Operating Guidelines for

Mobile Money Service Providers (MMSPs)

Reserve Bank of Vanuatu

JULY 2025

Content

1. Introduction

1.1 Purpose of the Guidelines

The Operating Guidelines for Mobile Money Service Providers (MMSP) are issued by the Reserve Bank of Vanuatu (RBV) in accordance with the National Payment System Act No. 8 of 2021. These guidelines aim to establish a structured and transparent operation, supervision, and regulation of MMSPs. The overarching objective of these guidelines is to ensure the sustainable development of mobile money services in Vanuatu while fostering innovation, promoting financial inclusion, and safeguarding the customers and financial system from risks such as fraud, cybercrime, and money laundering.

The guidelines are intended to:

a) Provide clear and consistent rules for the market entry, licensing, and operation of MMSPs.
b) Ensure mobile money services operate safely, securely, and efficiently.
c) Promote sound risk management practices to protect consumers and the broader financial system.
d) Enhance customer trust in mobile money services by ensuring that service providers comply with standards for data protection, customer rights, and consumer redressal.

1.2 Scope and Application

These guidelines apply to all entities operating or intending to operate as MMSPs within Vanuatu. They outline the regulatory requirements for obtaining and maintaining a license, operating mobile money services, managing agent networks, safeguarding customer funds, and complying with the Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) Act (AML/CTF Act) and its Regulations.

Excluded Entities: Licensed banks providing digital financial services directly under their banking license are not subject to these guidelines.

1.3 Definitions and Key Concepts

For these guidelines, the following key definitions are provided to ensure clarity and consistency in their interpretation and application:

Term	Definition
Agent/Mobile Money Agent	Individual/business providing mobile money services for a fee on behalf of Mobile Money Service providers.
AML/CTF	Anti-Money Laundering and Counter-Terrorism Financing as defined under the Anti-Money Laundering and Counter-Terrorism Financing Act, 2014 (amended 2021)
Central Bank	Reserve Bank of Vanuatu
Customer	Customer of the Mobile Money Services
Customer Funds	Funds in the wallet belonging to a customer of mobile money services
Digital Financial Services (DFS)	Financial services that are accessed and delivered mainly through digital channels
Digital Payment	Transfer of value from one payment account to another using digital devices or platforms
Dormant/Inactive Account	Mobile Money accounts with no customer transactions for 6 months
Electronic Money/E E-Money	Monetary value stored electronically as represented by a claim on the issuer
E-Money Issuer	Legal entity authorized to issue electronic money
Fintech	Technology or technology platforms offering or enabling financial services
Float	The total value of electronic money a Mobile Money Service Provider holds on behalf of customers

Term	Definition
Interoperability	Technical or legal compatibility enabling interconnectedness across different mobile money services and platforms
Know Your Customer (KYC)	Procedures and guidelines for verifying the identity of customers before allowing them to open a Mobile Money Account
Merchant	An individual or business entity that accepts mobile money payments for goods or services
Mobile Money	The monetary value of electronic money in a customer's mobile money account
Mobile Money Accounts/Mobile Wallet	Virtual account of a customer held with the Mobile Money Service Provider accessed through mobile devices
Mobile Money Operator (MMO)/Mobile Money Service Provider (MMSP)	An entity authorized and regulated by the Central Bank to provide mobile money services
Mobile Network Operator (MNO)	An entity authorized and regulated by the Telecom Regulator to provide mobile network services
Mobile Money Service	Financial services delivered by a mobile money service provider through a mobile phone ecosystem
Mobile Money Wallet	Mobile money product where the record of funds is stored and accessible through a mobile phone
Multi-factor Authentication (MFA)	Security protocol requiring additional layers for user authentication beyond just a username and password
PIN (Personal Identification Number)	The numerical code serving as a secret authentication method to verify a customer's identity
SIM (Subscriber Identity Module)/e-SIM	Chip-like card inserted or embedded into mobile phones holding subscriber identity data
Suspicious Transaction Report (STR) and Suspicious Activity Reporting (SAR)	Report filed with the Vanuatu Financial Intelligence Unit when encountering suspected money laundering or fraud
Telecom Regulator	Telecommunications, Radiocommunications, and Broadcasting Regulator (TRBR) of Vanuatu
Third-Party Service Provider (TSP)	Person or business to whom a mobile money service provider may outsource part of its responsibilities
Trust Account	Bank account held by the mobile money service provider to park funds equivalent to the total mobile money issued to customers

2. Licensing Requirements

2.1 Eligibility Criteria

The licensing process prescribed below is designed to ensure that only entities with the requisite financial, technical, and operational capacity are permitted to operate as MMSPs. Accordingly, entities wishing to offer Mobile Money Services in Vanuatu must meet the following criteria:

2.1.1. Financial Capacity: Applicants must show sufficient financial capacity, including a minimum unencumbered capital requirement of VUV 5,000,000 for Payment Service Providers as per the last audited balance sheet, to ensure the stability and sustainability of their operations. Funds must be held in a Trust Account with a licensed institution.

2.1.2. Have Technical Competence: The entity must possess the necessary technical infrastructure to support the secure and reliable provision of mobile money services. This includes platforms capable of handling transaction volumes, ensuring data security, and offering system redundancy to avoid service disruptions.

2.1.3. Robust Governance Structures: Applicants must demonstrate sound corporate governance with clear roles and responsibilities for key personnel, including an effective risk management framework that addresses operational, financial, and cybersecurity risks.

