Mobile Financial Services Risk Matrix

Developed in partnership between

Kenya School of Monetary Studies, Nairobi, Kenya

United States Agency for International Development, Washington, DC, USA

Booz | Allen | Hamilton, McLean, VA, USA

July 23, 2010

This document hopefully contributes some clarity to the systemic and consumer risks involved in mobile financial services and the options most commonly available for addressing those risks. The authors welcome feed back on errors or omissions that could materially improve the usefulness of this document in policy discussions.

The risks and response options identified in this Matrix do not represent the official position of the KSMS, USAID, BAH or any of those who have generously contributed their time and expertise to this project.

USAID
FROM THE AMERICAN PEOPLE

Mobile Financial Services Risk Matrix

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 countries such as the Philippines, Brazil, India, and Kenya has demonstrated that the technology is mature and brings real benefits to people who previously could not access financial products or services.

The Consultative Group to Assist the Poor (CGAP) has recognized this development with their seminal work on the impact that this technology is having on access to finance for the poor and in their Branchless Banking Diagnostic Template.

On September 25, 2009, the G-20 Leaders committed to improving access to financial services for the poor and directed the establishment of a G-20 Financial Inclusion Experts Group (FIEG) to support the safe and sound spread of new modes of financial service delivery capable of reaching the poor. The FIEG is identifying lessons learned on innovative approaches to providing financial services to these groups; promoting successful regulatory and policy approaches; and elaborating standards on financial access, financial literacy, and consumer protection.

Seminal work has been done in this area in Africa by the Central Bank of Kenya, which authorized Vodafone/Safaricom to introduce the M-PESA mobile payment system, with startling results. Some 25 percent of the population of Kenya is now using the service to make over 24 million transactions by May of 2010. The logic was that using a cell phone system to transmit and receive domestic remittances was a lower risk for the general population than the previous options available to make informal transfers back to villages. This service has just been expanded to include savings, loans and insurance in collaboration with Equity Bank. The explosive growth of use of mobile money has had the unintended benefit of increasing public involvement in the formal financial system, including expansion of savings accounts in the regulated financial intermediaries. However, it has also converted widely distributed consumer risk into a concentrated systemic risk, where the value of the items in transit on deposit through trustee accounts is no longer insignificant.

But this is not only an issue for Kenya (one that is being actively addressed) but is of concern to regulators in many other countries that are responsible for balancing the assurance of an enabling environment that is conducive to innovation and economic development against consumer protection concerns. Given that there is no common standard for the enabling environment, different regulators have responded in different ways, leading to a proliferation of inconsistent operating environments for account providers, and in some cases, limitations on the range of services that can be provided based on factors other than the underlying risks. This lack of consistency was lamented at the February 2009 Mobile World Congress in Barcelona.

The United States Agency for International Development felt that it could play a catalytic role in helping to harmonize legal and regulatory environments for mobile financial services through partnering with one of the leading international consulting firms, Booz Allen Hamilton, to undertake a detailed analysis of the various risks involved in the different models of mobile financial services, as viewed from each of the key stakeholders involved in these transactions. The research was undertaken in collaboration with the Kenya School of Monetary Studies, the policy research and training arm of the Central Bank of Kenya, and involved discussions with stakeholders in Ghana, Kenya, Malawi, Nigeria, Rwanda, South Africa, Tanzania, Uganda, and Zambia as well as with CGAP, the U.S. Treasury, the U.S. Federal Reserve in Atlanta, and the GSM Association.

The analysis produced consists of three parts: 1) the Mobile Financial Services Risk Matrix, 2) transaction flow mapping of some of the key transactions to show where these risks occur, and how these may differ depending on the service model, and 3)

an analysis of how various jurisdictions have already responded to these risks, based on analysis provided by CGAP.

This analysis is not intended to be all inclusive or prescriptive. Indeed, this would not have been possible since the topic of mobile banking is a rapidly evolving issue. Moreover, the flow charts are representative, since each account provider will have its own business model. And the options found for each risk are not necessarily mutually exclusive, since more than one policy option may be appropriate.

USAID sees this matrix as a living document that will undergo modification as our collective understanding of the risk factors and responses to these risk factors continues to develop. We invite you to participate in this process by reviewing this document and providing us with any material feedback that you believe would improve its contribution to the development of a sound, balanced regulatory framework for mobile financial services.

Comments/suggestions should be sent to Mr. Jeffrey Jackson, Senior Private Sector Advisor, USAID at jejackson@usaid.gov.

