Southern African Development Community

SADC Mobile Money Guidelines

January 2024

Version 1.2

1. Introduction:

The Protocol on Finance and Investment (FIP) in the Southern African Development Community (SADC) region remains the key to facilitating regional financial integration. It aims to make the SADC region an attractive destination for foreign direct and regional investments. A review was commissioned by the legal and payments sub-committees of the Committee of Central Bank Governors in SADC (CCBG) in 2013/14 to assess the laws, regulations, directives, circulars, guidelines and guidance notes directly applicable to the National Payment System in each of the 16 SADC countries. Since then, the 2016 and 2019 SADC Mobile Money Guidelines for the SADC CCBG have been approved. This reviewed version for 2023 aims to provide the SADC Member States with a systemic approach to putting a solid framework around the mobile money ecosystem under the National Payments System (NPS). This review further considers the impact of the most recent technological developments to harmonise the Member States' legal and regulatory frameworks, considering financial inclusion, innovation and FinTech development in the SADC region.

The Mobile Money Guidelines seek to provide:

1. These principles would be a baseline to be considered by the respective stakeholders, particularly Central Banks, in formulating or amending their country-specific Mobile Money guidelines.
2. Clarity on the Mobile Money ecosystem and components within the ecosystem that need to be addressed have been the subject of debate with different outcomes in multiple domestic jurisdictions.
3. Guidance on risk-based and rules-based approaches and monitoring frameworks to support innovation for new products in the mobile money ecosystem.

2. Objectives and Guiding Principles:

Mobile Money has evolved as a utility to provide financial services mainly to the unbanked and underserved population. Its success in specific emerging markets and countries with unsophisticated banking infrastructure has been unprecedented. The project aims to develop Mobile Money guidelines to assist SADC Member States with principles to facilitate the harmonisation of their legal and regulatory frameworks for Mobile Money in support of greater financial inclusion and market development in the SADC region.

In considering the adoption and implementation of these SADC Mobile Money Guidelines, the following principles must be considered:

2.1. The Central Bank is the regulatory authority empowered to regulate the provision of Mobile Money in its jurisdiction.

2.2. The telecommunications regulator is a critical and essential stakeholder in providing Mobile Money Services. The telecommunications regulator should be consulted while formulating the Mobile Money regulatory framework.

2.3. The E-Money Issuer is the entity the Central Bank licenses to provide Mobile Money Services.

2.4. The financial integrity regulator must be consulted about AML or CTF and applicable provisions for Mobile money-specific transactions; the E-Money Issuer must comply with AML/CFT regulations as directed by the financial intelligence / financial integrity regulator.

2.5. Mobile Money standards must suit domestic market conditions whilst considering SADC regional harmonisation objectives and imperatives. The SADC regionalisation objective and imperatives are, amongst others:

2.5.1. The implementation of a SADC regional clearing and settlement payment system;

2.5.2. The possibility of a SADC Central Bank with a single SADC currency;

2.5.3. The Remittance project continues to work with the regulators, money transfer operators, commercial banks, and national authorities in the SADC region to ensure transparency and reduce fees for cross-border remittances. In this process, regulators must establish the proportionate regulations that may be implemented without introducing unnecessary risk when implementing such relaxations.

2.5.4. Implementing a SADC FinTech Regulatory Framework for adoption by Member States;

2.5.5. Broader requirements are required for regional integrations discussed in the various CCBG subgroups addressing different areas of their CCBG responsibility, for example, Legal, Financial Markets, Supervision and Technology Infrastructure.

2.5.5.1. To enhance regional interoperability in the states, consider the recent technological developments in the mobile money industry.

3. Abbreviations and Glossary:

The following terms and acronyms shall have the meanings assigned to them below:

Term	Definition
Agents	Any third party acting on behalf of a bank, a financial institution or a non-bank institution (including an E-Money issuer or other payment services provider) to deal directly with customers under a contractual agreement. The term “agent” is commonly used even if a principal-agent relationship does not exist under the regulatory framework.
B2B	**Business-to-business** payments usually include those between two companies engaged in commercial activities.
B2G	**Business-to-government** payments such as paying taxes and fees and other government payments from commercial entities.
B2P	**Business-to-person** payments are usually from business to individuals, such as salary payments.
Central Bank	is the primary financial institution within a country or a group of countries that is responsible for managing the nation's money supply, implementing monetary policy, and overseeing the overall stability of the financial system
CICO	**Cash-In-Cash Out** is the exchange of cash for electronic value (e-money) and the exchange of electronic value (e-money) to cash via agent networks to subscribed users.
CDD	**Customer Due Diligence** is often used synonymously with Know Your Customer (KYC) measures. Generally, it refers more broadly to a financial institution’s policies and procedures for obtaining customer information and assessing the value of the information for detecting, monitoring, and reporting suspicious activities.
DDA	**Demand Deposit Account:** These are deposit accounts for bank consumers. Similarly, for e-money issuers, this would be wallet systems.
DFS	**Digital Financial Services:** The broad range of financial services accessed and delivered through digital channels, including payments, credit, savings, remittances and insurance. The digital financial services (DFS) concept includes mobile financial services (MFS). Mobile financial services (MFS) are a subset of DFS.
DFS Cashpoints	All locations where users can perform cash-in and cash-out transactions. Cash points may include active cash outlets, such as bank agents, ATMs, MNO agents, and cash agents offering DFS services.