2.1.4. Ensure Compliance with Legal and Regulatory Frameworks: Applicants must comply with Vanuatu's existing laws, including a license to operate a business in Vanuatu, AML/CTF ACT and Regulations, as well as Data Protection and Consumer Protection Laws.

2.2 Application and Approval Process

The process for applying for a license to operate as MMSP is designed to ensure that only qualified entities are approved. However, existing providers offering mobile money services based on the "No Objection Letter (NOL)" issued by RBV will have six (6) months from the date of issue of these guidelines to apply for the license as per the procedure detailed herein.

2.2.1. Initial Submission: The applicant must submit a formal application to the RBV in the prescribed format along with the following: -

2.2.1.1. Evidence to prove that MMSP has the prescribed unencumbered minimum capital. With the following key company documents.

2.2.1.1.1. VFSC Business registration

2.2.1.1.2. VFIU registration Letter.

2.2.1.1.3. Memorandum of Association (MoA).

2.2.1.1.4. Article of Association (AoA).

2.2.1.1.5 Details of Sources of Funds for MMSP

2.2.1.1.6. Board resolution approving the company to venture into the MMSP business, physical address of the MMSP, and designating a Point of Contact (PoC) to liaise with RBV on behalf of the company.

2.2.1.1.7. Certified statement of shareholding structure and shareholder approval stating they agree for the company to obtain a license to run the MMSP business in Vanuatu.

2.2.1.1.8. Fit & Proper Checks and KYC of the key company officials.

2.2.1.2. A comprehensive business plan with financial projections for the next 3 years outlining the scope of services, target market, and how these services fit in with its overall business strategy. Organization structure showing how the Mobile Money vertical is positioned within the overall structure, with the designation level of the person heading that vertical. Should also provide any outsourcing plans (if any) intended in the future.

2.2.1.3. List of products and services (both their products and those in partnership with other entities) to be provided through the mobile money platform, with a breakdown of agent commissions and fees to be charged to the customer

2.2.1.4. Criteria for the agent selection and copy of the agent agreement to be used for agent appointment.

2.2.1.5. Onboarding process for the merchants and a copy of the agreement to be signed with the merchants.

2.2.1.6. Copy of Agreement/Terms and Conditions to be used for customers during onboarding/signup for the Mobile Money services, as per Section 35 of the NPS Act.

2.2.1.7. Description of technical capacity, including the platform's capabilities and security standards that they conform to. A description, including diagrams of the configuration of the institution's electronic payment system and its capabilities, showing:

2.2.1.7.1. How the electronic payment system is linked to other host systems or the network infrastructure in the institution.

2.2.1.7.2. Transactions and data flow through the network, settlement process, and timings. This needs to include international remittances.

2.2.1.7.3. Technology/platform vendor and product name.

2.2.1.8. Signed copy of the following policy documents

2.2.1.8.1. IT/Technology security policy.

2.2.1.8.2. Risk management and Compliance Framework that includes cyber security, AML/CTF, and customer data protection and security measures.

2.2.1.8.3. Disaster Recovery and Business Continuity Plan for the systems and technical setup.

2.2.1.8.4. Consumer Protection Policy that includes consumer grievance redressal mechanisms and consumer awareness programs.

2.2.1.8.4. Financial Management and Internal Control Policies

2.2.2. Due Diligence and Background Checks: The RBV will conduct thorough due diligence on the applicant, including checks on shareholders, directors, and key personnel to verify their fitness and propriety. The checks will include assessments of their experience, financial standing, and legal history. RBV may call for more information if needed.

2.2.3. Evaluation of Business Model: The RBV will evaluate the applicant's business model to ensure that it aligns with regulatory objectives, promotes financial inclusion, and does not pose undue risk to the financial system. The business model must be viable and sustainable in Vanuatu's market context.

2.2.4. Technical and Infrastructure Review: The RBV will assess the technical infrastructure of the applicant to ensure that it is robust, secure, and scalable. This includes a review of data protection measures and cybersecurity protocols.

2.2.5. Final Decision: Upon completion of the evaluation, the RBV will issue a decision in not more than 90 days of receiving the application on the following lines.

2.2.5.1. If approved, the applicant will be granted a license to start the Mobile Money services in Vanuatu for the initial period of three years, subject to meeting ongoing compliance and reporting requirements.

2.2.5.2. If the application is incomplete in any manner or requires further clarity, RBV may request additional information. All such information should be furnished by the applicant within 30 days of receipt of the communication from RBV.

2.2.5.3. If the application is denied, the applicant will be provided with the reasons for rejection.

2.3 License Conditions and Obligations

The initial license will be granted for three years and shall be renewed every two years after that. Once licensed, MMSPs must adhere to specific conditions and obligations designed to safeguard the integrity of the mobile money ecosystem and protect consumer interests. These include:

2.3.1. Capital Adequacy and Liquidity Requirements: Licensees must always maintain the minimum unencumbered required capital of VUV 5,000,000 for Payment Service Providers within a Trust Account held with a licensed institution. They are also required to hold liquid assets sufficient to meet their financial obligations, including customer withdrawals and operational expenses.

2.3.2. Trust Account Management: MMSPs must maintain a Trust Account with a licensed commercial bank in Vanuatu, into which customer funds are deposited. The Bank details of the Trust Account shall be provided to RBV before the commencement of the operations by MMSP. The amount in the Trust Account must match the value of the mobile money issued to customers, ensuring that customer funds are always safeguarded. MMSP shall do daily reconciliation of the funds in the Trust Account and document the reasons for differences in the fund value. The reconciliation report needs to be submitted to RBV every week. The trust account cannot be used for any other purpose/ operations except that of mobile money services in Vanuatu.