Mobile Financial Services Model Definitions

1. Bank Model: In a pure bank model the bank (or other formal deposit taking institution) holds the license. Each client is required to have an established account with the bank. The service provides mobile access to normal banking services, such as balance inquiry, transfers between accounts, and payments. Access can be through the Internet or through a cell phone based system where the cell phone company provides a menu based communications services in partnership with a bank, but is not involved in any underlying financial transactions, all of which pass through the client's bank account and for which the bank assumes responsibility. This service provides convenience to existing bank clients and to the bank itself by enabling some routine transactions to be done without visiting a bank branch, which saves time and costs for both the client and for the bank while enabling bank branches to serve a larger number of clients due to the reduced branch traffic. All cash in and cash out transactions require access to a bank branch or ATM.

Banks may expand access through use of agents to represent the bank for account opening and cash in or out services. Transactions initiated through the bank's agents are relayed back to the bank and pass over the client's account, and the bank assumes responsibility for the actions of its agents.

2. MNO (Mobile Network Operator) Model: A pure cell phone company (MNO) service extends the wireless network messaging functionality to provide payment services that enable customers to remit funds to each other that can be settled through the MNO's established agent network. Individual payment transactions occur entirely within the MNO and do not require the service user to have a bank account. The funds in transit - paid in by the remitter but not yet withdrawn by the recipient, are in principle on deposit in a segregated account with one or more banks (trust account if under common law), so are within the formal financial system. Since the service provider is only executing client payment instructions and is not performing the credit evaluation and risk management function of a bank, these services arguably do not constitute "banking" and do not require the level of regulatory oversight needed for deposits that are used to fund lending. The depository bank has no involvement in or responsibility for payments through the MNO system. Given the relatively high cost of a bank account (minimum balance, service charges, full KYC requirements, and travel time to a branch) and the easy, low cost and increasingly universal access to cell phone services, the MNO model arguably is highly effective in brining informal cash transactions into a form of formal financial system, expanding access to financial services.

3. Hybrid Model: A combination of a bank, MNO or other third party that offers communications and financial transaction services that combine characteristics of both the pure bank and pure MNO models. Such combination hybrid models include but are not limited to:

- MNO/Bank Model: Cell phone company based payment services that handle payments internally with cash in/out through the MNO's agent network, yet link to formal banking services such as savings, loans and insurance in partnership with a regulated financial institution by enabling communications with the bank and transfers between the user's cell phone payment account and accounts at the bank. Most mobile financial services are hybrid, drawing on the relative strengths of the partners involved.
- Government Provider/Bank Model: A government sponsored interbank clearing system includes consumer access functionality, either using smart cards or smart cell phone Sims that temporarily act as a store of value and synchronize with a formal bank account. The cell phone company, if involved, provides communications services while the government operates the payment switch between banks and between accounts within banks.

Risk Definitions

1. 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 worse case scenario, a "run" on the system

2. 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

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

4. Legal: A risk which could result in unforeseeable lawsuits, judgment or contracts that could disrupt or affect MFS business practices

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

6. International: A systemic risk (as defined above) that could have cross-border contagion effect

TABLE OF CONTENTS

Part I - Risk Matrix
1. Consumers 4
2. Merchants 22
3. Agents 24
4. Account Providers 30
5. Trust Account Holding Financial Institutions 40
6. Payment Systems 42
7. National Regulators 43
8. International Regulatory Issues 61

Part II – Sample Transaction Flow Charts 64

Part III - Risk Response Details 77

Bibliography 175

Contributors 189

Mobile Financial Services Risk Matrix: Consumers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
1.1	Potential customers cannot access mobile payment services due to inability to prove his/her identity.	When initially registering for mobile financial services (MFS), the inability of the account provider or its agents to adequately verify the identity and personal information of applicants may block approval or access to mobile payment services.	Know Your Customer (KYC)/Customer Due Diligence (CDD) guidelines to be set commensurate with the risk of the service. Subject to regulatory approval and verification of implementation.	1.National ID system: Authorities issue universal IDs, which are used for access to financial services	• Universality removes potential for exclusion of those desiring service. • Burden on national authorities to institute universal ID program may be unaffordable or beyond the existing infrastructure's legal, technical or political capacity to enforce.			X	X		X	X	X	X
				2. Financial ID system: In the absence of universal ID, financial account providers (as a consortia) offer a financial ID with similar characteristics as a universal ID, but only issued to customers after meeting standard sector KYC requirements (e.g. a customer's phone # and SIM could be used as basic form of identification) Could link in with an industry ID system established for ensuring certainty of identity in credit bureaus, or with a tax ID system.	• With no universal national ID, the financial sector must rely on other forms of identity, which all customers may not have access to; however, they can set risk-based tiers to ensure access. • Coordination of various private actors in the financial sector could work through the bankers association and/or MFI association, possibly with leadership from the central bank.									
				3. Regulated KYC Requirements which leave implementation to institutions	• Each institution can interpret the requirements, which may allow various combinations of identification. Banks can set risk-based tiers to ensure access. • Each individual bank must establish a policy that meets regulatory requirement. • Reliance on existing forms of identification keeps cost low, but difference in policies across institutions creates some risk									

