East African Communications Organisation

MANUAL ON HARMONIZED STRATEGY TO ADDRESS RISKS IN DIGITAL FINANCIAL SERVICES

TABLE OF CONTENTS

ABBREVIATIONS 3
1. INTRODUCTION 4
2. OBJECTIVE OF THE MANUAL 4
3. SCOPE 4
4. DIGITAL FINANCIAL SERVICES ECOSYSTEM 5
5. RISKS IN DIGITAL FINANCIAL SERVICES 6
5.1. Nature of risks in Digital Financial Services 6
6. SITUATION ANALYSIS IN THE EACO REGION 6
6.1. Ecosystem of Digital Financial Services in EACO Member States 7
6.2. Institutional Collaborations in DFS 7
7. ITU RECOMMENDATIONS ON SECURITY FOR DIGITAL FINANCIAL SERVICES. 8
7.1. Recommendations on regulatory collaboration 8
7.2. Recommendations to manage threats to the DFS ecosystem and mechanism to secure mobile payment applications. 9
7.3. Recommendations to assess security controls and digital financial service applications. 9
7.4. Recommendations to address SIM swap fraud and related risks. 10
7.5. Recommendations to address Telecom infrastructure vulnerabilities. 10
7.6. Educate and Empower consumers 10
8. STRATEGIES TO MITIGATE RISKS IN DFS 10
8.1. Creating and enabling environment 10
8.2. Robust, resilient, and secure digital infrastructure 11
8.3 Research and Innovation 11
9. MONITORING AND EVALUATION 11
10. CONCLUSION 12
11. RECOMMENDATIONS 12
12. REFERENCES 12

ABBREVIATIONS

ATM's:	Automatic Teller Machines
BoU:	Bank of Uganda
DFS:	Digital Financial Services
EAC:	East African Community
EACO:	East African Communications Organisation
ICT:	Information and Communications Technology
ITU:	International Telecommunications Union
ITU-T-FG-DFS:	International Telecommunications Union Standardization Focus Group on Digital Financial Services.
KYC:	Know Your Customer
MMSP	Metering and Monitoring Service Package
MNO:	Mobile Network Operator
MoU:	Memorandum of Understanding
SIM:	Subscriber Identity Module
SS7:	Signaling System 7
STK:	SIM Application Toolkit
USSD:	Unstructured Supplementary Service Data
WG3:	Working Group Three

1. INTRODUCTION

Digital Financial Services (DFS) refers to a broad range of financial services accessed and delivered through digital channels other than the traditional means of using physical cash, notes, and coins. These services include, online banking, bank to bank transfers, use of Automatic Teller Machines (ATMs), online transactions, mobile banking, mobile lending, mobile money among others.

According to research by the International Telecommunications Union (ITU), 'the recent growth of digital financial services has allowed millions of people who are otherwise excluded from the formal financial system to perform financial transactions relatively cheaply, securely, and reliably[1]. For instance, mobile financial services have been a game changer for people of limited income and an enabler for financial inclusion in the East African Region.

2. OBJECTIVE OF THE MANUAL

This manual aims to give EACO member countries a harmonised roadmap on how to address the risks in digital financial services. The manual further highlights the risks and vulnerabilities that consumers and providers of digital financial services may face.

The Specific objectives of the manual are:

a.) To identify risks associated with digital financial services.

b.) To develop a common strategy to mitigate risks associated with the design, use and deployment of digital financial services; and

c.) To develop a mechanism to monitor the implementation of the strategies employed by EACO Member states.

3. SCOPE

The manual focuses on the risks in DFS in the six EACO member countries and proposes a strategy to address these risks.

The intention is not to duplicate efforts already undertaken by member countries, but rather recommend best practices related to policies and regulatory frameworks for digital financial safety.

The manual is guided by member countries' initiatives and programmes, literature on digital financial service and recommendations of the ITU-T FG-DFS.