> 2.3.2.1. An MMSP shall be expected to negotiate the interest rate with the commercial bank/s that maintain the Trust Account.
>
> 2.3.2.2. MMSP will have to mandatorily distribute a minimum of 25% of the interest earned in the Trust Account with the Mobile Money customers in the form of interest payouts. Eligible customers can be determined by the MMSPs basis criteria, like quarterly minimum balance held in the mobile money account, maximum usage, and any other criteria that benefit/incentivize the regular and consistent use of the services.

2.3.3. Reporting Obligations: Licensees are required to submit regular reports to the RBV on key operational metrics, including transaction volumes, customer activity, agent activity, liquidity levels, risk management updates, and compliance with AML/CTF requirements. Licensees will also be required to share the schedule of applicable fees and charges and the list of agents with RBV. The RBV will specify the frequency and format of these reports in line with evolving market conditions.

2.3.4. Onsite and Offsite Supervision: All MMSPs will be subject to onsite and offsite supervision as per the compliance procedures of the RBV.

2.3.5. Compliance with Consumer Protection Rules: MMSPs must adhere to Consumer Protection Guidelines for MMSPs, ensuring transparency in fees and charges, clear communication of terms and conditions, and accessible channels for consumer complaints and dispute resolution.

2.4. License Revocation

The RBV reserves the right to revoke a license if the MMSP is found to be in breach of the regulatory requirements as stated in Section 14 of the NPS Act. In addition, Licenses are non-transferable as stated in Section 15 of the NPS Act.

Grounds for revocation include:

2.4.1. Failure to meet capital requirements.

2.4.2. Failure to maintain a Trust Account or breach in the operations of the Trust Account as stipulated in clause 2.3.2.

2.4.3. Engaging in fraudulent or illegal activities.

2.4.4. Repeated non-compliance with reporting obligations or consumer protection rules.

2.4.5. Merger, Insolvency or financial instability.

2.4.6. The Parent Company licence is suspended or revoked by another Regulator.

In the event of a license revocation, the process as per section 14 of the NPS Act will be followed for orderly wind-down of services. The RBV will oversee this process to protect customer funds and minimize market disruption.

2.5 Winding Up of Operations by MMSPs

Mobile Money Service Providers (MMSPs) may voluntarily cease operations due to business restructuring, mergers, or other valid reasons. The Reserve Bank of Vanuatu (RBV) requires MMSPs to follow a structured and orderly process when winding up their operations to ensure the protection of customer funds and to maintain stability in the mobile money ecosystem.

2.5.1 Notification to the RBV

MMSPs intending to cease operations must notify the RBV in writing at least 90 calendar days prior to the proposed cessation date. The notification must include:

2.5.1.1. Reasons for winding up operations.

2.5.1.2. A detailed plan for winding up, including timelines, steps for notifying customers, and measures to safeguard funds held in the Trust Account.

2.5.1.3. Details of any proposed merger or acquisition, if applicable.

2.5.1.4. Trust Account and Customer Fund Protection

2.5.1.5. MMSPs must ensure that the balance in the Trust Account matches the total outstanding balance of all mobile money accounts at all times during the winding-up process.

2.2.2.6. MMSPs must submit updated records of customer account balances to the RBV and the bank holding the Trust Account.

2.2.2.7. The Trust Account must remain active until all customer funds are either withdrawn, transferred, or allocated to a designated account as directed by the RBV.

2.5.3 Communication to Customers

MMSPs must notify all customers through direct communication channels (SMS, email, or app notifications) and public notices in widely circulated media. Notifications must include:

2.5.3.1. The timeline for ceasing operations.

2.5.3.2. Procedures for cashing out funds or transferring balances to other accounts.

2.5.3.3. Customer support contact details for assistance during the wind-down period.

2.5.4 Timeline for Customer Fund Withdrawals

MMSPs must provide customers a minimum of six months to withdraw their funds or transfer them to alternate accounts.

Any unclaimed funds after the specified period must be transferred to a designated escrow account under RBV supervision for safekeeping and eventual reclamation by customers.

2.5.5 Final Reporting and Compliance

MMSPs must submit a final report to the RBV detailing:

2.5.5.1. The status of all customer accounts.

2.5.5.2. The total amount of funds disbursed or transferred.

2.5.5.3. A reconciliation statement of the Trust Account.

2.5.5.4. The MMSP must surrender its license to the RBV upon completion of the winding-up process.

3. Operational Framework

The Reserve Bank of Vanuatu (RBV) mandates all Mobile Money Service Providers (MMSPs) to adhere to strict operational standards that ensure the safety, efficiency, and sustainability of mobile money services. These standards are designed to protect consumers, promote financial inclusion, and mitigate systemic risks in the financial system.

3.1 Permitted Mobile Money Services

The MMSPSs are permitted to offer any or all of the services listed below:

3.1.1. Mobile Wallets: Virtual accounts held by customers that allow them to store electronic money, transfer funds, and make payments through their mobile devices.

3.1.2. Peer-to-Peer Transfers (P2P): Allowing customers to send and receive money between mobile wallets within the same network or across different networks (where interoperability exists).

3.1.3. Merchant Payments: Enabling customers to pay for goods and services at participating merchants using mobile money and QR Code Payment. This includes payments for any government services and school and college fees.

3.1.4. Bill Payments: Allowing customers to pay utility bills and recurring expenses directly from their mobile wallets.

3.1.5. Airtime Purchases: Mobile money users can purchase airtime for themselves or others using the balance in their mobile wallet.

