RISK MANAGEMENT POLICY

Confidentiality Agreement and Notice of Proprietary Information

This document contains information proprietary to **Selcom Tanzania** and by reading it you agree to protect its confidentiality and not to disclose the information herein to any third parties outside your organization. You further agree to ensure that any and all parties within your organization that are availed any information hereinabide by this confidentiality obligation.

This document shall not be reproduced in whole or in part without the express written consent of **Selcom Tanzania.** The disclosure of information, ideas or concepts presented and contained herein is solely meant for review by your organization and does not constitute any license or authorization to use the same for purposes other than the proposed project proposal.

Contents

Document Control

Date	Version	Requester	Tech. Writer	Change/Review
20-05-2017	V1.0	Sameer Hirji	Mohammedjawaad Kassam	Sarah Mohamed
08-06-2017	V1.1	Sameer Hirji	Mohammedjawaad Kassam	Sarah Mohammed
08-06-2019	V1.1	Sameer Hirji	Mohammedjawaad Kassam	Sarah Mohammed

1. Introduction

Mobile Financial Services offer significant opportunities for improving the efficiency of financial services by expanding access and lowering transaction costs. The rapid public acceptance of these services in many countries has demonstrated that the technology is mature and brings realbenefits to people who previously could not access financial products or services.

With the number of operations and a growing number of customers involved in the service, formalized risk management which balances the assurance of an enabling environment that is conducive to innovation and economic development against consumer protection concerns becomes more and more important.

This document aims to outline the risks involved with providing services that Selcom offers. Specifically, this document describes and analyses various risk types surrounding the services aswell as the parties that would be affected. Additionally, risk mitigation actives for each identified potential risk have also been described.

2. **Risk Definitions:**
The risk discussed in this document are those that different parties to a given transaction type would be exposed to. Each risk type is defined below:

- Systemic:
A risk that could cause collapse of, or significant damage to, the financial system or a risk which results in adverse public perception, possibly leading to lack of confidence and worst-case scenario, a "run" on the system and/or contagion effect.

- Operational:
A risk which damages the ability of one of the stakeholders to effectively operate their business or a risk which results in a direct or indirect loss from failed internal processes, people, systems or external events

- Reputation:
A risk that damages the image of one of the stakeholders, the mobile system, the financialsystem, or of a specific product.

- Legal:
A risk which could result in unforeseeable lawsuits, judgment or contracts that could disruptor affect MFS business practices

- Liquidity:
A risk that lessens the ability of a bank or MFS provider/agent to meet cash obligations upon demand

- Fraud:
A risk which increases the exposure of one or more stakeholders to loss of their money heldwithin the system because of deliberate deception, trickery, or cheating by other stakeholders in the system.

3. Roles

The roles assumed by each party include any or a combination of the following;

1. Brand Provider: This refers to the brand name carried by the Mobile Money product in themarket

2. Payment Services Provider (PSP): This refers to the role of managing a system whichswitches payment transactions on behalf of bank(s)

3. Agent Aggregator: this refers to the role of acquiring and managing the agency networkrequired to perform Agency banking.

4. Bank: This refers to the roles of float management and transaction settlement. This role onlyapplies to and MNO where that MNO has secured a banking license

5. Communications bearer: This is the role where an MNO delivers transactions to / from the Mobile Phone. For a bank to assume this role it typically needs to obtain an MNO or MVNO(Mobile Virtual Network Operator) license.

When analyzing the risk borne by an MNO or bank it is important first to analyze which of the above roles the entity is performing. In the Table below, the risks are analyzed by role rather thanperformer of the role.

4. Mobile Payment Risk Matrix

The matrix below demonstrates the most common risks identified in actual operations and maps themto the categories that may be applicable under the Selcom responsibilities.

Risk Name	Risk Description	Risk Impact	Risk Category	Mitigant
Identify theft	Sufficient elements of the customer data become compromised to allow another party to replicate the customer's identity in the system, thereby fraudulently using the customer's identity to conduct transactions	Agent– Reputational Bank – Reputational and Fraud PSP – Reputational Client – fraud Brand owner Reputational	Operational (Level 1 category – Internal and External Fraud; Level 2 – Theft and Fraud)	Only allowing each customer to have one account in the system PIN protection, and good processes for PIN resets.
Impersonation of provider status	An unauthorized agent acts as an authorized agent, mostly performing cash in and cash out transactions but charging fees which are not agreed to by the scheme operator, or for the purpose of confidence trickery to gain access to the customer's secret information. There have also been incidents where such "agents" have defrauded the depositor and absconded with the deposited amount	Agent– Reputational Bank – Reputational and Fraud PSP – Reputational Client – fraud Brand owner Reputational	Operational (L1 – Internal and External Fraud; L2 – Theft and Fraud)	Clearly publishing the fee structure to the client, as well as consistent agent branding. Agents should assist the MM provider to identify the active, but unauthorized agents in the market. Clients should be educated that, unless they are notified by the Mobile Money scheme directly of any given deposit, they should not pay over their cash to the agent.
Inability to transact	The transactions within a mobile payments network travel through many communications systems to reach the MM backend. Any breakage in this chain can lead to an inability to transact. Customer literacy levels are also a factor here.	Agent– Reputational Bank – Reputational PSP – Reputational Client – Inconvenience Brand owner Reputational	Operational (L1 – Execution, Delivery and Process Management; L2 - Transaction Capture, Execution, and Maintenance)	Redundant pathways through the network need to be established as far as is possible. The MM operation should also actively test the Mobile operator's ability to deliver messages via machine generated messages on a cyclical basis. Menu structures