[1] https://www.itu.int/en/ITU-T/focusgroups/dfs/Pages/default.aspx

4. DIGITAL FINANCIAL SERVICES ECOSYSTEM

The development and increased accessibility of digital financial services has seen a corresponding increase in consumer uptake of these services.
The provision of digital financial services is dependent on the following players in the market each with different responsibilities.

SN	Stakeholder	Responsibility
1	Regulating Bodies	➢ Set minimum operating requirements for mobile network operators. ➢ Set know-your-customer norms for mobile network operators. ➢ Supervise mobile network operators
2	Mobile Network Operators (MNO)	➢ Host and manage individual mobile money accounts for end-users. ➢ Set end-user operational requirements for mobile money. ➢ Manage and control mobile money transactions. ➢ Administer end-user mobile money accounts. ➢ Responsible for the information security management of mobile money. ➢ Oversight of mobile money agents.
3	Network Operators	➢ Provide wired and wireless communications services.
4	Financial Institutions	➢ Host the main mobile money account on behalf of the mobile network operators. ➢ Manage foreign exchange.
5	Mobile Application Developers	➢ Develop mobile money applications
6	Mobile Money Agents	➢ Register mobile money users. ➢ Disburse cash to mobile money end-users. ➢ Keep money float on behalf of MNO. ➢ Process electronic money for mobile money end-users.
7	Mobile Money End-users	➢ Hold mobile money accounts (electronic wallets). ➢ Send electronic money to the intended. ➢ Receive mobile cash.
8	Merchants and Retailers	➢ Accept mobile money in exchange for goods and services.
9	Device Manufacturers	➢ Manufacture and sell mobile devices such as mobile phones, tablets that MNO purchase to run the mobile money applications used by mobile money customers.
10	Law Enforcement agencies.	➢ Undertake investigations of incidences ➢ Support enforcement of regulatory Instruments.

5. RISKS IN DIGITAL FINANCIAL SERVICES

The development and increased accessibility of digital financial services has seen a corresponding increase in consumer uptake of these services. However, this development has also seen increased exposure to online risks and vulnerabilities to both the providers and consumers of DFS.

5.1. Nature of risks in Digital Financial Services

a) **Product Risk**. Owing to the design of digital financial services e.g., bulk payments, insurance, mobile savings and credit, prepaid cards, and cross-border and international money transfer services can create a lot of opportunities for fraud.
b) **Channel Risk**. This risk arises from the ubiquity of mobile phones and the extent to which new and less experienced consumers are entering the market through this channel.
c) **Agent Risk**. Providers with large agent networks find it challenging to build adequate infrastructure and systems for effective agent oversight and monitoring of compliance violations, especially in remote areas.
d) **Customer and Compliance Risk**. Countries with large numbers of unbanked, illiterate, and/or rural populations that lack national identification regimes find it difficult to ensure know your customer (KYC) due diligence and to track criminal activity, especially given that frontline KYC checks often rely on agents rather than branch staff.
e) **System and Delivery Risk**. System down times delay service delivery and can create opportunities for fraud. Inadequate system and access controls may also facilitate abuse of access rights and give rise to fraud. Lack of automated fraud management systems impede comprehensive transaction monitoring and sanctions screening to detect fraud and terrorist activity.
f) Regulatory, Supervision, and Enforcement Risk. Some markets also have inadequate regulatory regimes for mobile money, which can lead to the proliferation of unlicensed money transfer agencies or unregulated money transfer products, which in turn can facilitate fraud, money laundering, and other criminal activity. **See *Annex.1* for the detailed list of risks in DFS.**

6. SITUATION ANALYSIS IN THE EACO REGION

This section aims to collate and document information on current initiatives from member countries in DFS; best practices on policies, regulatory frameworks, consumer, and fraud prevention interventions, that shall inform a harmonized strategy. We have since established that:

6.1. Ecosystem of Digital Financial Services in EACO Member States

It is notable that the region is leading in the adoption of DFS. Within the EACO member states, regulators of the ICT, and financial sectors exist. Additionally, several states have entered into collaborative agreements in form of MoU's to jointly address issues relating to the provision of digital financial services.