DFSPs,	**Digital Financial Service Providers,** are e-money issuers and banks
EFT	**Electronic Funds Transfer)** - Any funds transfer initiated through an electronic terminal, telephone, computer, or magnetic tape to order, instruct, or authorise a financial institution to debit or credit a consumer's bank or e-money account.
E-Money	A type of monetary value electronically stored and generally understood to have the following attributes: (i) issued upon receipt of funds in an amount no lesser in value than the value of the E-Money issued and in the same currency, (ii) stored on an electronic device, whether or not it is SIM enabled (e.g. a chip, pre-paid card, mobile phone, tablet, phablet or any other computer system), (iii) accepted as a means of payment by parties other than the issuer and (iv) convertible into cash.
E-Money Issuer	is the entity that initially issues E-Money against receipt of funds. Some countries only permit banks to issue E-Money, while others permit non-banks. For these guidelines, E-Money issuers are nonbank DFSPs.
E-Float	is the total outstanding amount of e-money issued by an e-money issuer. Customer funds backing a float should be subject to fund safeguarding and isolation measures.
FATF	Financial Action Task Force
G2B	**Government-to-business** payments are made from government to commercial entities, which may include tax refunds, goods and services purchases and payments, and subsidies.
G2P	**Government-to-person** payments are made from government to individuals, which may include the disbursement of government benefits and salary payments.
ICT	Information and Communication Technology
ID	Identification
IMT	International Money Transfer
Interoperability	Enabling payment instruments for a particular scheme or business model to be used or interoperated between other schemes or business models. Interoperability requires technical compatibility between systems and can only take effect once commercial interconnectivity agreements have been concluded.
KYC	**Know-Your-Customer** is a set of due diligence measures undertaken by a financial institution, including policies and procedures, to identify a customer and the motivations behind their financial activities.

MFS	**Mobile Financial Services** Uses a mobile phone to access financial services and execute financial transactions. This includes transactional services, such as transferring funds to make a mobile payment, and non-transactional services, such as viewing financial information.
MNO	**Mobile Network Operator** a mobile network operator licensed by the respective SADC Member State telecommunications regulator to provide wireless voice and data communication for its subscribed users.
Mobile Money	is a type of electronic money (e-money) transferred electronically using mobile networks and SIM-enabled devices, primarily mobile phones. Depending on local law and the business model, the issuer of mobile money may be an MNO, a financial institution or another licensed third-party provider.
Mobile Money Service Provider	**E-Money Issuer,** licensed by the respective Central Bank to issue Mobile Money and provide Mobile Money Services.
Mobile Money Services	Services are provided by the E-Money Issuer to support the utility of Mobile Money for the consumer. These include but are not limited to cash-in, cash redemption at various channels and mobile payment services such as person-to-person, business-to-person and government-to-person.
NPS	**National Payments System:** The complete range of institutional and infrastructure arrangements and processes in a country for retail payments. This includes payment instruments, participating institutions, payment infrastructure, market arrangements and the regulatory framework.
PSP	**Payment Service Provider:** An entity providing services that enable funds to be deposited into an account and withdrawn from an account; payment transactions (transfer of funds between, into, or from accounts); issuance and acquisition of payment instruments that enable the user to transfer funds (e.g. checks, e-money, credit cards, and debit cards); and money remittances and other services central to the transfer of money.
P2B	**Person-to-Business** payments are made from individuals to commercial entities, merchants, SMEs, etc, and may include payments for purchasing goods and services.
P2G	**Person-to-Government** payments from individuals to government-related activities may include paying taxes and other fees.
PII	Personal Identifiable Information
Regtech	Refers to the use of technology, particularly information technology, to help companies and financial institutions comply with regulations efficiently and at a lower cost

Risk-based approach	A method for complying with AML/CFT standards outlined in FATF Recommendation 1. The risk-based approach is based on the general principle that where there are higher risks, countries should require financial services providers to take enhanced measures to manage and mitigate those risks. Where risks are lower (i.e. no suspicion of money laundering or terrorist financing), simplified measures may be allowed.
RTGS	Real-time Gross Settlement.
RTPS	Real-time Payment System.
SADC Mobile Money Guidelines	The SADC Mobile Money guidelines are set out in this document and adopted by the Committee of Central Bank Governors in SADC (CCBG).
Switch	is a payment ecosystem platform that enables payment transactions to be routed from one payment system participant to another, whether within the same network or between different networks or schemes.
Trust Account	is a bank account which holds funds received from Mobile Money customers, which account is held in trust or a fiduciary capacity on behalf of the Mobile Money customers (may also be referred to as an Escrow Account or a Custodial Account).

4. Authorisation: Regulatory Framework and Role of Stakeholders

4.1. Governing Standards

4.1.1. Only Non-Bank Entities that intend to offer Mobile Money Services must apply to the Central Bank for E-Money Issuer licensing. Banks and other financial institutions should be exempted.

4.1.2. Banks and other licensed Financial service providers are exempted from applying for the e-money issuer licensing.

4.1.3. The Central Bank shall draft the required application form for the licensing.

4.1.4. The E-Money Issuer may be required to apply for renewal of the E-Money Issuer license every five years.

4.1.5. The E-Money Issuer shall be required to implement processes, procedures and documents supporting the Mobile Money offering. These documents will be available for inspection by the Central Bank. They shall submit their application to the Central Bank with the following documents (amongst other documents specified by the Central Bank):

- 4.1.5.1. Company registration documents;
- 4.1.5.2. Human Resources structures and including competencies of the potential company's executive directors;
- 4.1.5.3. Detailed product and business plans;
- 4.1.5.4. Risk Management Framework;
- 4.1.5.5. Information and Communications Technology capabilities;
- 4.1.5.6. Operational capabilities;
- 4.1.5.7. MNO's network capability and availability;
- 4.1.5.8. Agent distribution network (if applicable);
- 4.1.5.9. Ability to comply with minimum and ongoing capital requirements;
- 4.1.5.10. Service level agreements, including envisaged draft agreements with agents;
- 4.1.5.11. Ability to have internal audit capability and external auditors;

4.1.6. The trust deed will contain the names and contact details of the nominated trustees with required supporting information and the operational mandate concerning trust account transactions and

4.1.7. Once the bank and financial services regulator approves the application for an E-Money Issuer license, it shall issue an E-Money Issuer license to the applicant. The bank and financial services regulator may include suitable conditions for granting the E-Money Issuer license.