3.1.6. International Remittances: Subject to RBV's approval to offer international remittance services, MMSPs may offer cross-border remittance services, enabling customers to send or receive money from abroad, following appropriate AML/CTF protocols.

3.2. Prohibited Services and Activities

To maintain the integrity of the mobile money ecosystem and protect consumers, the following activities are strictly prohibited:

3.2.1. Issuing Credit: MMSPs are not permitted to engage in the business of extending loans or offering credit directly through mobile money accounts unless explicitly authorized by the RBV under separate licensing provisions.

3.2.2. Activities restricted under AML/CTF compliance: Any activity that comes under the definition of Money Laundering as per the **AML/CTF Act.** This includes unauthorized cross-border payments.

3.2.3. Unapproved Partnerships: MMSPs are not permitted to offer any service in partnerships with any institution other than those defined as third-party service providers for the delivery of the permitted Mobile Money services in part or in full

3.2.3 The RBV may issue other directives in prohibiting certain services and activities, which risk the integrity of the financial system.

3.3. Merchant Registrations

All businesses, public or private, that want to accept payments for goods and services through mobile money accounts need to be registered as merchants by the MMSPs in their system. MMSPs will onboard all such entities as per the KYC process applicable to the business entities.

MMSPs will maintain a separate merchant code for all the merchants registered in the system. MMSPs will also classify merchant business and sub-business activities as per the classification provided by RBV.

3.4 Transaction Limits

The MMSPs will be required to design their product features in line with the transaction limits prescribed below. These limits have been prescribed to manage risks and ensure consumer protection, as well as to mitigate the potential for fraud, money laundering, and financing terrorism while balancing accessibility and convenience for users.

3.4.1. Domestic Transaction Limits: The following thresholds will apply for daily and monthly transaction volumes, including cash-in, cash-out, and transfer limits. These limits will be reviewed periodically and adjusted based on risk assessments and market conditions.

3.4.1.1. Cash-in and Cash-out transactions will be capped at VUV 100,000 /Day (24-hour period) with a maximum of 3 transactions allowed in a day in the mobile wallet.

3.4.1.2. P2P transactions will be capped at VUV 500,000/Day with a Maximum of 3 transactions allowed in day per wallet.

3.4.1.3. Maximum funds that can be held in the wallet for the customer should not go beyond VUV 1,000,000 at any given point in time.

3.4.1.4. Merchant Payments needs to be identified separately, and there shall be no limit on the number of merchant payments that a person can make in a day provided they have sufficient balance and all other internal risk rules as described in section 6.3 are in place.

3.4.2 Cross-Border Transaction Limits: Additional scrutiny and limits may apply to cross-border transactions, particularly for high-risk jurisdictions or large-value transfers. These transactions must comply with AML/CTF requirements.

3.4.2.1. Inward Remittance:

3.4.2.2. Outward Remittance

3.5. Dormant Accounts and Unclaimed Funds

3.5.1. MMSP shall be required to have in place an operational policy regarding the treatment of dormant accounts and unclaimed funds. All accounts that are not transacted/have no credit or debit activity except interest credit, rewards, cashback, etc., for a continuous period of 3 months will be regarded as dormant accounts. MMSPs will be required to mark/tag all such accounts as dormant in their system for reporting purposes. All these dormant accounts will be required to do a KYC again for reactivation.

3.5.2. MMSPs will close all such accounts after a continuous period of 1 year of no activity if the account balance is less than Vt. 10,000; in case of account balance above Vt. 10,000 the MMSP must wait addition 6 months with reporting to RBV in writing regarding the account and refund the money to the customer or their nominees through other means wherever it is possible to track the customer or when the customer claims the money. If the customer is not reachable, the funds for all such accounts will be moved to an "Unclaimed Funds Account," specifically designated to park unclaimed funds from the closed accounts. The MMSP should demonstrate that it has made possible effort to contact the customer. This includes phone calls and messages, or any other means possible.

3.6 Risk Management Framework

All MMSPs must implement a robust risk management framework to identify, assess, and mitigate risks associated with the operation of mobile money services. This framework must be continuously updated and monitored to ensure alignment with the regulatory requirements set by the RBV.

3.6.1. Operational Risks: MMSPs must have systems in place to manage operational risks, including technology failures, system downtime, and errors in transaction processing. The MMSPs must implement a business continuity and disaster recovery plan to address such risks. RBV mandates an uptime of 99.5% for the systems responsible for the delivery of Mobile Money Services.

3.6.2. Cybersecurity Risks: Given the digital nature of mobile money services, MMSPs must establish comprehensive cybersecurity protocols, including encryption, Multi-Factor Authentication (MFA), and yearly system audits to detect vulnerabilities.

3.6.3. Fraud and Financial Crime Risks: The guidelines require MMSPs to implement measures to detect, prevent, and report fraud, money laundering, and other financial crimes. This includes monitoring suspicious transactions and reporting any concerns to the Vanuatu Financial Intelligence Unit (VFIU) in line with their guidelines.

3.6.4. Customer Protection and Redressal: MMSPs must ensure that there are mechanisms in place to protect consumers from potential risks, including fraud, identity theft, and data breaches. A clear process for dispute resolution must be established, providing customers with accessible channels for lodging complaints and seeking redress.

4. Agent Network Management

The effective management of agent networks is crucial for the successful deployment and expansion of mobile money services in Vanuatu. Agents serve as the primary interface between MMSP and customers, facilitating essential services such as cash-in/cash-out, customer registration, and basic customer support. These guidelines mandate that agents operate with transparency, accountability, and compliance, thereby promoting trust and financial inclusion across the country.