With regards to access to digital financial services, most of the services are accessed over the mobile phone through use of USSD or STK and services mainly accessed through mobile service providers.

It is notable that the member states have various concerns relating to the design, access, and deployment of digital financial services, specifically challenges in the following areas:

1. Regulatory challenges such as violation of legislation on SIM Registration which then results in fraud and exposure to social engineering attacks on DFS customers. Other challenges revolve around the boundaries and scope of the various regulatory agencies and the regulation of the digital financial services.
2. Interoperability issues owing to need for more efficient and affordable mechanism to facilitate interoperability across various service providers and agencies in the DFS ecosystem. This has resulted in high costs that are then transferred to the consumers of these services and consequently affecting the adoption of DFS services.
3. Tax regimes have seen these services as a source of revenue and as such, increasingly taxed for these services and consequently affecting the adoption of DFS services.
4. In most of the member countries, connectivity is a major impediment to its citizens having access to communication services including digital financial services.
5. Mobile money agents experience challenges such as liquidity management, fraud, limited support from MMSPs, and theft, among others.
6. Low digital literacy, compounded by low digital financial literacy limit the adoption of digital financial services in rural areas.
7. Low levels of awareness on consumer rights and responsibilities.
8. Limited mobile phone penetration inhibits access to digital financial services.

6.2. Institutional Collaborations in DFS

Given the different players in the DFS space, successful strategies to address the risks require a collective concerted effort from key stakeholders.

In furtherance to the commitments made in their respective MOUs with the financial sector regulator, is notable that two (2) out of the six (6) EACO member states have initiated projects that are geared towards securing infrastructure that is to be used by Digital

financial services. The following are some of the projects and initiatives that have been undertaken in the region.

1. Joint Consumer Awareness on Digital financial services
2. Development of a Digital Financial Literacy Module
3. Collaboration on complaints handling and redress
4. The setting up of a DFS security lab
5. Joint training on DFS security by the ITU FG-DFS
6. Adoption of ITU recommendations.

7. ITU RECOMMENDATIONS ON SECURITY FOR DIGITAL FINANCIAL SERVICES.

In 2014, the International Telecommunication Union (ITU) established a Focus Group on Digital Financial Services (ITU FG-DFS). The focus of the group is to provide a platform that brings together various stakeholders in the digital financial system ecosystem with a view to developing a roadmap for use by policymakers and regulatory authorities to facilitate the development of digital financial services[2].

At the end of the Focus Group's activities in 2017, the Financial Inclusion Global Initiative (FIGI) was established. This three-year program, funded by the Bill & Melinda Gates Foundation and implemented in partnership with the World Bank Group (WBG), the Committee on Payments and Market Infrastructure (CPMI), and the International Telecommunications Union (ITU) sought to support and accelerate the implementation of country-led reform actions so as to meet national financial inclusion targets, with the ultimate global of achieving the '*Universal Financial Access 2020'* Agenda3. The Universal Financial Access 2020 goal, as defined by World Bank, envisions that all adults would have access to a transaction account or electronic instrument to store money, send and receive payments4.

The FIGI's three working groups; Digital Identity, Electronic Payments Acceptance, and Security, Infrastructure and Trust sought to advance research and accelerate of digital financial inclusion in developing countries. Below is a summary of the recommendations from the technical reports developed by the Security, Infrastructure and Trust Working Group under FIGI:

7.1. Recommendations on regulatory collaboration

This recommendation details the areas of convergence and the roles that regulators need to play to promote the deployment of secure, safe, and reliable DFS.

[2] https://www.itu.int/en/ITU-T/focusgroups/dfs/Pages/default.aspx
[3] https://figi.itu.int/about-us/
[4] https://ufa.worldbank.org/en/ufa#:~:text=Universal%20Financial%20Access%202020&text=Financial%20access%20is%20the%20first,%2C%20payments%2C%20credit%20and%20insurance.