				which do not change often can be used by illiterate people who learn keystroke sequences to navigate menus. All transactions are to be defined with clear completion boundaries, thus allowing for clear rollback procedures in the event of uncertainty.
Transaction replay by the network	MNO's often have retry patterns to deliver an SMS to a destination. These are triggered when a send to the recipient does not generate an appropriate receipt. MM platforms which receive SMS's sometimes receive multiple copies of the same SMS bearing a transaction, which the system could interpret to be multiple instructions from the client to affect a payment.	Agent– Reputational Bank – Reputational / Commercial PSP – Reputational Client – Loss of funds / difficulty recovering them Brand owner – Reputational	Operational (L1 – Execution, Delivery and Process Management; L2 - Transaction Capture, Execution, and Maintenance)	Arrangements should be made with the operator to disable SMS retry patterns for MM transactions. This means that a transaction will either succeed in a very short period of time or fail, leaving the customer in a surer position after transaction submission. Transaction requests should also be numbered at source by the MM menu on the phone, and the back end system should only post a given transaction request once.
Relationship difficulties between the owners of the service – leading to service outage	MM products are often delivered by consortia of mobile operator(s), bank(s) agent network manager(s) and agents. These consortia are often serviced by third party software vendors whose support is critical for systems changes. Any significant relationship difficulty	Agent– Reputational and commercial Bank – Commercial PSP – Reputational and commercial Client – Inconvenience through loss of service Brand owner – Reputational	Operational (L1 – Execution, Delivery and Process Management; L2 – Vendors and Suppliers)	The relationships need to be carefully planned at service inception to ensure that all parties are adequately reimbursed for their participation in the process. The MM provider needs to retain a position of consortium leadership to ensure that all parties

	within this consortium could result in service unavailability to a client or to all clients.			remain committed to the product.
Transaction delayed by network	Message delivery through a mobile network takes place via multiple interconnected systems. At each point in the chain delays are possible. Any delay in transmission leaves the customer and agent in a difficult position of not knowing whether or not the transaction has been delivered, and therefore whether or not to re-submit the transaction.	Agent– Reputational Bank – Reputational PSP – Reputational Client – Inconvenience and the risk of incorrectly making the same payment more than once Brand owner – Reputational	Operational (L1 – Execution, Delivery and Process Management; L2 – Transaction Capture, Execution, and Maintenance)	Arrangements should be made with the operator to disable sms retry patterns for MM transactions. This means that a transaction will either succeed in a very short period of time or fail, leaving the customer in a more sure position after transaction submission. Agent and customers should also be educated to confirm balances where there is uncertainty regarding completions of a given transaction.
Insufficient points at which to use Mobile Money leading to customers withdrawing from the service	A pure mobile money offering seldom has access to any parts of the existing payments system, which means that many of these payment destinations need to be re-created for the mobile money operation. Any client who takes up the product before a significant number of these points has been activated will find little use for the product	Agent– Reputational, insufficient business volume Bank – Commercial PSP – Reputational, insufficient business volume Client – Inconvenience Brand owner – Reputational	Strategic Operational (L1 – Execution, Delivery and Process Management; L2 – Vendors and Suppliers	The product rollout needs to be managed as a network product, i.e. agents, bill pay recipients, merchant payment locations etc. need to be rolled out in a geographically harmonized manner. Rolling out a card (Selcom Card) in conjunction with the mobile money product may also enable access to existing payment system resources.
Lack of cash or electronic float at agent outlet	A client wishing to deposit or withdraw money to the system may	Agent– Reputational, insufficient business	liquidity	Agents need to be rolled out in conjunction with consumers, and