4.1.8. The E-Money Issuer may be required to submit monthly reports to the Central Bank; the contemplated reports may include customers onboarded with KYC information, agents onboarded with KYC information, businesses onboarded with KYC information, transactions processed information for a specified period, active versus inactive Mobile Money accounts, unclaimed funds, any data and security breaches and any other related information. Depending on the market conditions, the regulator may request real-time reporting from the e-money issuers for regtech and data analysis.

4.1.9. The Central Bank may use these reports for review when renewing an E-Money Issuer's license.

4.1.10. The Central Bank may, if it so wishes, conduct site visits at the E-Money Issuer's address to verify the provided information.

4.1.11. For declined applications, the Central Bank must set out the appeals procedures available for the applicant to follow to appeal the decision of the Central Bank. Regarding licensing, the Central Bank may also include provisions relating to.

4.1.11.1. The display of the E-Money Issuer license;

4.1.11.2. The E-Money Issuer license should not be transferable;

4.1.11.3. Terms relating to the cancellation of the E-Money Issuer License;

4.1.11.4. In the event of a cancelled E-Money Issuer License, conditions upon which an E-Money Issuer License may be reinstated and

4.1.11.5. Publicly display licensed E-Money Issuers.

4.2. Governing Operational Requirements

4.2.1. An E-Money Issuer must notify the Central Bank of any significant proposed changes to the nature and scope of its services at least 30 days before the implementation date.

4.2.2. The E-Money Issuer shall put measures in place to restrict the processing of Mobile Money transactions that are above the stipulated limits or that exceed the set account balances. The regulator will monitor this.

4.2.3. The E-Money Issuer shall ensure that its operational procedures and processes are by domestic provisions relating to AML and CTF.

4.2.4. The bank and financial services regulator may establish processes, procedures and systems to ensure the clearing and settlement of transactions. Such measures should address some of the following provisions:

4.2.4.1. Open and interoperable;

4.2.4.2. Push credit transfers;

4.2.4.3. Guaranteed same-day settlement;

4.2.4.4. Irrevocability of transactions;

4.2.4.5. Price transparency;

4.2.4.6. Payment addressing;

4.2.4.7. Inclusive governance;

4.2.4.8. Accessible to a broad range of users, including all use cases;

4.2.4.9. Standardised user experience;

4.2.4.10. Fraud Utility;

4.2.4.11. Interoperability and connection to other schemes;

4.2.4.12. Dispute resolution mechanism and regulatory oversight;

4.2.4.13. Sufficient backup mechanisms to de-risk technical failures;

4.3. Stakeholders Roles and Responsibilities

The Payments Ecosystem comprises various stakeholders, including Mobile Money customers, service providers, and multiple regulators. When we refer to the ecosystem or stakeholders, we refer to the parties set out below:

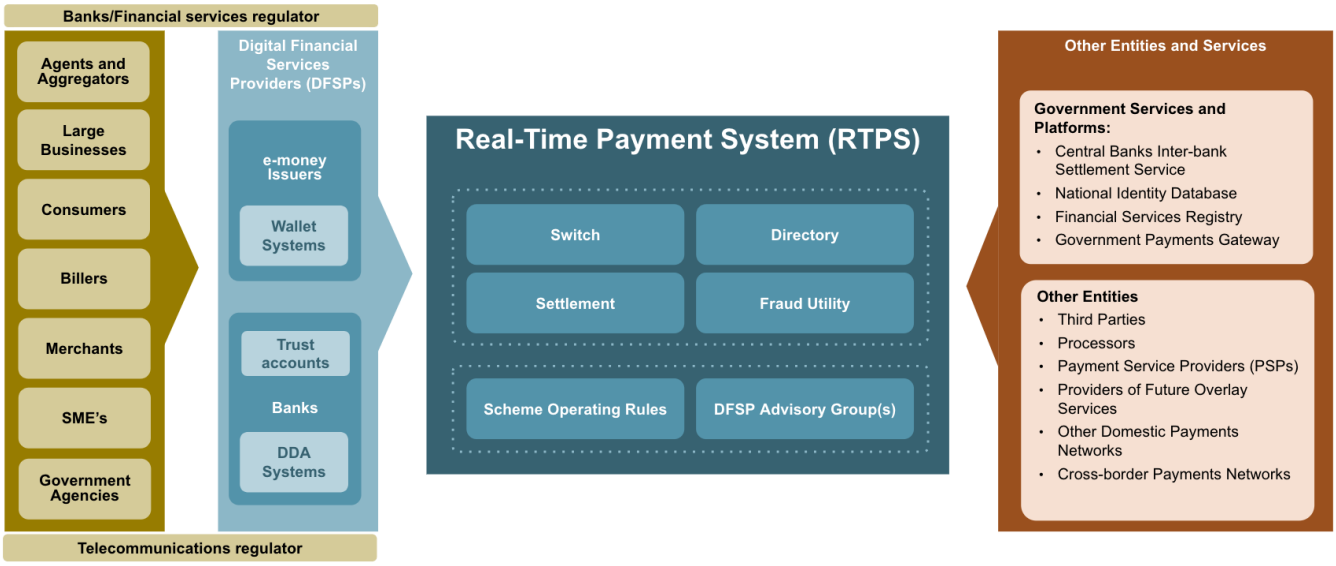

Figure 1: National Payment Ecosystem

4.3.1. Bank and Financial Services Regulators

The Central Bank regulates financial activities and is responsible for the countries' financial stability within its jurisdiction and oversight of payment and settlement systems. Accordingly, a Central Bank may:

4.3.1.1. Issue a letter of no objection;

4.3.1.2. Issue an E-Money Issuer license;

4.3.1.3. Decline to issue an E-Money Issuer license;

4.3.1.4. Amend or, vary or reinstate an existing E-Money Issuer license; or

4.3.1.5. If good cause is not shown, terminate an E-Money Issuer license;

4.3.1.6. Issue, amend/vary, renew, reinstate and terminate an E-Money Issuer License;

4.3.1.7. Set the operational standards and rules for participation by an E-Money Issuer;

4.3.1.8. Set out capital and ongoing capital limits;

4.3.1.9. Ensure that customer funds are protected against any insolvency actions;

4.3.1.10. Set out strict regulations and measures for monitoring of Trust Accounts;

4.3.1.11. Endeavour creating systems allowing the Central Bank to monitor transactions in the Trust Account as necessary;

4.3.1.12. Set out balance and transactions limits;

4.3.1.13. Take into consideration SADC regional imperatives.

4.3.2. Telecommunications Regulators

The Telecommunications Regulator regulates and issues domestic telecommunications licenses to Mobile Network Operators (MNOs). Accordingly, a telecommunications regulator may:

4.3.2.1. Issue the primary licence and ensure compliance with the Telecommunications laws and regulations

4.3.2.2. Advise the Central Bank of any material breaches by the MNO (an E-Money Issuer or supports an E-Money Issuer) of its license provisions;

4.3.2.3. Support the Central Bank on telecommunications issues such as network availability and capacity;

4.3.3. Digital Financial Services Providers

These entities include banks and non-banks. The responsibilities are as follows:

4.3.3.1. **E-Money Issuers**

These entities, also known as mobile network operators (MNOs), issue e-money against the receipt of funds. This entity is typically differentiated as a specialised licensed entity to differentiate from other financial services providers. Typically, an e-money issuer will be responsible for:

4.3.3.1.1. Conduct its Mobile Money business in compliance with the Central Bank regulatory provisions and its E-Money Issuer license conditions.

4.3.3.1.2. Ensure that the trustees of the Trust Account manage the Trust Account in a manner consistent with the protection of customer funds.

4.3.3.1.3. Ensure that its agreements with Agents are by regulatory provisions.

4.3.3.1.4. Endeavour to provide Mobile Money customers with ongoing, uninterrupted service.

4.3.3.1.5. Provide adequate notice to the Central Bank of any anticipated business model(s) changes.

4.3.3.1.6. Obtain written approval from the Central Bank concerning the usage/distribution of commercially negotiated interest arising from the Trust Account.

4.3.3.1.7. Timeously submit required reports and information to the Central Bank.

4.3.3.1.8. Acceptance of customer funds and funds held by the E-Money Issuer by Mobile Money Services shall not constitute deposit taking or be regarded to fall within the definition of activities associated with a bank's business.

4.3.3.1.9. E-money issuers may not engage in activities other than issuing Mobile Money and providing services related to Mobile Money, except for entities licensed for different activities by the respective Central Bank.

4.3.3.2. **Banks**

These entities provide regulated banking facilities where the money collected by the E-Money Issuer is deposited on behalf of the customers. Aside from providing traditional banking services, the bank in this ecosystem partners closely with the E-Money Issuer due to a direct connection via the “Trust Account”, where the consumers' funds sit. Typically, a bank is a sponsor in this case and does not own or have a direct contractual relationship with the MNO’s customer. Therefore, the bank's role is:

4.3.3.2.1. Direct participant in clearing and settlement, it clears and settles the payment obligations of the E-Money Issuer;

4.3.3.2.2. Holds and maintains the trust account and accordingly monitors and reports it.

4.3.3.3. **DFSP Advisory Group**

This organisation serves as a space for participants in the National Payment System (NPS) to converse about payment schemes for digital financial services. It serves as a vital forum where stakeholders, including regulators and providers of digital finance services, can work together to tackle and improve various facets of E-Money and digital payment solutions. To guarantee the advisory group's efficiency, it must embrace inclusivity and transparency and be guided by clear rules and protocols. Additionally, the group should promote consistent meetings, exchange information, and formulate practical plans to resolve identified issues. Therefore, the role of the group is to

4.3.3.3.1. Facilitate open and constructive dialogue among NPS participants. It allows them to effectively discuss and resolve payment scheme issues, fostering collaboration in the digital financial services ecosystem;

4.3.3.3.2. Address a wide range of issues, including pricing structures, participation rules, penalties for non-compliance, fraud prevention and mitigation, and the utility of payment schemes;

4.3.3.3.3. Provide an opportunity for stakeholders to ensure alignment with regulatory requirements and standards. This is especially important in electronic money, where adherence to regulations is critical;

4.3.3.3.4. Share best practices, insights, and experiences related to digital payment solutions;

4.3.3.3.5. Discuss promoting innovation in digital financial services, necessary policy changes for innovative digital payment schemes, monitoring data sharing and reporting requirements, and developing stakeholder skills and knowledge.