Mobile Financial Services Risk Matrix: Consumers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
				4. No regulatory KYC requirements	• Each institution will determine requirements for account opening based on their perception of risk. Lack of regulatory requirement should keep barriers to access low. • Lack of requirement opens cross-organization risk for criminal activity.									
1.2	Existing customer cannot access mobile payment services due to inability to prove his/her identity.	Verifying identity and personal information to protect customers when using mobile payment services may block access if the customer is not able to adequately prove his/her identity.	Transaction size and KYC/CDD levels commensurate with the user's ability to self identify through PIN, photo attached to the account, national ID or biometric ID system. Easily accessible process for replacing lost SIM or PIN. Subject to regulatory approval and verification of implementation.	1. Restrict access to mobile financial services to those who can meet the same KYC requirement as account opening	• Requiring that agents repeat the same KYC requirements at the transaction level that are required at account opening is not practical. It would place an enormous time requirement on agents, and should not be necessary if the account opening procedure is implemented. (This would be the equivalent of requiring a photo ID check at the ATM.) • Regulatory authorities would not be able to effectively police such a requirement.			X	X		X	X	X	X
				2. Ensure that appropriate risk based service access requirements are established at account opening	• Strict KYC requirement for agent transactions will create inconveniences for customers and create more bureaucracy for agents. • Expecting agents to conduct this due diligence for transactions of existing customers, especially during busy times is impractical. • Risk-based allowances ensure customers still have some access even without full KYC; yet the limits protect against fraud. (Option									

Mobile Financial Services Risk Matrix: Consumers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
					enables customers who have lost their ID to maintain some access) • Lower requirements for small, or low risk, transactions reduce regulatory burden for agents									
				3. Require that funds transferred to recipients who do not have established KYC credentials are returned to sender	• Risks unwarranted returns if agents do not want to complete pay-outs for non-KYC reasons									
				4. Require that account providers have acceptable procedures in place for replacing PIN and other provider ID	• Balance protection of customers against theft of funds against inconvenience of denial of service for legitimate transactions									
1.3	Customer's identity is stolen and used to open a mobile payment account fraudulently.	The risk of stolen identity can have multiple ramifications, including: • Customer's identity could be used to access other services • Customer is held accountable for fraudulent transactions made in his/her name • Customer is unable to access mobile services because an account using his/her name/identity has already been established fraudulently.	Protect service users against results of identity theft Subject to regulatory approval and verification of implementation.	1. Biometric national ID, or financial ID, system with biometric validation required for account opening.	• Though biometric ID and validation reduces the possibility that a stolen ID could be used to fraudulently open an account in a customer's name, the cost of implementing such a program can be high. • Different biometric options have varying cost associated with them (e.g. voice tends to be less expensive as it can occur over the phone, whereas fingerprinting and retinal scans are more costly) • Biometric ID program may be beyond the technical capacity of a regulator to implement and maintain, as the infrastructure for capture and validation will require maintenance. • Costs will likely decline as the technology improves – in the interim other and possibly multiple forms of				X		X	X	X	X

Mobile Financial Services Risk Matrix: Consumers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
					ID may be required, such as birth certificates or passports where available.									
				2. Account providers provide an effective process for alerting users of unusual activity, and blocking accounts when notified of fraudulent activity.	• Requiring a rapid alert system to advise users that their accounts may be compromised and block procedure to stop fraudulent activity once recognized is a simple and pragmatic way to deal with stolen identity. • The procedure can be easily validated by regulators.									
				3. Develop of best practices for enhancement of fraud detection systems. Provider reports suspicious or fraudulent activity to central authorities (Central Bank/Financial Intelligence Unit or FIU).	• KYC mechanisms, which could include point-based multiple ID requirement, limits potential for fraudulent account opening. • Reporting helps target systemic fraud, thus reducing risk. • Enforcement mechanisms for reported illicit activity may not exist or may be weak. Creating or enhancing such mechanisms will require investment.									
				4. With adequate account opening protections, including adoption of policies above, providers can limit the liability of fraudulent activity in account agreement. Periodic account validation would protect the integrity of these protections.	• Consumer protections embedded in contracts will reduce barriers to adoption, and should not be terribly costly with adequate fraud controls. • Contract enforcement could be required to ensure customer protection which would require an effective court system.									