4.1 Agent Onboarding and Due Diligence

MMSPs are required to implement a thorough process for the selection and onboarding of agents to ensure that only competent and trustworthy individuals or entities serve as intermediaries for mobile money services.

4.1.1. Know Your Agent (KYA): MMSPs must conduct comprehensive due diligence on prospective agents. This includes verifying the agent's identity, business registration (if applicable), financial standing, and prior history in handling financial or commercial transactions. Due diligence should mirror the rigor applied in Know Your Customer (KYC) processes.

4.1.2. Background and Risk Assessment: MMSPs must assess potential agents for risks such as prior involvement in fraudulent activities, financial instability, or other factors that could undermine the agent's ability to perform its role effectively and in compliance with regulatory standards.

4.1.3. Capability Assessment: Agents must demonstrate that they possess the infrastructure, financial capacity, and technical skills required to perform mobile money services. This includes ensuring that agents can maintain sufficient liquidity to meet customer demands for cash-ins and cash-outs.

4.1.4. Agent Agreement: MMSPs are required to sign an agreement with every agent that they appoint for the delivery of Mobile Money services. The agreement should clearly define

4.1.4.1. The agent and MMSP's responsibilities and liabilities.

4.1.4.2. The commission structure for the agent for each customer onboarding and transaction type

4.1.4.3. Minimum service levels for the customer handling; and

4.1.4.4. Termination conditions

4.1.5. Training and Certification: Agents must undergo mandatory training on mobile money services, including topics such as transaction handling, fraud prevention, Know Your Customer (KYC) compliance, anti-money laundering (AML), and counter-terrorism financing (CTF) obligations, customer service, and dispute resolution. Upon completion of this training, agents should receive certification from the MMSP, affirming their capability to operate as agents.

4.2 Agent Roles and Responsibilities

Agents play a key role in the delivery of mobile money services and must adhere to a clearly defined set of responsibilities to maintain the integrity and security of transactions.

4.2.1. Customer Onboarding and KYC Compliance: Agents may assist in onboarding new customers by collecting KYC documentation and verifying identity information by doing an initial screening of the documents. The final activation of the customer's mobile money account must be performed by the MMSP after validation of the customer's details. Activations can be done based on the documentation uploaded by the Agent, subject to receipt of the original documentation by the MMSP in 15 days. MMSPs may be fined for the non-availability of the documents of an active Mobile Money Account during the on-site supervision exercise of RBV.

4.2.2. Transaction Facilitation: Agents are authorized to facilitate cash-in and cash-out transactions, balance inquiries, peer-to-peer transfers, bill payments, and other services as approved by the MMSP. These transactions must be conducted in real-time using the mobile money platform to ensure accuracy and traceability. No offline transactions are allowed at the agent points.

4.2.3. Customer Education: Agents are responsible for educating customers about mobile money services, transaction limits, fees, and consumer rights. This is particularly important in rural and underserved areas where financial literacy may be low.

4.2.4. Record Keeping: Agents are required to maintain accurate and up-to-date records of all transactions they facilitate. These records must be generated and stored within the MMSP system and be available for audit and inspection by the RBV. Manual record-keeping is not permitted, except where agents are required to report suspicious transactions or other regulatory breaches.

4.3 Agent Supervision and Monitoring

MMSPs are responsible for the continuous supervision and monitoring of their agent networks to ensure compliance with regulatory requirements and to maintain high standards of service delivery.

4.3.1. Regular Inspections and Audits: MMSPs must conduct periodic inspections of agents, including on-site visits and audits of business premises for at least 30% of the agents in a financial year. These audits should assess the agent's compliance with KYC, AML/CTF requirements, operational guidelines, and customer service standards.

4.3.2. Real-Time Monitoring: MMSPs must deploy digital monitoring systems to track agent activities in real-time. These systems should be capable of flagging suspicious activities, detecting anomalies such as large or unusual transactions, and providing alerts to the MMSP for further investigation.

4.3.3. Performance Reviews: MMSPs must establish a performance review process for agents, ensuring that agents meet the expected service standards. Poor performance, non-compliance, or customer complaints should trigger corrective measures or, in extreme cases, termination of the agent agreement.

4.4 Liquidity Management for Agents

Liquidity management is a critical aspect of agent operations. MMSPs must ensure that their agents have the necessary tools and support to manage liquidity effectively, ensuring that customers can reliably access cash-in and cash-out services.

4.4.1. Pre-Funding Requirements: Agents may be required to pre-fund their accounts with electronic money (float) to handle expected transaction volumes. RBV proposes a minimum pre-funding of VUV 10,000 or more for agents to initiate their business operations. The pre-funding levels should be based on the agent's transaction history, customer demand, and geographic location.

4.4.2. Emergency Liquidity Support: MMSPs must establish mechanisms to provide emergency liquidity support to agents in situations where they run out of cash or digital float. This could include agent-to-agent float transfers, rapid mobile replenishment services, or the deployment of mobile liquidity managers to high-demand areas.

4.4.3. Liquidity Forecasting and Training: MMSPs must provide agents with tools and training to help them forecast customer demand, manage their float effectively, and avoid liquidity shortages. This ensures uninterrupted service delivery, particularly in rural areas where agent liquidity may be limited.

4.5 Agent Exclusivity and Competition

To promote competition, enhance service availability, and ensure the financial viability of agents, they are permitted to represent multiple MMSPs, allowing them to offer services from different service providers at the same time.