4.3.3.4. **Fraud Utility/AML/CFT Regulator**

The domestic working group or team is empowered to adopt and implement regulations relating to Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) provisions, which relate to customer due diligence requirements as a function of both regulators' requirements for the DFS ecosystem. In some Member states, this would already exist as FIUs.

4.3.3.4.1. Be responsible for adopting and implementing regulations relating to AML and CTF provisions related to customer due diligence requirements.

4.3.3.4.2. Provide the regulators with the support required to determine tiered Mobile Money account balances and transactional limits.

4.3.3.4.3. Guide the information required in the reports submitted by the DFSPs to the Central Banks to monitor transactions.

4.4. Governing Supervision Approaches

4.4.1. The regulators, especially under the DFSP Advisory Group, will need to align the suggested monitoring approaches of risk-based supervision to the mobile money ecosystem. The regulator must identify all products by assessing the risk profile using six types of risks:

4.4.1.1. Systemic Risk: A risk capable of causing a collapse or significant damage to the financial system.

4.4.1.2. Operational Risk: A risk that impairs the ability of stakeholders to operate their business effectively, for example, failed internal processes, people, systems, or external events.

4.4.1.3. Reputation Risk: A risk that tarnishes the image of stakeholders, the mobile system, the financial system, or a specific product.

4.4.1.4. Legal Risk: This could lead to unforeseeable lawsuits, judgments, or contracts disrupting or affecting Mobile Money Services' business practices.

4.4.1.5. Liquidity Risk: A risk diminishing the ability of a financial institution to meet cash obligations.

4.4.1.6. International Risk: A systemic risk with the potential for cross-border risks that extend beyond national borders, affecting multiple jurisdictions in the SADC region.

4.4.2. The regulator must account for ongoing on-site and off-site surveillance. Suggested approaches with FIUs must incorporate the following;

4.4.2.1. On-Site Surveillance: Comprehensive on-site examinations should focus on a targeted assessment of individual institutions and explicitly address the risk profiles.

4.4.2.2. Off-Site Surveillance: Financial soundness assessment involves analysing statistical and electronic returns submitted periodically by entities to the regulators and any subsequent early warning reports needed.

4.4.2.3. Other Supervisory Tools: Planned and ad hoc meetings with the management of entities with all stakeholders as part of the DFSP Advisory groups for discussions on financial performance, risk profile, strategies, and other supervisory issues. It is also advised that engagements with external auditors are also considered, especially if no in-house expertise is available.

5. Capital and Ongoing Capital Requirements

5.1. The Central Bank may set out the minimum capital amount to be paid and maintained by an E-Money Issuer. The respective Central Bank will determine the minimum capital amount. The Central Bank may decide its ratios to be similar to those of existing financial institutions.

5.1.1. Acceptable costs to set barriers to market entry for new institutions that want to pursue the business initiative.

5.2. The Central Bank must implement mechanisms enabling the Central Bank and E-Money Issuer to monitor and calculate the required ongoing capital amount regularly.

5.2.1. They are typically calculated as a percentage of outstanding mobile money liabilities intended to ensure that the E-Money issuer's capital continues to grow along with their obligations.

5.2.2. However, exceedingly high minimum capital requirements may increase compliance costs, making the business case difficult to justify for new entrants. This needs to be considered because if excessive capital is immobilised, this can increase business costs, stifle innovation and reduce competition.

5.2.3. Consider that E-Money issuers are subject to additional requirements that safeguard customer funds and lower the risk profile of mobile money.

6. Interest-Bearing Mobile Money Trust Accounts

6.1. The distribution of interest to mobile money account holders is still under debate in a number of countries as the account isn't considered deposit-taking and cannot accrue interest like bank savings accounts. The discussion stands because it may be considered an activity only for an entity with a banking license. Some jurisdictions restrict interest payments on Mobile Money to delineate between banking activity and Mobile Money.

6.1.1. The "Trust Account", an escrow account, is officially held at a commercial bank.

6.1.2. Some regulators have cited concerns that paying interest on mobile money or other e-money accounts may lead e-money deposit holders to believe that mobile money accounts are like savings accounts.

6.1.3. The emerging trend in SADC has been that Trust Accounts do earn interest, and the distribution of the interest earned is negotiated and approved by the e-money issuer and financial services regulator:

6.1.3.1. The distribution method and usage of the interest are typically determined by e-money issuers, regulators and advisory groups. Potential models should be considered to change mobile money's adoption or usage rate;

6.1.3.1.1. Distribute to deposit holders as it legally belongs to e-money deposit holders rather than e-money issuers

6.1.3.1.2. It can be used to subsidise transaction costs to e-money issuers

6.1.3.1.3. Investment of interest income in the mobile money business or with the government as CSR

6.1.3.1.4. To defray customer transaction costs.

6.1.3.2. The E-Money issuer may negotiate the interest rate or other related commercial arrangements with the bank.

6.1.3.3. The E-money issuers shall keep the interest earned in the Trust Account in a separate bank account (this includes interest earned on interest) with a separate record of the interest earned.

6.1.3.4. Any use of frivolous fees or the invention of a new account type to hold e-money to limit interest shall be regarded as an attempt to defraud the e-money holders and grounds for severe sanction of the bank and any colluding partner.

6.1.3.5. The interest record earned in the Trust Account shall be submitted to the Central Bank as part of the E-Money Issuer's monthly reporting.