	be temporarily or permanently unable to do so on account of the agent not having sufficient cash or electronic float to perform a transaction.	volume Bank – Commercial PSP – Reputational, insufficient business volume Client – Inconvenience Brand owner – Reputational		need ongoing management to ensure that there are no e money shortfalls at the agent locations. Agents need to adequately fund this line of business in terms of cash and electronic float. Ongoing systems monitoring is also crucial to prevent systems outages from preventing access to the agent's electronic balances
Abuse of customer details by any member of the supply chain	MM operations often rely on networks of agents, managed by agent network managers to gather customer details for KYC. Any member of this chain with access to the customer registration details could use these details for other fraudulent purposes.	Agent– Reputational Bank – Reputational PSP – Reputational Client– Fraud Brand owner Reputational	Operational (L1 – Execution, Delivery and Process Management; L2 - Transaction Capture, Execution, and Maintenance) (L1 – Clients Products and Business Practices;L2 – Selection, Sponsorship and Exposure) L1 – Internal and External Fraud; L2 – Theft and Fraud)	Rapid collection of original documentation from the network may reduce the incidence of this type of fraud. Agents need to be vetted for character during their appointment process. Clear and direct action in the event of occurrence will also mitigate against recurrence. The agent needs to implement stringent customer detail management processes in its outlets.
Spoofed transactions being used to make cash withdrawals	Depending upon the security level of the underlying system, it may be possible for people posing as clients of the MM solution to inject notifications to the merchant which appear to be cash withdrawal approvals. If these are acted upon	Agent– Fraud Bank – Commercial / fraud PSP – Reputational Client – Fraud Brand owner – Reputational	Operational (L1 – Internal and External Fraud; L2 – Theft and Fraud)	The Mobile Money system needs to have sufficient inherent system security features to minimize these types of technical attacks. Examples of this include anything from end to end transaction encryption and

	the resultant cash paid out will be lost by the agent This may result in the agents withdrawing their support for the Mobile Money operator.			mac'ing to keeping the agent's mobile number secret and requesting that the MNO block SMS header spoofing. The agent also needs to train its staff to focus on the transactions to ensure that they are valid.
Teller counting errors during cash in and cash out operations	If the teller miscounts the amount of cash deposited or withdrawn, the resultant shortfall / surplus will accrue to the agent This may result in the agents withdrawing their support for the Mobile Money operator.	Agent– Commercial Bank – Commercial PSP – none Client – Commercial Brand owner – Reputational	Operational (L1 – Execution, Delivery and Process Management; L2 - Transaction Capture, Execution, and Maintenance)	The tellers need to maintain vigilance.
Mobile money program fails to reach sustainability	If the Mobile Money program as a whole fails to reach the point of commercial sustainability, the sponsors may withdraw	Agent– Reputational and commercial Bank – Reputational and Commercial PSP – Reputational Client – Inconvenience Brand owner Reputational	Strategic Operational (L1 – Execution, Delivery and Process Management; L2 – Vendors and Suppliers)	The MM operator needs to ensure that the system overall grows at a suitable pace.
Improper data capture by agents during OTC remittance transaction	Data capture errors made by the agent may result in misdirected remittance transactions	Agent– Reputational / relationship Bank – Reputational / commercial PSP – None Client – Inconvenience / loss of funds Brand owner	Operational (L1 – Execution, Delivery and Process Management; L2 - Transaction Capture, Execution, and Maintenance)	Customers remitting to the same recipients multiple times should be encouraged to pre-register their beneficiaries Remitting banks should validate the remittance fields (such as account number and name) Full details of recipients should be obtained from the remitter and should be validated by the payout station
System and Bank Pool	The funds under management in a	Agent– None Bank – Liquidity	Operational (L1 –	Mobile money system integration

Account Variances	mobile money system are reflected in a corresponding 'pool' bank account. The mobile money system mainly comprises of payments within the 'closed loop' of the system. These intra-system value transfers do not impact total value within the system. However external payments into the system (e.g. payroll & G2P) & out of the systems (3 rd party bank ATM withdrawals, & bill-payment), require 'system-value' adjustments. The adjustments need to be reflected in corresponding bank pool account. The risk is that there is a variance between the two values	PSP – None Client – Inconvenience / loss of funds Brand owner Reputational	Execution, Delivery and Process Management; L2 - Transaction Capture, Execution, and Maintenance)	into bank pool account so all changes to main bank account is reflected. End of day variance reports to managed and signed off by appropriate business management. If manual system value changes are required. Robust system authority approver & checker function is required by operator & bank personel

Monitoring Controls

Compliance Unit carry out reviews and implement any procedures as deemed necessary, A full reviewof the risks that the organization faces are undertaken annually. Risk Monitoring is done on daily basisfor the Mobile Financial transactions. AML Policy is in place which is further monitored by Compliance Team. Compliance unit consists of the Legal Officer, Senior Manager-Revenue Assurance andReconciliation Officer and IT Compliance Officer.

Compliance Unit reports to the director for strategy who reviews all risk monitoring related documentation. A formal review of all the risks mentioned in this document will need to be done at a departmental level. If any risks have materialized, changes should be implemented as and if necessaryand applicable.