4.6 Agent Termination and Exit Procedures

There needs to be clear procedures for the termination of agent agreements and the orderly exit of agents from the market. This is necessary to protect customer interests and ensure continuity of services.

4.6.1. Grounds for Termination: MMSPs may terminate agent agreements for the following reasons

4.6.1.1 Non-compliance with regulatory requirements

4.6.1.2. Poor performance, fraudulent activities, or breach of contract.

Agents must be notified/warned in writing of the reasons for termination and allowed to rectify any deficiencies before termination is finalized.

4.6.2. Exit Strategy: If an agent ceases operations, MMSPs must implement an exit strategy to ensure that customers are informed and that services are transferred to another agent or an alternative delivery channel.

5. Customer Protection

The Reserve Bank of Vanuatu (RBV) places a high priority on protecting the rights and interests of customers using mobile money services. MMSPs are required to adhere to strict customer protection measures that promote transparency, fairness, and security. These measures are essential for building and maintaining customer trust, fostering financial inclusion, and ensuring the long-term success of mobile money in Vanuatu.

5.1 Disclosure of Fees and Charges

MMSPs must display all the fees and charges applicable to customer transactions prominently on their premises at the head office, branch office, and any other place of business. All digital mediums, like apps and websites, should also clearly mention these fees and charges. MMSPs will provide a fees and charges chart to all their agent to be displayed on the agent's premises Agent is expected to explain this chart to the customer before dealing with them.

MMSPs must provide regular updates to customers about their accrued interest and any changes to the terms of interest payments.

5.2 Customer Onboarding

MMSPs shall follow the **Anti-Money Laundering and Counter-Terrorism Financing Act No. 13 of 2014** customer onboarding and due diligence procedures. MMSPs should verify the information produced by the customer using the source documents or the available government and authorized non-government databases, wherever applicable.

5.2.1. Customer Agreements: MMSPs, either directly or through their agents, must sign an agreement/terms and conditions with customers who choose to open a Mobile Money Account or access related services. These terms and conditions should be in accordance with section 35 of NPSA. MMSPs must ensure that customers fully understand the key features and associated costs of the account and services. Customers must confirm their understanding and acceptance of the terms by providing a signature. If a customer is unable to sign, an alternative unique identifier, such as a fingerprint, may be used. Customers who are onboarded through the mobile app through a self-signup procedure can agree to the conditions digitally. The contract must identify the customer and the MMSP providing the services.

5.2.2. One Account Per Customer: To ensure transparency, accountability, and prevent misuse, MMSPs must implement a One Account per Customer policy. Each customer shall be allowed to register and maintain only one active mobile money account with an MMSP, linked to their unique identification credentials. Exceptions, such as joint accounts or specific use cases, may be permitted subject to prior approval from RBV.

Accounts must have a provision for registering nominees/beneficiary(s).

5.3 Data Privacy and Security Measures

5.3.1. Data Collection and Consent: MMSPs must only collect the data necessary to provide services. Customer consent must be obtained before collecting, using, or sharing their data, and customers should be informed of how their data will be used and with who it may be shared with.

5.3.2. Data Encryption and Security Protocols: All customer data must be protected using industry-standard encryption methods, both in transit and at rest. MMSPs must regularly update their security measures to guard against emerging threats and data breaches.

5.3.3. Customer Access and Control over Data: Customers have the right to access and review their data held by MMSPs. They must also have the ability to request corrections or deletions of inaccurate information, as well as opt out of data-sharing for marketing purposes.

5.4 Customer Redress and Dispute Resolution Mechanisms

To ensure fairness and trust in mobile money services, MMSPs must establish effective mechanisms for resolving customer complaints and disputes.

5.4.1. Internal Dispute Resolution (IDR): MMSPs are required to maintain an accessible and efficient internal complaint-handling system. Customers must be able to lodge complaints via multiple channels, including in-person, through agents, online, or via mobile applications. All complaints must be acknowledged promptly by providing a service request number to the customer, and resolutions should be provided within a specified time frame.

MMSPs must adhere to the wider provisions of section 45 of NPSA for the settlement of disputes by arbitration.

5.4.2. Tracking and Reporting Complaints: MMSPs must keep detailed records of all customer complaints, including the nature of the complaint, actions taken, and outcomes. These records should be reported to RBV via the IRPS (Incident Report Payment System) and will be subject to review by the RBV to ensure compliance and assess the effectiveness of dispute resolution mechanisms.

5.4.3. Escalation to External Bodies: If a customer is dissatisfied with the outcome of the internal dispute resolution process, they should be given the option to escalate the complaint to RBV's customer complaint redressal desk. Customers will have the option to take legal recourse if they are still not satisfied with the resolution.

5.5 Transactions

Fraud prevention is a critical component of the customer protection framework. MMSPs must implement measures to safeguard customers from fraud and ensure their safety when using mobile money services.

5.5.1. Transaction Authentication and Multi-Factor Authentication (MFA): MMSPs must use strong customer authentication protocols, including PINs, passwords, and multi-factor authentication (MFA), to verify the identity of users and secure transactions. Customers should be regularly reminded not to share their credentials with others.

5.5.2. Transaction Verification: There must be a mechanism for the customer to verify the name and number of the funds' recipient for confirmation before a transaction is completed.

5.5.3. Transaction Receipts and History: The customer shall immediately receive written confirmation of the execution of a transaction, including the fee charged. The mobile money service provider shall provide in writing the balance remaining in the customer’s mobile wallet and a statement on previous transactions. This can be provided in the form of a physical receipt or digitally on the mobile application of the user using a smartphone.

