTR Regulations, and other policies and guidelines issued by the Reserve Bank of Fiji or the Fiji FIU from time to time. The risk management framework must include procedures and systems that include the following:

a) implementing customer identification requirements;
b) implementing record keeping and retention requirements;
c) implementing processes and systems for monitoring customers;
d) implementing reporting requirements;
e) making its officers, employees, and agents aware of the laws and policies for compliance with the AML/CTF standards;
f) training its officers, employees and agents to recognize suspicious transactions;
g) screening potential employees and agents, and monitoring fitness and propriety on an on-going basis;
h) appointing a compliance officer to be responsible for ensuring the licensed entity's compliance with the requirements of the FTR Act[6]; and
i) establishing an audit function[7] to test its procedures and systems to comply with the requirements.

6.2 Each licensed PSP is required to prepare a customer profile for its ongoing business relationships by collating all necessary information obtained through CDD measures. This will determine the level and type of ongoing monitoring, and support its decision whether to enter into, continue or terminate a business relationship. Where the appropriate level of CDD is not possible, licensed PSPs must not enter into a business relationship or carry out an occasional transaction or terminate an already-existing business relationship; and consider filing a suspicious transaction report in relation to the customer.

6.3 Licensed PSPs also deal with agents in their business, whereby settlement between them may be undertaken through cash courier, net settlement, or other mechanisms without any direct wire transfers between the originator and beneficiary to transfer funds. As such, it is essential that prior to entering a new relationship with an agent, licensed PSPs must:

a) identify and verify the agent with whom it conducts a business relationship;
b) gather information about the nature of its business;
c) determine from publicly available information the reputation of the agent and the quality of supervision it is subject to;

[6] Refer to Section 21(2) of FTR Act and Section 31 of FTR Regulations
[7] Refer to paragraph 10.2

d) assess the agent's anti-money laundering and combating terrorist financing controls;
e) document an agreement with the agent and clearly outline the responsibilities of the licensed PSP and the agent. The written agreement must outline that:
    i. the agent would conduct customer identification requirements equivalent to Fiji's requirements; and
    ii. where required, the agent will make information available to the licensed entity without delay.
f) obtain approval by senior management before establishing a new intermediary relationship; and
g) conduct a review of the relationship on an annual basis.

6.4 Licensed PSPs are required to develop as part of their ML/TF Risk Management Framework, an Anti-Money Laundering/Combating of Financing of Terrorism ("AML/CFT") Policy that outlines the licensed PSPs' approach to managing ML/TF risk and the processes involved. At a minimum, the internal AML/CFT Policy must include measures for:

a) customer due diligence, in compliance with Sections 4, 6 and 7 of the FTR Act and sections 5 to 12, 14 & 20, 21, 22 of the FTR Regulations and the Fiji Financial Intelligence Unit ("FIU")'s Policy Advisories issued from time to time. Refer to Guidelines on Customer Identification & Verification[8]; Guidelines on Politically Exposed Persons (PEPs)[9], Guidelines on Use of Digital ID Systems/eKYC for Customer Due Diligence[10];
b) relationships with Agent:
    i. for any business transactions conducted through its agents, PSPs must enforce requirements on their agents to comply with the requirements of CDD of the PSP including Recognition and Reporting of Suspicious Transactions as required;
    ii. PSPs are required to set out the processes that must be undertaken by the agents in conducting CDD as well as appropriate enforceable action by PSPs in its arrangement or agreement with the agents for failure to conduct CDD.
c) record keeping and retention as per the requirements of sections 8 and 9 of the FTR Act;
d) on-going monitoring of transactions as per the requirements of sections 10 and 11 of the FTR Act and sections 17 & 18 of the FTR Regulations;
e) protection of persons and information in suspicious transaction reports as per the requirements under Section 19 and 20 of the FTR Act;
f) recognition and reporting of suspicious transactions in compliance with the requirements of sections 14 and 18 of the FTR Act and sections 24, 27, 28 of the FTR Regulations;
g) reporting of cash transactions and electronic fund transfers as per the requirements under section 13 of the FTR Act and sections 25, 26, 27, 28 of the FTR Regulations[11];
h) recording information on the originators and beneficiaries of wire transfers as per the requirements of section 12 of the FTR Act, sections

[8] Guideline 4 – Customer Identification & Verification
[9] Guideline 7 – Politically Exposed Persons (PEPs)
[10] Guideline 10 - Use of Digital ID Systems/eKYC for Customer Due Diligence
[11] EFTR form requires details of both originator and beneficiary to be collected

19,23, 26, 28 of the FTR Regulations and the requirements of the EFTR form;

i) the development of new products, new business practices, including new delivery mechanism and the use of new or developing technologies for both new and pre-existing products as per requirements under the FIU's Enforceable Guideline on New Technologies[12]. Furthermore, licensed PSPs must undertake risk assessments which include assessing ML/TF risk prior to the launch of a product, process or technology and implement appropriate measures to manage and mitigate identified risks; and

j) AML/CFT training program for all its officers and employees as per section 21 of the FTR Act and section 33 of the FTR Regulations.