6.1.3.6. The aggregate amount held in the Trust Account should always equal the total Mobile Money liabilities.

6.1.3.7. The Trust Account shall be managed to demonstrate that the account is held in trust for the e-money deposit holders to safeguard the funds and shall be separated from the e-money issuer's operational funds.

6.1.3.8. In the event of insolvency or liquidation of the E-Money Issuer, the Trust Account (in which the customer funds are held) and the capital amount shall not be the subject of and be part of the assets available for distribution by the liquidator.

6.1.3.9. E-money issuers could partner with a licensed financial institution to offer savings and credit products, allowing account holders to earn interest and borrow from the scheme. This can be considered to incentivise savings behaviour.

6.2. Issuance of mobile money as a form of E-Money

6.2.1. E-Money funds shall be redeemable at par value to the SADC Member States currency in the country of issue.

6.2.2. The creation of E-money only happens when an Agent of a DFSP or Aggregator deposits money into a trust account,

6.2.3. Digital Finance products should be configured to make transactions acceptable to the issuer while enabling general domestic acceptance and possible future acceptance in the SADC Region.

6.2.4. Regulators will allow the market to determine and report fees transparently and keep oversight and reviews with the e-money issuers.

6.2.5. E-money issuers must comply and ensure the customer is fully aware of fees and any changes after that.

7. Financial Integrity - AML/CFT

Appropriate AML and CTF provisions, which relate to the financial integrity of the transactions, are essential for the success of mobile money services. The majority of SADC countries have tiered AML provisions. These have proven to allow for ease of opening Mobile Money whilst mitigating potential money laundering risks. A uniform approach is required when dealing with e-money issuers.

7.1. E-money issuers shall be accountable institutions by the SADC Member States' domestic AML and CTF legislation as Fraud Utility.

7.2. The E-Money issuer shall ensure that its Mobile Money accounts are not misused for money laundering, terrorist financing, or any other unlawful activity as regulated by the SADC Member States' AML and CTF legislation.

7.2.1. E-money issuers should provide staff training, agents and aggregators to ensure they are prepared to carry out their AML/CFT obligations.

7.3. The Central Bank will stipulate tiered Mobile Money account balance and transactional limits with the appropriate customer due diligence. These limits will take cognisance of the domestic market economic conditions whilst mitigating the risks associated with money laundering and terrorist financing.

7.3.1. Transaction limits may be progressively reviewed.

7.3.2. The E-money issuers should not breach transaction limits.

7.3.3. A tiered approach to KYC allows the regulator to distinguish between low and high-risk scenarios.

7.4. The E-Money Issuer shall demonstrate to the Central Bank its capacity to monitor transactions and report if there are transactions that exceed the stipulated limits. The E-Money Issuer shall report all transactions that exceed the AML limits to the Central Bank as part of its monthly reporting.

7.4.1. Appropriate individual and daily transaction value limits need to be placed.

7.4.2. Appropriate maximum account balance limits for funds must be in place

7.4.3. E-Money Issuer should have an adequately funded and resourced AML/CFT unit commensurate with the risks.

8. KYC and Centralised Registries

8.1. To open wallets, e-money deposit holders must provide proof of identity as all digital financial service providers, comply with KYC requirements, and follow best practices. To sign up for a mobile money account, a consumer typically visits a mobile money agent and provides proof of identity.

8.1.1. This is important to ensure the financial services' commercial reliability and compliance with regulators' rules on KYC, mainly anti-money laundering (AML) and countering the financing of terrorism (CFT) policy requirements.

8.1.2. These have to be in addition to the requirements for mandatory SIM registration imposed by telecommunications regulators.

8.1.3. Both regulators need to determine an acceptable form of ID as the minimum KYC so they do not inadvertently isolate segments of the population from essential mobile money services.

8.1.3.1. Basic Tier: This level is often associated with minimal KYC requirements, making it accessible to individuals with limited identification documents. In this layer, the regulator can harmonise identity-related SIM registration requirements as the lowest tier of KYC requirements to enable instant SIM registration and low KYC enablement.

8.1.3.2. Intermediate Tier: This level might require more extensive KYC information. Users in this tier may also have higher transaction and balance limits.

8.1.3.3. Advanced Tier: The advanced tier requires comprehensive KYC verification and is typically associated with more sophisticated services, such as savings and credit products.

8.1.4. Member states must ensure a data privacy or protection framework.

8.1.5. Comprehensive frameworks may need greater transparency in using personal data primarily for personally identifiable information.

8.1.6. Mobile and digital technology must be positioned to enable secure and inclusive digital identity, and regulators must mandate developing ID-linked services.

8.1.6.1. Alternative forms of ID are often only accepted for certain types of transactions and have specified thresholds and limits.

8.1.7. Regulators should allow the use of an agent network for (1) customer registration, (2) identity verification, and (3) cash-in and cash-out services.

8.1.8. Financial regulators should ensure that CDD requirements for low-value accounts are simple enough for agents' duties.

8.1.9. The relevant regulatory authorities should consider a progressively tiered, risk-based approach to account opening without a digitised national ID system. Regulators should use the referred approaches to manage transaction limits, guided by

8.1.9.1. Limits on individual transactions and several transactions in a specific period (e.g. per day),

8.1.9.2. Limits on the total transaction value over a given period (usually per month, but in some instances per day or year),

8.1.9.3. Limits on mobile money balances based on KYC.

8.1.9.4. By providing a “test and learn” environment, regulators may support KYC innovations, such as solutions that allow remote onboarding of customers, especially to create an e-KYC structure for further automated verification.