The recommendation calls for the Telecommunications Regulator and Financial Regulator to enter an MoU to progress the implementation of joint initiatives that achieve this objective. The ITU FG-DFS has developed a model MoU for consideration by the regulators.

7.2. Recommendations to manage threats to the DFS ecosystem and mechanism to secure mobile payment applications.

These recommendations are documented in the [5]Digital Financial services Assurance Framework and the [6]Consumer competency framework.

The recommendations detail the best practices that regulators could adopt as technical regulations to set the minimum-security baselines for DFS regulators, and developers and which can also be audited thereafter by the regulator to verify compliance.

The DFS security assurance framework details recommendations that manage the threats and vulnerabilities to the digital finance ecosystem. These are to be implemented by regulators in both the telecommunications and financial sectors; and industry providers in the two markets; digital finance regulators and providers. Recommendations relate to consumers' competency, detail consumer knowledge and skills requirements to enable them have a safer experience when accessing and using DFS services.

7.3. Recommendations to assess security controls and digital financial service applications.

These recommendations are documented in the DFS Security Audit Guidelines and the Mobile Application Security Best practices. They call for regulators in both the telecoms and financial sector, and industry players to have in place an audit system and process that ensures adequate protection to DFS systems exist, are functional and operational. This would consequently result in strengthening and hardening of the security and process controls.

With regards to security controls for DFS applications, ITU FG-DFS recommends that specific minimum-security requirements are provided for in technical guidelines or regulations.

[5] https://figi.itu.int/wp-content/uploads/2021/04/Technical-report-on-Digital-Financial-Services-Security-Assurance-Framework_f-1-1.pdf

[6] https://figi.itu.int/wp-content/uploads/2021/04/Digital-Financial-Services-Consumer-Competency-Framework-1.pdf

7.4. Recommendations to address SIM swap fraud and related risks.

Documented in the Security recommendations to protect against DFS SIM risks and SIM swap fraud. They call for regulators and service providers to develop and implement technical measures to mitigate SIM vulnerabilities (SIM swaps, SIM recycling, and attacks on SIMs like binary over the air attacks).

It is notable that these recommendations require collaborative effort between the regulator of the financial sector and the telecom regulator.

7.5. Recommendations to address Telecom infrastructure vulnerabilities.

This recommendation is detailed in the[7]SS7 Vulnerabilities and Mitigation Measures for DFS Transactions and acknowledges the existence of vulnerabilities on the telecom infrastructure network, where calls and SMSs can be intercepted, mobile money gets stolen, and network operations are interrupted.

It provides mechanisms that could be employed by regulators and service providers to address these vulnerabilities. In addition, ITU-T has issued Recommendation X.805 *'Security architecture for systems providing end-to-end communications*. This recommendation defines the general security related architectural elements, when appropriately applied can provide end-to-end network security.

7.6. Educate and Empower consumers

The ITU FG-DFS recommendation titled "[8]DFS Consumer Competency Framework" provides guidance to policymakers, national regulators and DFS providers on how to develop consumer awareness and literacy programmes as part of the DFS/financial inclusion strategy.

8. STRATEGIES TO MITIGATE RISKS IN DFS

8.1. Creating and enabling environment

To increase access and use of DFS within the East African region, it is critical that Member States develop and implement the relevant legal and legislative provisions to promote the development of secure and reliable DFS.

[7] https://figi.itu.int/wp-content/uploads/2021/04/Technical-report-on-the-SS7-vulnerabilities-and-their-impact-on-DFS-transactions_f-1-1.pdf
[8] https://figi.itu.int/wp-content/uploads/2021/04/Digital-Financial-Services-Consumer-Competency-Framework-1.pdf

EACO member states would in addition need to develop an institutional collaborative framework with relevant stakeholders in the DFS ecosystem to leverage their respective mandates and roles within the ecosystem.