6.5 Furthermore, each PSP must ensure that its internal AML/CFT Policy complies with all the relevant requirements outlined in the FIU's policy guidelines and policy advisories.

6.6 The AML/CFT Policy must be documented, easily understood, auditable, accessible to all staff and reflective of the size, complexity and nature of the PSP's ML/TF risk profile and exposure. Furthermore, the AML/CFT Policy must be approved by the Board or its proxy.

6.7 Licensed PSPs must regularly review and update the documents, data or information collected under their internal AML/CFT Policy so that it complies with the prevailing regulatory requirements with regards to ML/TF risk, for example, changes or additions to FIU guidelines.

7.0 Roles and Responsibilities of the Board

7.1 The ultimate responsibility and accountability for ensuring the licensed PSP's compliance with this Policy, the AML/CFT laws such as the FTR Act and FTR Regulations, FIU Guidelines and Policy Advisories, rests with the licensed PSP's board or proxy.

7.2 At a minimum, the Board or its proxy is required to:

a) identify and understand the ML/TF risks faced by the licensed PSP on an on-going basis;

b) ensure the safety and soundness of the licensed PSP by establishing an appropriate, adequate and effective system for ML/TF risk management framework which is aligned with the requirements of the FTR Act, FTR Regulations, FIU's policy advisories and guidelines;

c) ensure that senior management implements documented policies and procedures for the management of ML/TF risk, have a system of reviewing compliance with the same and detecting any exceptions to documented policies;

d) approve the policies and procedures for the evaluation and management of ML/TF risk;

e) review and approve the ML/TF Risk Management Framework annually or whenever there are changes in circumstances that could impact on ML/TF risk; and

[12] Guideline 5 - New Technologies

f) monitor and review the internal audit function periodically as needed.

8.0 Role and Responsibilities of Senior Management

8.1 The responsibilities of the Senior Management include, at a minimum:

a) developing effective internal policies, procedures and controls that identify, measure, manage and monitor the ML/TF risk faced by the licensed PSP;
b) effectively implementing the ML/TF risk management framework approved by the Board and provide periodic[13] reports on its effectiveness to the Board;
c) ensure that the licensed entity complies with the FTR Act and FTR Regulations, and the FIU's policy advisories and guidelines;
d) monitoring changes to AML/CFT standards and laws and informing the board of any policies/procedures that require changes;
e) monitoring appropriateness, adequacy and effectiveness of the ML/TF risk management system on an on-going basis;
f) ensure that employees are free of criminal offences involving fraud and dishonesty and have the necessary competence to carry out their duties;
g) ensure that all officers and employees are provided with training on an on-going basis with regards to AML/CFT laws and the company's internal policies and procedures relating to AML/CFT standards;
h) assist and cooperate with the relevant law enforcement authorities in Fiji such as Financial Intelligence Unit and Fiji Police Force, in investigating money laundering and terrorist financing activities; and
i) establish effective reporting to the Board on all relevant requirements.

8.2 Senior Management must develop (document) the ML/TF risks profile of the institution to understand where vulnerabilities reside. Key aspects of the ML/TF risk profile would include but are not limited to:

a) customer base characteristics (such as types of customers, geographic distribution);
b) products and services offered;
c) delivery channels used (including agents, intermediaries, and non-face-to-face interactions);
d) number and location of branches, subsidiaries, and counterparties;
e) economic sectors where business is concentrated; and
f) risk factors that would impact the ML/TF risk assessment of the institution.

8.3 The ML/TF risk profile must be prepared every two years or more frequently if there are significant changes in business operations or regulatory requirements.

9.0 Roles and Responsibilities of the AML Compliance Officer

9.1 Licensed PSPs must comply with section 21(2) of the FTR Act and section 31 of the FTR Regulations which stipulate that licensed PSP must appoint an AML compliance officer at the management level to perform the following functions:

[13] At least quarterly

a) be responsible for ensuring compliance with the FTR Act, FTR Regulations and other related policies and guidelines;
b) be given appropriate and adequate authority and responsibility to implement the requirements of the FTR Act and FTR Regulations; and
c) have the authority to act independently and to report to senior management above the compliance officer's reporting level.

9.2 The AML Compliance Officer and other employees designated by such officer must have timely access to customer identification data and other customer due diligence information, transaction records and other relevant information.

9.3 The AML Compliance Officer must report to the FIU, in the prescribed form and manner, any suspicious transactions under section 14 of the FTR Act, and Cash Transaction Reporting (CTR) according to the FIU Notices issued under the FTR (Amendment) Act 2022.