5.5.4. Offline Transactions: No offline transactions, either initiated by the customer or through an agent, are allowed. All the Mobile Money transactions should happen in an online mode, with all the ledgers in the systems getting updated in real-time.

6. Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF)

Mobile Money Service Providers (MMSPs) are integral parts of Vanuatu’s financial system and, as such, must implement stringent AML/CTF measures. The Reserve Bank of Vanuatu (RBV) mandates compliance with the **AML/CTF Act** to prevent the use of mobile money services for illicit activities. This section outlines the required protocols to identify, monitor, and report suspicious activities while maintaining robust KYC and Customer Due Diligence (CDD) procedures.

6.1 Risk-Based Approach (RBA) to AML/CTF

A risk-based approach (RBA) is central to the AML/CTF compliance framework. MMSPs must assess the risks posed by different types of customers, transactions, and agents and apply appropriate preventive measures based on the level of risk.

6.1.1. Risk Assessment: MMSPs must conduct regular risk assessments to identify vulnerabilities within their operations, including geographic areas of service, transaction volumes, customer types, and agent networks. These assessments must evaluate potential risks related to money laundering, terrorism financing, and fraud.

6.1.2. Risk Classification: Customers, agents, and transactions must be classified into different risk categories (e.g., low, medium, high). Higher-risk profiles, such as politically exposed persons (PEPs) or customers from high-risk jurisdictions, must be subject to enhanced scrutiny and monitoring.

6.1.3. Proportional Controls: The controls applied must be proportional to the identified risks. For low-risk customers, simplified due diligence may be appropriate, while high-risk customers will require enhanced due diligence (EDD) and ongoing monitoring.

6.2 Know Your Customer (KYC) and Customer Due Diligence (CDD) Requirements

To comply with AML/CTF regulations, MMSPs are required to implement comprehensive KYC and CDD procedures. These procedures ensure that customers are properly identified and that their transactions are monitored for any signs of suspicious activity.

6.2.1. Customer Identification and Verification: MMSPs must collect key customer information during the onboarding process. This includes the customer's full name, date of birth, residential address, and identification document details (e.g., National ID, passport, VNPF ID, Birth certificate). The verification process should be based on reliable, independent sources, such as government-issued databases or identity verification services, as and when it is made available for KYC purposes by the RBV.

6.2.2. Simplified Due Diligence (SDD): For low-risk customers, such as those conducting small-value transactions or using basic mobile wallet services, simplified due diligence procedures may be applied. This allows for quicker onboarding while still meeting regulatory standards.

6.2.3. Enhanced Due Diligence (EDD): Higher-risk customers, such as PEPs, non-resident individuals, and customers with complex business structures, must undergo enhanced due diligence. This includes a more detailed review of the customer's background, the source of their funds, and closer monitoring of their transactions.

6.3 Transaction Monitoring and Reporting

Transaction monitoring is essential for detecting and reporting suspicious activity that could indicate money laundering, terrorism financing, or other financial crimes. MMSPs must have automated systems in place to track transactions in real time.

6.3.1. Automated Transaction Monitoring Systems: MMSPs must implement automated transaction monitoring systems capable of analysing transaction patterns in real-time. These systems should flag transactions that deviate from established norms, such as unusually large or frequent transfers, sudden spikes in activity, or any other value and velocity-based rules.

6.3.2. Suspicious Activity Report (SAR) and Suspicious Transaction Reporting (STR): If a suspicious transaction or pattern of transactions is identified, MMSPs must file a **SAR and STR**, respectively, with the Vanuatu Financial Intelligence Unit (VFIU). Reports must be submitted promptly and include all relevant information about the transaction, the customer, and the nature of the suspicious activity.

6.3.3. Threshold-Based Reporting: Certain transactions that exceed predefined thresholds, as defined by VFIU from time to time, regardless of whether they appear suspicious, must be reported to the VFIU. These thresholds are established by the VFIU and may vary based on the type of transaction, customer profile, or geographic area.

6.3.4. Record-Keeping Obligations: MMSPs are required to maintain detailed records of all transactions, customer profiles, and KYC documentation for a minimum period of 7 years. These records can be maintained in digital format and must be readily accessible for inspection by regulators and law enforcement agencies.

6.4 Cross-Border Transactions and Remittances

Cross-border transactions and international remittances are particularly vulnerable to money laundering and terrorism financing risks. The RBV requires MMSPs to implement enhanced controls for these types of transactions.

6.4.1. Enhanced Due Diligence for Cross-Border Transactions: MMSPs must apply enhanced due diligence to cross-border transactions, particularly those involving high-risk jurisdictions or unregulated entities.

6.4.2. Partnerships with Correspondent Banks: MMSPs offering cross-border services must ensure that they have robust AML/CTF arrangements with their correspondent banks. These arrangements should include clear information-sharing protocols, compliance checks, and regular audits to ensure that both parties are meeting their regulatory obligations.

6.4.3. International Funds Transfer Report (IFTR): Large cash transactions that exceed predefined thresholds must be reported to the VFIU as an **International Funds Transfer Report (IFTR).** The thresholds for such reports are set by the VFIU and are periodically reviewed to reflect the evolving risk landscape.

7. Technology and Infrastructure Considerations

Mobile Money Service Providers (MMSPs) rely heavily on technology and infrastructure to deliver secure, efficient, and scalable digital financial services. The Reserve Bank of Vanuatu (RBV) mandates the following requirements to ensure the integrity, security, and resilience of mobile money services.

7.1 Technology Standards and Compliance

To safeguard the stability and reliability of the mobile money ecosystem, MMSPs must adhere to established technology standards, ensuring that their platforms are secure, resilient, and compliant with regulatory requirements.