Mobile Financial Services Risk Matrix: Consumers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
				5. No regulatory KYC/CDD requirements or provider-based consumer protection against fraudulent account opening.	• Lack of KYC/CDD requirements open financial system to fraud risk, whether through ID theft or ID fraud. • Lack of protection represents a potential cost for consumers and thus a barrier to entry.									
1.4	Customer's account security credentials and / or account information and transaction history are improperly released (e.g., PIN biometrics, and stolen phone/subscriber identity module [SIM]).	If a customer's account credentials, account information and transaction history are not adequately protected, the customer's account can be illegally accessed to steal funds or to process illicit activities. Customers may also be subject to identity theft or blackmail. Some models, particularly the hybrid, may share customer data as a means to mitigate fraud by enabling a clear audit trail of the financial transaction.	Account providers maintain a rapid account block process for customers if customer/MNO believes the account has been compromised. Development of best practices for enhancement of fraud detection systems. MNOs mitigate risk of unauthorized/ inappropriate access to customer transaction data. To mitigate the risk of customer account credentials, information, and transaction history being compromised, implement best practices for data security maintenance, including data sharing between service providers and other business entities. Subject to regulatory review and verification of implementation.	1. Strong privacy legislation / regulation requires institutions to institute controls to reduce the likelihood for unauthorized release, or theft, of personal information.	• Regulatory requirement reduces likelihood for improper release. Standard requirements for all institutions limit criminal targeting of weak institution policies. • Burden on national authorities to institute and enforce; may be unaffordable or beyond the existing infrastructure's legal, technical or political capacity, or authority, to implement and enforce. • Requirement will impose a cost on providers.		X	X	X		X	X	X	X
				2. Provider led controls instituted to mitigate the likelihood of unauthorized release or theft of customer information.	• Institutional policies reduce likelihood for improper release. Lack of standard requirements for all institutions allows for criminal targeting of institutions with weaker policies. • Institutional programs will impose a cost on providers; however, lack of a regulatory requirement allows institutions to determine the level of mitigation.									
				3. Providers institute a "disaster plan" to	• Can result in denial of access to									

Mobile Financial Services Risk Matrix: Consumers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
				notify customers impacted by breach, Plan could include procedures to block transactions on all impacted accounts and to issue new credentials to customers.	services, resulting in hardship for funds recipients until problem resolved. • Quick action can limit operational, systemic, and reputation risk.									
				4. No formal regulatory requirement or provider policies for customer protection or disaster recovery plan	• Lack of policy raises the systemic fraud risk. • Ineffective response to a breach of privacy could undermine public confidence in the financial system and its regulators.									
1.5	Customer is unable to efficiently dispute a transaction or account charge.	Customers are not able to resolve disputes with an account provider and recourse to a government body or regulatory authority to arbitrate disputes is weak or non-existent. Note: The dispute requiring resolution could be a transaction that is initiated by a customer on the customer's phone, as well as a transaction that an agent makes on behalf of a customer who does not have his/her own phone.	MNOs provide an efficient dispute resolution process. Clear, published service standards to minimize the cause of disputes. Regulatory domain able to define consumer protection for error resolution, in terms of responsibilities, time frames, and liabilities. Subject to regulatory review and verification of implementation.	1. Regulatory oversight authority refers disputes back to the account provider but verifies account provider dispute resolution process.	• Licensing authority needs to set an "acceptable level of disputes" above which continuation of the account provider's license may be put in question. • Implies regulatory monitoring of the account provider's error resolution program, not just complaints. • Regulatory authority may not have capacity to handle complaints of disputes		X		X		X	X	X	X
				2. Association of providers, or NGO, provides dispute resolution process.	• Association ownership could be perceived as biased toward providers, but less biased than a provider run system. An NGO focused on consumer protection could be preferable. • Allowing other providers in the association (or NGOs with other motivations) to interact with customers could create provider									

Mobile Financial Services Risk Matrix: Consumers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
					animosity • Association may not have capacity to support, or the budget to develop, this function.									
				3. Individual providers provide dispute resolution process	• Provider management could be biased toward provider; however, competition should enhance customer position.									
				4. Independent alternative dispute resolution (ADR) function developed to handle appeals to other processes.	• Existence of an independent ADR function provides consumer protection against industry bias in other processes.									
				5. No dispute resolution process	• Lack of consumer protection raises cost for consumers, thus creating a barrier to adoption. • The only incentive for resolving customer disputes will be customer retention and reputation, which will be stronger in competitive environments, and environments with an active business press corps.									
1.6	Customer is charged unauthorized fees by agent.	Agent may overcharge or have a side transaction fee that is not authorized that they impose on the consumer. Customers may not understand the complexity of the contract signed, making it possible for him/her to face additional fees/services without being aware	Account providers use clear contracts that fully disclose all fees to be charged, tailored for various customer situations, including different languages and illiteracy (i.e. pictogram-based contracts). Service charges clearly posted at each agent's location. Disclosures reasonably comprehendible to all	1. Regulatory authority requires full disclosure of all fees in account agreement.	• Full disclosure of all fees limits potential for consumer exploitation by providers. • Regulators may lack the capacity/budget to monitor and enforce the requirement, especially considering the abuse is more likely to happen at the agent level than the corporate level.			X	X		X	X	X	X