Further still, to increase consumers' confidence in the use of DFS, there would need to be extensive consumer education and empowerment on DFS Access, benefits, and risks.

To create an enabling environment, Member States would need to develop a National Digital Financial Services policy that would enable each to build an efficient and effective digital financial services ecosystem.

In addition to the above, each member country would need to develop and implement the appropriate legislative provisions of services, mitigation of the risks, and security assurances; as well as mechanisms to avail information to consumers and provide for consumer data protection and privacy safeguards.

8.2. Robust, resilient, and secure digital infrastructure

The growth and development of DFS relies on the existence of a robust, resilient, and secure digital infrastructure. And for consumers to access these services, it is crucial that appropriate technical and operational measures leverage and infuse into existing and future digital infrastructure.

In so doing, member states are encouraged to develop appropriate industry guidelines for solutions, applications, and devices that spell out the required technical, operational, and security standards that provide the necessary safeguards for digital transactions.

There would be need for capacity building across the entire DFS value chain to ensure that the appropriate safeguards are in place and the technical and operational expertise is availed in the market. This further strengthens collaborative efforts by the various entities within the DFS ecosystem.

8.3 Research and Innovation

EACO member countries have extensively leveraged DFS, however, there is need to invest in research and innovation to enable countries within the region to benefit from the role that DFS plays in financial inclusion.

9. MONITORING AND EVALUATION

It is anticipated that EACO member states shall implement this strategy at the different Country levels. The EACO WG3 shall monitor the implementation of this strategy and prepare an annual report on the status of its implementation.

10. CONCLUSION

The use of DFS has grown exponentially, especially after the COVID-19 pandemic. Both consumers and service providers are exposed to numerous risks and vulnerabilities in the access, deployment, and use of digital financial services

There is a need to embed security measures in the deployment of DFS end-to-end, and an urgent need for collaboration in the development and implementation of standards for the design and deployment of digital financial services.

11. RECOMMENDATIONS

Members states are encouraged to prioritize the implementation of this strategy and demonstrate commitment at all levels.

Regulators of ICTs in each member state need to enter into Memoranda of Understanding with financial regulation institutions to address financial security aspects in the DFS.

EACO Members states need to commit resources to implement the strategy (Financial and Human).

12. REFERENCES

1) ITU-T Focus Group Digital Financial Services, The Digital Financial Services Ecosystem - 2016

2) Recommendation ITU-T - 'Terms of Reference for the Focus Group Digital Financial Services.

STRATEGIC PLAN

Key Result Area	Strategic Objective	Strategic Initiative	Strategic Activity	Expected Output	Responsible agencies
Enabling Environment to support development of DFS	Promote development of secure and reliable digital financial services	Enhance legislative framework to address DFS risks and vulnerabilities	Develop a National Digital Finance Services Policy	National Policy	Ministry/National Regulatory Agency
			Develop regulations for provision and management of digital financial services	Regulations	National Regulatory Agencies (Telecoms and financial sector)
			Develop and implement industry risk assessment framework for digital financial services	Framework	National Regulatory Agencies (Telecoms and financial sector) Industry players
			Develop and implement industry security assurance framework	Framework	National Regulatory Agencies (Telecoms and financial sector) Industry players
			Develop licence conditions that mitigate risks related to Digital financial services	Reviewed Licence	National Regulatory Agencies (Telecoms and financial sector)