7.1.1. System Integrity and Reliability: MMSPs must ensure that their technology platforms are designed to provide consistent service with minimal disruptions. This includes maintaining high availability, system redundancy, and scalable infrastructure that can accommodate growing transaction volumes and new service offerings.

7.1.2. Compliance with International and Local Standards: MMSPs are required to comply with local regulatory standards and relevant international standards, including those set by the International Organization for Standardization (ISO) for information security and data management (e.g., ISO/IEC 27001). Compliance with these standards ensures that mobile money platforms meet global best practices for security, performance, and risk management.

7.1.3. Regular System Updates and Maintenance: To keep systems secure and operationally effective, MMSPs must regularly update their software and hardware infrastructure. Security patches and updates should be promptly applied to mitigate emerging threats and vulnerabilities. MMSP shall maintain a log of system updates and patches that can be provided to RBV upon request.

7.2 Cybersecurity and Data Protection

The security of customer data and the protection of mobile money platforms from cyber threats are of paramount importance. MMSPs must implement comprehensive cybersecurity measures to protect their systems and customers from data breaches, fraud, and other malicious activities.

7.2.1. Risk-Based Cybersecurity Framework: MMSPs must adopt a risk-based approach to cybersecurity, which includes identifying potential threats, assessing vulnerabilities, and implementing protective measures. A cybersecurity framework should be regularly reviewed and updated to address new and evolving risks.

7.2.2. Data Encryption: All customer data, including personal information, transaction records, and financial details, must be encrypted both in transit and at rest. Strong encryption protocols, such as AES-256, should be used to ensure the confidentiality and integrity of customer information.

7.2.3. Access Control and Authentication: MMSPs must implement multi-factor authentication (MFA) for both internal users (e.g., staff) and customers to prevent unauthorized access to mobile money accounts. The system should block the user after 3 unsuccessful attempts to log in to the system in real time. The role-based access controls should be enforced to limit access to sensitive data and systems based on user responsibilities.

7.2.4. Incident Response and Recovery Plans: MMSPs must develop and implement robust incident response plans to quickly detect, respond to, and mitigate cybersecurity incidents. This includes protocols for isolating affected systems, notifying the RBV and relevant authorities, and restoring services. Regular cybersecurity drills should be conducted to test the effectiveness of these plans.

7.3 Interoperability and System Integration

Interoperability is key to creating a seamless and inclusive mobile money ecosystem, enabling customers to transact across different platforms and networks. MMSPs must prioritize system integration and interoperability to support the growth of the digital financial services sector.

7.3.1. Interoperability Standards: MMSPs must ensure their systems are designed to support interoperability with other mobile money platforms, financial institutions, and payment systems. Adopting industry-standard messaging formats such as ISO 20022 for payment processing can facilitate seamless integration across different providers.

7.3.2. Cross-Platform Transactions: MMSPs are encouraged to enable cross-platform mobile money transactions, allowing customers from different mobile networks or service providers to transact with each other. This fosters competition, improves service availability, and expands customer choice.

7.3.3. Collaboration with Financial Institutions: MMSPs should collaborate with banks and other financial institutions to integrate mobile wallets with traditional banking services, enabling seamless transfers between mobile money accounts and bank accounts. This enhances financial inclusion by providing customers with more options for managing their funds.

7.4 Business Continuity and Disaster Recovery

To ensure the uninterrupted provision of mobile money services, MMSPs must establish comprehensive business continuity and disaster recovery plans. These plans are essential for maintaining service availability in the face of natural disasters, cyberattacks, or other operational disruptions, particularly given Vanuatu's geographical vulnerability to natural events.

7.4.1. Business Continuity Planning (BCP): MMSPs must develop and maintain a business continuity plan that outlines how critical services will continue in the event of a disruption. The plan should include procedures for maintaining essential operations, ensuring communication with customers, and managing service outages.

7.4.2. Disaster Recovery Plans (DRP): MMSPs must implement disaster recovery plans that detail the steps to restore critical systems and services after a disruption. This includes backup and recovery processes for data, alternative infrastructure arrangements, and coordination with key service providers (e.g., Mobile Network Operator -telecommunications operators).

7.4.3. Testing and Simulation: Business continuity and disaster recovery plans must be regularly tested through simulations and drills to ensure readiness. These exercises should be reviewed and updated as needed to address any identified weaknesses or gaps. MMSPs need to keep RBV informed on these testing and simulation exercises.

7.4.4. Crisis Management and Communication: In the event of a disruption, MMSPs must have protocols in place for communicating with customers, agents, and stakeholders. Customers must be informed of any service outages or interruptions, along with guidance on alternative service options or timelines for restoration.

8. Financial Literacy and Education Initiatives

MMSPs are required to implement financial literacy and education initiatives to raise awareness and build customer confidence in their mobile money and overall digital financial services. To spread financial education effectively, MMSP can use digital platforms, agent networks and community influencer. The MMSPs should also train agent and local merchants as financial literacy promoters.

MMSPs must develop and deliver targeted education programs to inform customers about the features, benefits, and safe use of mobile money services. These programs should cover, but not be limited to, topics such as:

- How to register for mobile money services and open a mobile wallet.
- How to perform transactions, including transfers, bill payments, and cash-ins/cash-outs.
- Understanding transaction fees, limits, and service terms.
- Protecting personal information, PINs, and passwords.
- Identifying and avoiding common fraud schemes, such as phishing and SIM swaps.
- Complaint registration, escalation, and follow-up