Mobile Financial Services Risk Matrix: Consumers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		of it. The lack of clarity of contract could be further exacerbated by language barriers or illiteracy. Additional government charges, such as VAT, may complicate the disclosure of true costs and tariffs.	customer groups (i.e. major language disclosures and potentially pictograms) Subject to regulatory review and verification of implementation.	2. Account providers required to ensure fee structure is posted in all service locations in a format understandable to the broad population. (i.e. major language disclosures and potentially pictograms) Account providers required to discipline or expel consistently non-compliant agents.	• Account provider disclosure mitigates potential for consumer exploitation, • Account providers may have difficulty ensuring reasonable compliance throughout their agent network.									
				3. No fee disclosure policy	• Account providers may not fully disclose fees, and/or agents may violate terms of service, undermining public satisfaction with the service, potentially resulting in complaints to the regulator.									
1.7	Customer cannot access cash from mobile money account due to lack of agent availability.	Insufficient numbers/availability of mobile money and/or bank correspondent agents in a given geography results in consumers not being able to access cash or incurring excessive travel costs and inconvenience.	Providers responsible for market coverage No unreasonable regulatory constraints on expansion of agent networks	1. Regulatory authority mandates minimal geographic coverage as part of financial access/inclusion interests.	• Requirement raises the cost for account providers so that the service may not be profitable. Also, the requirement raises barriers to entry for smaller players. • Account providers may agree to collaborate in areas where population density does not justify multiple service access points.			X	X	X		X	X	X
				2. Regulatory authority mandates community reinvestment by account providers to extend agent coverage	• Coverage would improve in rural areas • Requirement is a cost for providers; however, it has positive reputation benefits and could be scaled based on network size.									

Mobile Financial Services Risk Matrix: Consumers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
				3. Regulatory authority requires disclosure of agent network coverage in service-level agreements (SLAs)	• Customer expectations are set at account opening. • Cost of compliance is low for providers and the cost of oversight is minimal. • Agent network will expand with market demand.									
				4. Regulatory authority allows account providers to appoint agents at their discretion, but with registration at the regulatory authority and subject to inspection as deemed necessary.	• Allowing account providers to determine the type and distribution of its agent network maximizes market efficiency. • The registration of agents and potential to inspect them provides the regulatory authority with a degree of oversight. • Agent network will expand with market demand.									
				5. Treat as internal account provider issue - no regulatory oversight of extent of agent network or required disclosure.	• Customer expectations may not be reasonable due to lack of transparency regarding network coverage and SLAs. Customer complaints may rise. • The reputation of the service may suffer. • Agent network will expand with market demand.									
1.8	Agent unwilling to perform transaction for customer.	The agent may be unwilling to perform a transaction because of liquidity management concerns. Agent may wish to conserve cash by restricting large transactions	Adoption of payment services best practices including optimization of agent and super-agent compensation models for cash distribution, cash pick up, and deposits.	1. Regulatory authority establishes anti-discriminatory policies with verification of compliance.	• Motivates account providers to encourage agents to serve the "customer in front of them" • Regulatory authority may lack capacity and/or authority for			X	X		X	X	X	X

Mobile Financial Services Risk Matrix: Consumers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		to more profitably service a larger number of smaller transactions. Agent is unwilling to serve customer due to discrimination (race, tribe, religion, sex, etc). Agent is instructed by super agent not to perform transactions during specific hours of the day due to cash pickup and deposit burdens.	Standards for agents barring discriminatory practices, with regulatory review and verification of compliance.		consumer protection oversight; Discrimination complaints are the task of other agencies									
				2. Regulatory authority provides oversight to ensure agents and other service providers perform transactions in compliance with account agreements.	• Regulatory authority may lack the capacity to perform this role with sufficient credibility to deter abuse.									
				3. Account providers set institutional anti-discrimination policies and monitor agent behavior/compliance	• Institutional policies mitigate discrimination likelihood by setting up a disincentive for agents. • Providers may be more reactive in preventing discrimination if there is no regulatory cost. • Providers may lack the capacity to monitor and enforce policy.									
				4. No regulatory requirement or provider policies requiring agents to complete transactions	• Relies on existing general anti-discrimination statutes and practices.									
1.9 **Refer to 4.7**	Customer cannot access cash from mobile money account due to lack of agent liquidity	Customer cannot perform cash-out transaction because the agent does not have sufficient cash on hand to perform the transaction. Agent may be experiencing unusually high cash-out requests due to special events, including public events, public disturbances, or loss of public confidence. Super agents providing physical cash distribution to individual agents are not able to manage cash stocks effectively.	Account providers are responsible to customers for providing cash-out services in a timely manner, including contingency plans to deal with liquidity crises, Subject to regulatory review and verification of implementation.	1. Monitor complaints of unavailability of cash - factor the level of instances into license extension discussions/decisions.	• Forecasting and management capabilities are similar for ATM and Branch cash forecasting/ management. • Only a regulatory issue if account provider performance egregious - impact on license extension. • Account providers face a reputation risk if they cannot manage liquidity well.		X		X	X	X	X		X
				2. Account providers forecast and manage liquidity of agent network to	• Requirement ensures customers access to cash within a reasonable									