Key Result Area	Strategic Objective	Strategic Initiative	Strategic Activity	Expected Output	Responsible agencies
		Develop institutional collaborative framework for stakeholders in the Digital financial services ecosystem	Institution collaboration between the ICT regulator and the regulator of the financial sector	Memorandum of Understanding	National Regulatory Agencies (Telecoms and financial sector)
			Engage relevant agencies and organizations through appropriate collaborative instrument (MoU etc.)	Memorandum of Understanding	National Regulatory Agencies (Telecoms and financial sector) Industry Players Industry Stakeholders
			Implement joint collaborative initiatives and programmes to increase security and reliability of digital financial services	Reports	National Regulatory Agencies (Telecoms and financial sector) Industry Players Industry Stakeholders Law enforcement agencies
			Implement joint compliance and enforcement activities	Reports	National Regulatory Agencies (Telecoms and financial sector) Industry Players Industry Stakeholders Law enforcement agencies
	Empower Consumers of	Ensure transparency in the provision of	Develop mechanism to avail and proactively	Consumer information	National Regulatory Agencies (Telecoms,

Key Result Area	Strategic Objective	Strategic Initiative	Strategic Activity	Expected Output	Responsible agencies
	Digital Financial Services	digital financial services	disclose information on digital financial services		Financial sector, Competition) Consumer Organizations
		Promote use of data protection mechanisms in provision of digital financial services	Develop and implement data protection requirements in the provision of digital financial services	Legislation (Law/ regulations/ guidelines/ licence conditions e.t.c)	National Regulatory Agencies (Telecoms and financial sector) National Data Protection agency Industry Players Industry Stakeholders
		Education and empower consumers	Establish consumer information, knowledge and skills gap of users of digital financial services	Reports	National Regulatory Agencies (Telecoms, Financial sector, Competition) Consumer Organizations
			Develop and implement consumer education and empowerment programmes on digital financial services	Reports	National Regulatory Agencies (Telecoms, Financial sector, Competition) Consumer Organizations
Robust, resilient, and secure	Technical and Operational Effectiveness	Secure DFS applications and services	Develop industry technical and operational requirements for	Legislation (Law/ regulations/ guidelines/	National Regulatory Agencies (Telecoms and financial sector)

Key Result Area	Strategic Objective	Strategic Initiative	Strategic Activity	Expected Output	Responsible agencies
digital infrastructure			provision of Digital Financial Services	licence conditions e.t.c)	Industry Players Industry Stakeholders
			Develop industry guidelines for development of digital financial services solutions, applications and design of devices	Industry Guidelines	National Regulatory Agencies (Telecoms and financial sector) Industry Players Industry Stakeholders
			Develop accreditation/ testing/ verification mechanism for digital financial services, applications and devices	Mechanism	National Regulatory Agencies (Telecoms and financial sector) Industry Players Industry Stakeholders
		Effective Incident resolution mechanisms	Development of an efficient and effective reporting and incident management framework	Framework	National Regulatory Agencies (Telecoms and financial sector) Industry Players Industry Stakeholders
			Harmonization of incident resolution mechanisms across agencies, organizations and EACO member states	Regional Framework	National Regulatory Agencies (Telecoms and financial sector) Industry Players Industry Stakeholders
	Capacity building on	Build capacity and expertise	Develop curriculum	Curriculum	National Regulatory Agencies (Telecoms and financial sector)

Key Result Area	Strategic Objective	Strategic Initiative	Strategic Activity	Expected Output	Responsible agencies
	regulation and provision of DFS				Industry Players Industry Stakeholders
			Undertake capacity building initiatives	Reports	National Regulatory Agencies (Telecoms and financial sector) Industry Players Industry Stakeholders
Research and Innovation	Build an effective, resilient and versatile ecosystem	Understand DFS ecosystem	Undertake research on trends in the provision and use of digital financial services	Reports	National Regulatory Agencies (Telecoms, Financial sector, Competition) Industry players
			Undertake benchmarking activities	Reports	National Regulatory Agencies (Telecoms, Financial sector, Competition)
			Establish liaisons and relationships with other organizations in the DFS.	Instruments of Engagement (e.g. MoUs)	
			Organize country thematic workshops (ITU-T recommendation) to collect input from various stakeholders (Telecommunications	Reports	

Key Result Area	Strategic Objective	Strategic Initiative	Strategic Activity	Expected Output	Responsible agencies
			regulators, financial regulators, policymakers, and law enforcement agencies.		
		Enhance consumer protection mechanisms	Leverage emerging technologies to ease use of privacy and security features of digital financial services	Mechanisms	National Regulatory Agencies (Telecoms, Financial sector) Industry players
			Undertake consumer behavior research on access and use of digital financial services	Reports	National Regulatory Agencies (Telecoms, Financial sector) Industry players

Annex I: Compiled Consumer Risks on Mobile Financial Services from Kenya, Rwanda, TZ and Uganda.