9. Consumer Protection and Education:

9.1. Customer protection measures entail safeguarding the customer's funds. In most instances, customer funds are protected by imposing restrictions on the use of customer funds by the E-Money Issuer and isolating funds from institutional risks. In addition, the customer must be protected against insolvency by the E-Money Issuers. The risk of Mobile Money customers losing their money is generally mitigated if:

9.1.1. A requirement on the E-Money Issuer for initial capital combined with ongoing capital to ensure an appropriate level of consumer protection and sound and prudent operation of an E-Money Issuer. Maintaining minimum capital is essential to protect against credit risk and associated insolvency.

9.1.2. 100% of the cash backing Mobile Money is held in a fully prudentially regulated institution, such as a bank; most Central banks require that the cash be held in a registered bank in a "Trust Account".

9.1.3. Customer funds are isolated from the issuer's funds (via the TrustAccount) and claims by the issuer's creditors, protection against insolvency. The isolation of funds also protects against credit risk and insolvency.

9.1.4. The initial and continuing capital requirement is supplemented by the ring-fencing of the funds in addressing customer protection; accordingly, Central Banks must be cognisant to avoid setting out stringent capital requirements that may restrict participation by prospective E-Money issuers.

9.2. Most countries have developed and implemented consumer protection frameworks to minimise these risks, protect consumers, and ensure that E-Money Issuers act appropriately towards their customers. These frameworks typically include a mix of

9.2.1. Stand-alone consumer protection legislation, which applies to all transactions, irrespective of the sector, product, provider or user;

9.2.2. Competition and contract legislation often includes consumer protection elements and

9.2.3. Sector-specific legislation like credit legislation can provide more targeted consumer protection.

9.3. E-Money Issuers shall comply with the following customer protection measures:

9.3.1. Transparency in pricing;

9.3.2. Full disclosure;

9.3.3. Protection of customer assets;

9.3.4. Protection of personal information;

9.3.5. Access to recourse mechanisms;

9.3.6. Provision of advice that is not sub-par; and

9.3.7. Availability to terms and conditions in plain language or language the customer understands.

9.4. E-money issuers should implement measures to ensure customers know mobile money accounts' transactional balance and limits.

9.5. The E-Money Issuer will comply with the Member State's legislation that regulates customer protection and all other related legislation, and the Central Bank shall take cognisance of the type and application of legislation that governs an E-Money Issuer.

9.6. An E-Money Issuer shall provide Mobile Money customers with the terms and conditions of Mobile Money Services, provide customers with information on how to raise disputes, and make available the E-Money Issuer's contact information.

9.7. The E-Money Issuer shall ensure that it has educational material available to its Mobile Money customers, which will advise on the Mobile Money services, the product information and relevant information required to enable the Mobile Money customer to manage their Mobile Money account.

9.8. The E-Money Issuer's systems must record all transactions. Such records must be made available to the Central Bank when required. Each system should be built in such a way that it can detect any breaches associated with customer accounts and transactions.

10. Interoperability

10.1. There are various levels of interoperability, which may be categorised as follows:

10.1.1. Platform-level interoperability enables customers of one E-Money Issuer to send money to customers of another E-Money Issuer;

10.1.2. Agent-level interoperability enables Agents of one E-Money Issuer to serve customers of another E-Money Issuer;

10.1.3. Customer-level interoperability enables customers to access their accounts through any SIM

10.2. These three forms of interoperability entail Mobile Money Services in one market interworking with each other.

10.3. The additional proposal for interoperability amongst Mobile Money Services is the provision of standard interfaces in which two or more E-Money Issuers in one country, each offering commercially and technically independent Mobile Money Services, offering a single interface to third parties to simplify the provision of bulk payments (P2B, B2P, B2B, G2P and P2G) merchant payments, and peer to peer payments (P2P). It is also possible for Mobile Money Services to interwork with other platforms outside their country and industry.

10.4. International Mobile Money interoperability is when two mobile money operators in different countries, each offering two commercially and technically independent Mobile Money Services, interconnect their respective technical platforms to enable their customers to send money to each other.

10.5. interoperability with banks: one E-Money Issuer in one country, operating its own commercially and technically independent Mobile Money Service, interconnecting its technical platform with the technical platform of a traditional financial services provider to enable interaction between the two platforms (i.e. the ability for a customer to send money from a Mobile Money account to a bank account, etc.)

10.6. interoperability with other payment networks: one e-money issuer, in one country, operating its own commercially and technically independent Mobile Money Service, interconnecting with a separate payment system (i.e. connecting with the Visa or MasterCard payment networks)

10.7. Most markets in SADC do not mandate interoperability; However, they include provisions encouraging E-Money issuers to create solutions that will cater to future interoperability. It is recommended that the Central Bank have provisions that will promote interoperability amongst E-Money Issuers irrespective of the issuer type.

11. Agent Network

11.1. The E-Money Issuer may contract agreements with Agents to offer Mobile Money Services. In such an instance, the E-Money Issuer is wholly responsible and liable for ensuring that the Agents comply with all legal and regulatory requirements set out by the Regulator. This arrangement is in line with the principal-agent relationship.