Mobile Financial Services Risk Matrix: Consumers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
				optimize service for consumers.	amount of time. • Forecasting and management capabilities are similar for ATM and Branch cash forecasting/ management. • Market forces will improve liquidity management over time as providers keep reliable agents, take on some agent responsibilities, or partner with other institutions as agents of last resort.									
1.10	Customer cannot access cash from mobile money account due to lack of personal access.	Customer cannot receive cash from agent or perform cash-out transaction during regular "business hours" due to one of the following situations: • Customer has exhausted his/her pre-paid minutes. • Customer's cell phone battery is dead. • Customer has lost his/her cell phone.	Customer's responsibilities and process for regaining access to cash spelled out in contracts and in account provider's operating procedures. Simple remedies to each situation spelled out and available to users.	1. Provider ensures alternative access procedures in the event of customer notification of access failure; terms and conditions of each party's responsibilities outlined in account agreement.	• Customers responsible for maintaining their access. But failure to resolve access problems could undermine public acceptance by increasing the user's risk.		X	X	X			X	X	X
				2. No alternative access measures exist	• Customer must pursue through dispute resolution if they can not reestablish connectivity.									
1.11	Customer cannot access cash from mobile money account due to lack of system availability.	Customer cannot receive cash from agent or perform cash-out transaction during regular "business hours" because of one of the following situations: • Cell phone service is not available in that location. • The account provider is experiencing a temporary	Providers are responsible to customers for providing cash-out services in a timely manner. Account providers post realistic access standards and area coverage to ensure appropriate client service expectations. Subject to regulatory review and verification of compliance.	1. Regulatory authority requires system availability service levels. Business continuity plans must be clearly stipulated in terms and conditions of customer agreements. Significant complaint levels will impact license extension.	• Required service levels and continuity plans mitigate system availability risk. • High system availability requirement will impose a cost to some providers and raise a barrier to entry for potential providers. • Regulatory authority capacity/authority to regulate and enforce system availability may not	X	X	X	X	X	X	X	X	X

Mobile Financial Services Risk Matrix: Consumers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		system outage. A record of complaints may indicate questionable business practices, or a lack of complaints could mean there is no established avenue for consumer remediation. Unscrupulous businesses or business may change names and locations to hide complaint histories once the business ceases operations.			be practical. (Whether the regulatory authority in this situation is financial or telecommunication is debatable.)									
				2. Regulatory authority establishes a comprehensive licensing and registration process for service providers to mitigate risk exposure from migration of weak business practices.	• Requires careful balancing of the enabling environment to prevent bad practices while not inhibiting market entry of new players and innovation. • Risk of stifling initiative through over regulation.									
				3. Regulatory authority monitors system availability service levels. Significant complaint levels could impact license extension.	• Any new market entrant is likely to take time to fully roll out its service, particularly if competition is entrenched. Failure to do so within a reasonable time could lead to failure of the service, resulting in the regulator having to ensure an orderly withdrawal. • Regulatory capacity to monitor system availability may be limited. • Lack of a regulatory requirement keeps barriers to entry low, relative to this issue.									
				4. No system availability requirement by regulators or commitment by providers	• Adoption rates will be low if customers cannot depend on system availability.									
1.12 **Refer to 5.13**	Lack of network interoperability prevents consumer from transacting with desired party.	Closed loop networks with no capability to transfer funds between account holders of different account providers' payment networks due to lack of interoperability. Among	No protectionist barriers to transfer funds between systems. Intra- account provider transfers conducted within the account provider's system.	1. National regulators require interoperability of payment networks (through inter-account provider links or through a switch)	• Requirement of interoperability may raise a barrier to entry as the technology requirements could be more challenging than a simple closed network. Further, the requirement may stifle innovation in			X			X	X	X	X