9.4 Furthermore, the AML Compliance Officer must ensure that all employees and officers are aware of the laws, procedures and policies relating to money laundering and financing of terrorism. As per section 21 (2) of the Act and section 33 (3) of the Regulations, staff training should include new developments, recent trends in money laundering and identification of suspicious transactions.

10.0 Roles and Responsibilities of the Internal Audit Function

10.1 Licensed PSPs must, under section 21 (3) of the FTR Act and section 32 of the FTR Regulations, establish an audit function[14] to test its procedures and systems for combating money laundering and financing of terrorism.

10.2 The PSP's audit function must test compliance (including sample testing) with the procedures, policies and controls required, including:

a) attestation of the overall integrity and effectiveness of the written procedures, policies, systems, and controls and technical compliance with the Act and FTR Regulations;
b) transaction testing in all areas of the PSP with emphasis on high-risk areas, products and services to ensure that the PSP is complying with the Act and FTR Regulations;
c) assessment of the employees' knowledge of procedures, policies, systems, and controls;
d) assessment of the adequacy, accuracy, and completeness of employee training programmes; and
e) assessment of the adequacy and effectiveness of PSP's process for identifying and reporting suspicious transactions and activities, and other reporting requirements under the Act and FTR Regulations.

10.3 The internal audit function must report to the Fiji FIU any suspicious information or transactions noted during the internal audit[15].

[14] An internal audit function that is independent of the activities audited should be sufficient and commensurate to their risk profile, proportionately based on their size and complexity of operations

[15] Section 15 of the FTR Act 2004

PART 3: OVERSIGHT AND IMPLEMENTATION ARRANGEMENTS

11.0 Oversight by the Reserve Bank of Fiji

11.1 For the purpose of this Policy, all licensed PSPs are required to provide to the Reserve Bank, their AML/CFT Policy, within 3 months after the implementation of this Policy**.** In the event of material changes made to the management of ML/TF risks, a copy of the revised Policy must be submitted to the Reserve Bank within 30 days after changes have been approved by the board.

11.2 The Reserve Bank will assess the compliance of each PSP with the requirements of this Policy in the normal course of its supervision.

11.3 Non-compliance with this Policy may result in sanctions, as provided under section 24(6) of the National Payment System Regulations 2022, and further sanctions under the FTR Act 2004 and the FTR Regulations 2007.

12.0 Reporting to the Reserve Bank of Fiji

12.1 The Reserve Bank may require from time to time, ML/TF risk management information, in a format specified, to meet the objectives of this policy.

12.2 PSPs need to conduct thorough risk assessments to identify, understand, and evaluate the ML/TF risks associated with their products, services, delivery channels, customers, and geographic locations. This assessment report is to be provided to the Reserve Bank on an annual basis.

13.0 Implementation Arrangements

13.1 This Policy applies to all payment service providers licensed under the National Payment System Act 2021.

13.2 This Policy becomes effective from 01 June 2026.

Reserve Bank of Fiji
January 2026

Attach:
Schedule: Interpretation

SCHEDULE

Interpretation -

(1) Any term or expression used in this Notice that is not defined in this Notice:

a) which is defined in the Act shall, unless the context otherwise requires, have the meaning given to it by the Act;
b) which is not defined in the Act and which is defined in any of the Reserve Bank of Fiji Policy Statements shall, unless the context otherwise requires, have the meaning given to it by those policy statements; and
c) which is not defined in the Act or in any of the Reserve Bank of Fiji's Policy Statements shall, unless the context otherwise requires, be interpreted in accordance with generally accepted accounting practice.

(2) In this Notice, unless the context otherwise requires:

Act: means the Financial Transactions Reporting Act 2004 unless otherwise specified as the National Payment System Act 2021.

Agent: means a person that has been contracted by a payment service provider to provider a payment service on behalf, and in the name, of the payment service provider in the manner specified in the National Payment System Act 2021.

Board: means the board of directors of the payment service provider.

Money Laundering/Terrorism Financing risks: risks relating to e-money accounts and transactions being used to launder criminals' money and/or to finance terrorist activities

Payment Service: means a service enabling cash deposits or withdrawals, the execution of payment transactions, the issuance or acquisition of payment instruments and any other service functional to the transfer of money, including the issuance of electronic money, electronic money instruments and electronic money services provided by a mobile network and other operators, but does not include the provision of solely online or telecommunication services or network access.

Payment Service Provider: means an entity providing a payment service.

Proxy: for the purpose of this Policy is relevant to licensed payment service providers which operate as a branch in Fiji. Foreign incorporated licensed entities must appoint a board proxy (whether a director or senior executive or a committee) outside the Fiji operations, with delegated authority from the board who will be responsible for overseeing the Fiji branch operations.

Senior Management: include those persons whose conduct has a significant impact on the sound and prudent management of the PSP's operations, and includes but not limited to Senior Managers, Senior Executives, General Managers/Chief Executive Officer.