Risk Name	**Risk Description**	**Recommendations to address risks**
Identity theft	Sufficient elements of the customer data becomes compromised to allow another party to replicate the customer's identity in the system, thereby fraudulently using the customer's identity to conduct transactions	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.	Clearly publishing the fee structure to the client, as well as consistent agent branding. Agents should assist the MM providers 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.	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

Risk Name	Risk Description	Recommendations to address risks
		event of uncertainty.
Transaction replay by the network	MNO's often have retried 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.	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. 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 outag	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 within this consortium could result in service unavailability to a client or to all clients.	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 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	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 position of not knowing whether or not the transaction has been delivered, and therefore whether or not to re-submit the transaction. The risk of incorrectly making the same payment more than once sure position after transaction submission.

Risk Name	Risk Description	Recommendations to address risks
		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	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 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 be temporarily or permanently unable to do so on account of the agent not having sufficient cash or electronic float to perform a transaction.	Agents need to be rolled out in conjunction with consumers, and 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.	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

Risk Name	Risk Description	Recommendations to address risks
		mitigate against recurrence. The agent needs to implement stringent customer detail management processes in its outlets.
Delays in balance updates by the service	Given the length of the chains of message handling within Mobile Money operations, balance updates may be delayed for any given transaction. This exposes the customer to future transactions possibly being incorrectly declined due to "insufficient funds" or to unexpected overdrafts if a withdrawal transaction is delayed.	All efforts must be made to shorten the message delivery paths through the network, and to give the priority over network components. MM platforms must be adequately scaled to support the customer numbers enrolled. The systems need to be designed with clear transaction commitment points that lead to balance updates. These should also support clear confirmation, failure and rollback mechanisms.
Receipt of counterfeit notes from customers	In most Mobile Money implementations, the agent cash in transaction takes the form of an exchange of cash for electronic float at the point of sale. If the client should successfully tender counterfeit funds in exchange for electronic float, the overall integrity of the system will not be compromised, but the agent will lose the corresponding amount of electronic float. This may result in the agents, their agent managers and any banks which supply cash management services to the Mobile Money operation, withdrawing their support for the Mobile Money operator	Training in the detection of counterfeit money linked to processes which ensure its application in transactions.
Burglary of cash float	Accepting cash in transactions at point of sale may increase the float size within a given retail outlet. This additional cash may	Stocks of cash need to be kept small enough to remain uninteresting to criminal gangs, while simultaneously

Risk Name	Risk Description	Recommendations to address risks
	increase the likelihood of burglary attempts at the point of sale. This may result in the agents withdrawing their support for the Mobile Money operator.	maintaining enough cash stock to cover the activity level in the agent.
Split transactions	In many Mobile Money implementations, proportionally risk adjusted AML procedures have been applied to extend the service to the un / under banked. These adjusted AML requirements are normally counterbalanced by transaction volume and value restrictions placed on the account. To circumvent these controls, the client may be tempted to split large transactions into several smaller ones which fit within the definition of the restrictions applied.	AML software should be deployed to check for clusters of transactions and to flag these up to the risk departments of the bank or MMO as suspicious. These are then managed by the risk department on an exception basis.
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 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.	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 making 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	If the teller miscounts the amount of cash deposited or withdrawn, the resultant shortfall / surplus will accrue to the agent	The tellers need to maintain vigilance.