Mobile Financial Services Risk Matrix: Consumers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		providers or their non-participation on a national payment platform block payments outside of the account provider's network. The first player to enter the market can gain monopoly power, limiting competition, but can help justify initial market entry into virgin markets.	Inter-account provider transfers conducted through a national switch, either directly or through correspondent clearing accounts, without unreasonable usage fees or penalties.		a new technology through keeping new entrants out. • Consumers might benefit as there would be no network limitations on sending mobile money. • Account providers might be forced to compete on cost, products, and service, rather than size of network. • Limits first mover advantage, potentially discouraging initial market entry.									
				2. Competition agency empowered to investigate non-competitive behavior	• Requires a competition agency with the capacity to investigate and enforce non-competitive behavior, such as predatory pricing.									
				3. No regulatory action	• Predatory pricing and expanded monopoly power are possible; however, experience with networked technologies (cell phones/ATMs) suggests that the market will move toward interoperability without regulatory action.									
1.13	Customer loses balance due to failure of a bank holding trust fund, or a similar situation where trust fund is compromised.	Trustee impaired: Should the trustee fail or become insolvent, trust accounts that are not legally segregated from the general pool of bank assets available to satisfy creditors may be pulled into the bankruptcy process, with access blocked. The trust account may be	Trust funds holding the value of items in transit are legally segregated from the trustee's own assets in bankruptcy. Trust accounts are divisible (to spread risk) and transferable (in case of failure of the trustee to perform). Management and investment of trust funds regulated similarly to insurance	1. Law / Regulation relating to bank failure or insolvency segregates assets held in trust accounts from the general pool of assets of a trustee in the bankruptcy process.	• Requires trust law - normal in common law systems but typically difficult in statute law systems. • Requires a court system that both understands trust law and is empowered to enforce it.		X	X	X	X	X	X	X	X
				2. Law / Regulation on trust funds that provides for:	• Diversification of trust accounts spreads risk across multiple financial									

Mobile Financial Services Risk Matrix: Consumers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		technically segregated, but no rapid procedure for transferring funds held in trust to another trustee may exist, preventing access to the funds	company loss reserves to limit risk of impairment of value.	• Transferability of the trust to another trustee in case of non-performance or failure of the trustee. • Investment guidelines for trust funds that limit risk concentrations for funds not invested in marketable or short maturity government securities. • Clear segregation of trust funds covering customer funds from the operating funds of the account provider. • Periodic regulatory verification of the adequacy of trust funds	institutions thus reducing the exposure of providers. Holding across multiple institutions will create a bit more complexity for payment providers in managing several bank relationships. • Monitoring and enforcement of trust account diversification should be possible through periodic reporting.								
				3. No regulatory action	• Deficiencies in the trust account, if leading to the inability of an account provider to cash out for clients, could have systemic impact through weakening of public confidence in the financial system.									
1.14	Pooled deposits within a trust account can create a funding concentration risk which would not protect individual customers if trust is impaired.	Trust impaired: Trust funds deposited by the trustee in an account with the trustee bank or other banks are pooled deposits that may be significant compared to the size of the bank, representing a funding concentration risk, and may not be fully protected under bank closing/insolvency/ deposit insurance rules. • Even if available, deposit insurance is at the account level, and if the trust account is	Trust funds holding the value of items in transit are legally segregated from the trustee's own assets in bankruptcy. Trust accounts are divisible (to spread risk) and transferable (in case of failure of the trustee to perform). Trust fund investment policy to provide liquidity for cash-out needs and to protect against impairment of value.	1. Law / Regulation relating to bank failure or insolvency segregates assets held in trust accounts from the general pool of assets of a trustee in the bankruptcy process.	• Requires trust law - normal in common law systems but typically difficult in statute law systems. • Requires a court system that both understands trust law and is empowered to enforce it.		X	X	X	X	X	X	X	X
				2. Law / Regulation on trust funds that provides for: • Transferability of the trust to another trustee in case of non-performance or failure of the trustee. • Investment guidelines for trust funds that limit risk concentrations for funds	• Diversification of trust accounts spreads risk across multiple financial institutions thus reducing the exposure of providers. Adds complexity for payment providers in managing several bank relationships. • Monitoring and enforcement of trust									