11.2. The Central Bank will set out procedures to be followed by the E-Money Issuer when contracting with Agents; information such as the below may be submitted for consideration and approval by the Central Bank when the E-money issuer is applying for a license:

11.2.1. A document that outlines the strategy of the E-Money Issuer, including current and potential engagements, geographical spread and benefits to be derived from appointing an Agent;

11.2.2. A document setting out the type of Agents envisaged, i.e. sole, sub or Super Agents and the allocation of Agent types;

11.2.2.1. Qualifying criteria for contracting Agents:

11.2.2.2. Outreach (network availability and connectivity)

11.2.2.3. Competencies

11.2.2.4. Financial Integrity - AML/ CFT

11.2.2.5. Agent E-money issuer agreements should not include exclusivity clauses to facilitate interoperability.

11.3. A copy of the draft service level agreements, including liquidity management provisions;

11.4. Risk management, internal control, operational procedures and any other policy and procedures relevant to the management of an Agent;

11.5. Description of the proposed technology to be used by the Agent;

11.6. Agent training materials:

11.6.1. KYC and AML provisions and supporting documents/material that Agent must comply with; and

11.6.2. An internal audit report regarding adopting internal controls was performed in readiness for the Agent to provide Mobile Money Services.

12. Data Privacy and Protection

All licensed DFSPs (E-money issuers and Banks) must comply with their respective countries' Data Privacy and Consumer Protection Act. DFSPs must comply with applicable data protection laws and regulations in their country of operation. In addition, they must:

12.1. Perform ongoing assessments and policy updates that align with evolving legal requirements.

12.2. Obtain customer consent before collecting and processing personal information.

12.3. Outline the security measures to protect customer data from unauthorised access, disclosure, alteration, and destruction.

12.4. Implement encryption protocols, secure storage practices, and access controls to prevent data breaches.

12.5. Ensure that data is deleted securely and promptly when no longer needed for the stated purpose.

12.6. Address the transfer of customer data across borders, primarily if the mobile money service providers are sending money across to another jurisdiction.

12.7. Ensure that such transfers comply with relevant data protection regulations.

12.8. E-money issuers are encouraged to educate users about data privacy practices. And provide information to users about how their data will be used and protected.

12.9. Acknowledge the role of regulatory authorities in overseeing and enforcing data protection measures.

12.10. Encourage ethical handling of customer data, emphasising transparency and fairness.

12.11. Incorporate privacy principles by design and default in the development and operation of mobile money services.

13. Technical standards

13.1. The Central Bank must set out the minimum technical standards to be complied with by the MMSP. The set standards promote interoperability and should align with international best practices/international standards. The minimum technical standards should be set out.

13.1.1. The standard messaging format is an example. ISO20022;

13.1.2. Security/Data Recovery protocols are to be observed, and

13.1.3. Data encryption protocols.

13.2. The technical standards for Mobile Money must consider the risk and security issues associated with technology-based products. The Central Bank must determine and make available an acceptable authentication mechanism to ensure security.

13.3. The technology deployed for Mobile Money transactions must adhere to domestic and international data and privacy protection protocols.

13.4. E-money issuers are encouraged to build innovative Mobile Money offerings that will suit the domestic market's requirements whilst considering future interoperability within the domestic market and the SADC Region.

14. Risk Management

Strategies for managing various payment risks include incorporating comprehensive frameworks to address multiple types of risks.

14.1. Outline measures to prevent, detect, and respond to fraud and security risks. This includes authentication protocols, encryption standards, and continuous monitoring for suspicious activities.

14.2. Since systems are susceptible to operational risks such as system failures, service interruptions, and technology glitches. Service providers must adhere to standards of redundancy, disaster recovery plans, and regular system audits.

14.3. Mobile money service providers must implement robust Know Your Customer (KYC) procedures to prevent illicit activities.

14.4. Service providers must protect against liquidity and credit risks to ensure the stability of the mobile money ecosystem. Adequate capital reserves and liquidity management strategies are recommended.

14.5. E-money issuers must establish partnerships with regulated financial institutions to manage financial transactions effectively through a trust account.

14.6. E-money issuers must implement measures to protect customer data and privacy. This includes clauses on data encryption, secure storage, and mechanisms for obtaining customer consent for data usage. Other risks that the service providers must mitigate are technology, consumer education and awareness, business continuity, and agent network risks.

14.7. The E-Money Issuer must have adequate Disaster Recovery and Business Continuity Plans to ensure the continued provision of Mobile Money Services.

15. Unclaimed Funds and Dormancy:

15.1. The E-Money Issuer shall be required to keep records of all inactive accounts with the associated unclaimed funds.

15.2. The Central Bank shall have provisions that will set out the processes to be followed by the E-Money Issuer when dealing with any unclaimed funds held by the E-Money Issuer and dormant and closed Mobile Money accounts.

15.3. In regulating unclaimed funds and closed Mobile Money accounts, the Central Bank shall consult the telecommunications regulator to ensure practical mechanisms for the transfer/termination and dormancy of the unclaimed funds or dormant or closed Mobile Money accounts.

15.4. The contemplated unclaimed funds' processes must consider the following aspects:

15.4.1. The period after which unclaimed funds are deemed “abandoned.”

15.4.2. The manner and mechanism in which the E-Money Issuer must hold the “abandoned” funds.

15.4.3. The period after which the customer has to claim the unclaimed funds.

15.4.4. If the stipulated period to claim the funds expires, the Central Bank must indicate where the funds should be apportioned.

16. Compliance and Enforcement:

16.1. The Central Bank shall include penalty clauses which may stipulate that:

16.1.1. It is an offence for any party to provide Mobile Money Services without being duly licensed by the respective Central Bank.

16.1.2. It is an offence for any E-Money Issuer to contravene or breach any provision of the Central Bank published document on Mobile Money regulation.

16.1.3. The Central Bank shall stipulate penalties to E-Money Issuers who do not comply with the technical standards for transaction limits and processing.

16.1.4. The Central Bank shall stipulate the penalties related to the offences by its domestic legislation.