Risk Name	Risk Description	Recommendations to address risks
out operations	This may result in the agents withdrawing their support for the Mobile Money operator.	
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.	The MM operator needs to ensure that the system overall grows at a suitable pace.
Too many short term deposits	Mobile Money operations can grow very quickly, attracting substantial, but short-term deposits.	Diversify the product, to add savings deposits capabilities, as well as short term lending.
Insolvency of the underlying float provider	A typical MM product is a "deposit and pay" service, meaning that the customer has deposited funds into the system. These funds are typically held by a licensed bank. It is possible that the underlying bank could face financial difficulties, placing the customer deposit at risk.	Credit Regulators need to watch the capital adequacy of the float holders carefully as mobile money has the potential to create concentration risks within the economy. Diversification of deposits into multiple banks is an effective mitigant. Mobile Money operators need to partner with responsible banks to ensure that the float will be managed appropriately.
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. Any significant relationship difficulty within this consortium could result in service unavailability to a client or to all clients.	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 remain committed to the product.
Lack of clarity as to who holds	Mobile Money products are often offered under another brand (such as that of an MNO) and the client may not be aware of the	All marketing communications with the client should clearly explain to them who the bank of last resort in the system really

Risk Name	Risk Description	Recommendations to address risks
customer money	licensed financial entity which actually holds his / her funds. This could make enforcing rights more complicated for the client.	is. This enables the customer to access consumer protection capabilities within the country.
Keystroke errors	Keystroke errors could result in the client paying incorrect beneficiaries or paying an incorrect amount, or both.	In many Mobile Money applications, the customer telephone number is used as the primary identifier of the customer. Adding and processing a check digit into the customer mobile number to make the account number decreases the likelihood of an incorrectly captured number being accepted as a beneficiary number. The Mobile Money operation needs to provide customer with a redress process in the event of incorrect beneficiary data capture.
Fraudulent use of mobile number	Mobile numbers are aliases for the customer IMSEI within the GSM networks. These can therefore be re-appropriated within the network, or the number can be appropriated in the street via handset or SIM card theft.	PIN security is key for managing this risk. To prevent network centered replay, encryption of the pin, to a higher standard than the GSM native encryption, within any SMS messages is also recommended.
Fraudulent use of customer details to establish a loan	Agents acting alone or in collaboration with external entities may use fraudulent customer details to secure a loan	The bank should only lend to customers with a stable transaction history with the Mobile Money operation. The bank should validate the data provided by the agents via credit scoring agencies and by direct contact with the customer.
Reduction in level of relationship between the bank	On account of the complex branding and distribution structure, the client may have no relationship with the lender, and may therefore feel a diminished obligation to repay loans granted to	The lender needs to closely monitor repayment patterns and respond quickly to unexpected behavior by the client

Risk Name	Risk Description	Recommendations to address risks
and the customer	him / her.	
Improper verification of KYC information during account registration	Agents are typically reimbursed for their activities via commissions paid for new accounts opened. This may make them less diligent in checking the customer's KYC information while registering a new customer account.	Depending on the regulation customer accounts can be opened with limited services until KYC identification can be confirmed. The operator can leverage databases to confirm ID matches and official black list reports to reduce the risk of fraudulent and criminal accounts. Education of agents is critical to quality, as is delayed commission payments, agent irregularity reporting and commission claw back rules that reduce this risk In the case of remittance transactions, the value of remittance transactions originated via OTC channels should be kept low enough to prevent systemic and money laundering damage. The Bank under whose auspices the transactions are conducted should conduct spot checks on the transactions submitted as well as tracking behavior of the agents. Ongoing agent training is essential
Improper data capture by agents during OTC remittance transactions	Data capture errors made by the agent may result in misdirected remittance transactions	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 prior to cash out.

Risk Name	Risk Description	Recommendations to address risks
System and Bank Pool Account Variances	The funds under management in a 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 (3rd 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	Mobile money system integration 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 personnel