Mobile Financial Services Risk Matrix: Consumers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		viewed as a single account, rather than many, the cap would be insignificant compared to the size of the trust account. • The value of trust funds invested in other financial instruments or institutions may be impaired by a decline in market value of the investments. • Significant and unusual outflows could present the trust with liquidity difficulties if investments cannot be unwound.		not invested in marketable or short maturity government securities. • Clear segregation of trust funds covering customer funds from the operating funds of the account provider. • Periodic regulatory verification of the adequacy of trust funds	account diversification should be possible through periodic reporting. • Excessive risk concentrations in a trust fund could heighten systemic vulnerability should a loss of public confidence in the account provider result in disintermediation with consequent demand to liquidate investments by the trust.									
				3. No regulatory action	• Deficiencies in the trust account, if leading to the inability of an account provider to cash out for clients, could have systemic impact through weakening of public confidence in the financial system.									
1.15	Customer loses balance due to bank/provider not maintaining a 1:1 coverage requirement in the payment account trust fund.	If the financial services provider or bank holding the trust fund does not maintain a balance equal to the total value of all payments in transit, the customer may not be able to recover his/her funds if the service were to be terminated. The risk is particularly severe if the account provider is experiencing operating losses or cash flow strains due to network expansion or other operating or investment costs and may see client funds in transit as a source of operating funding.	Prevent co-mingling of account provider company operating funds and customer funds in transit. The sum of the lower of cost or market value of trust funds in account provider trust accounts must at least fully cover the value of all transfer items in transit or funds stored in mobile phone accounts that are defined as funds paid in by customers into payment accounts and not yet withdrawn. Subject to regulatory supervision (this is probably the dominant systemic risk issue).	1. 1:1 trust account balance requirement.	• Requires periodic reporting by banks/providers to regulators. • Reporting requirements Regulators will need the capacity to effectively monitor and verify reports.		X		X		X	X	X	X
				2. No regulatory action	• Failure to ensure that items in transit are fully covered by corresponding funds held in trust could result in a messy winding up of a failed account provider, with systemic impact on financial markets.									
1.16	Consumers may respond to social pressures by drawing	Increasing the ease with which funds may be transferred to	Public awareness of the risks of over indebtedness.	1. Regulatory authority prohibits use of credit facilities for funding mobile money	• Not implementable since money is fungible.	X				X	X	X	X	X

Mobile Financial Services Risk Matrix: Consumers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	on credit lines to fund payments, risking over indebtedness.	family members may increase social pressures for such transfers, possibly leading remitters to tap credit lines to supplement payments. This may increase the risk of remitters increasing their debts to unsustainable levels.	Lender policies and procedures that protect against over indebtedness. This is a general (not cell phone specific) consumer protection and portfolio quality issue that should be already under regulatory oversight, although may not be in place in many countries.	accounts.	• Financial institutions will reject regulators limiting how credit facilities can be used on a situational basis.									
				2. Regulatory authority may provide general consumer protection guidelines for over indebtedness, but otherwise take no action	• Requires support from the on-site examination of regulated institutions' lending policies and procedures, as a normal part of market supervision.									
1.17	Customer's family is unable to access account funds if the customer dies.	If account providers have not established escheatment guidelines for customer mobile payment accounts in case of death, customer's families will be unable to access the balances and the account will remain dormant on the provider's system.	Escheatment guidelines to mimic the guidelines for demand deposits accounts. Subject to regulatory oversight and verification of compliance.	1. Regulatory authority mandates establishing beneficial owners for stored value fund balances payable on death of the owner	• Account opening complicated, increasing operating costs and potentially deterring usage. • Regulation implies enforcement capacity and costs.		X				X	X	X	X
				2. No regulation, but account providers establish beneficial owners for stored value fund balances in the event of death or incapacity of the owner	• Account opening complicated, increasing operating costs and potentially deterring usage.									
				3. Service users protect themselves by sharing access codes with trusted family member(s)	• Could result in miss-allocation of funds by overly trusted family member(s)									
				4. Institute "abandoned property" regulations that transfer unclaimed funds to the state after a prescribed period.	• Requires an accounting process for abandoned funds and may require a process for responding to claims received after the prescribed period.									
1.18	The beneficial owner(s) of stored value and transactional accounts (e.g., mobile money) cannot be determined by authorities in the event of illicit account	Single accounts opened in the name of a group or a member of a group for shared usage. For example an individual within a village establishes an account to be used to receive remittances	Responsibility for any transaction passing through a mobile account clearly defined.	1. Law / Regulation prohibits group registration for transactional accounts.	• The law cannot realistically prevent informal group use of accounts – individual associated with the SIM card bears responsibility for any issues. • Enforcement will focus on provider			X	X		X	X	X	X

Mobile Financial Services Risk Matrix: Consumers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	activity when group accounts are used	for anyone in the village, or a village based solidarity or small group lending program jointly opens a mobile money account, making regular deposits with an intention to "share out" funds to individual group members as micro-loans. As the account is associated with multiple individuals, authorities have difficulty identifying specific actor when illicit activity occurs. Use of shared accounts is not permitted under FATF due to AML/CFT concerns, since such accounts effectively permit anonymity of most of the beneficial owners of the account. The FATF framework generally requires the beneficial owner(s) of an account to be known to the financial institution so using one person to send/receive money on behalf of a community is not permitted.			policy and investigation when criminal activity is suspected – implies enforcement costs									
				2. Law / Regulation limits group registration for transactional accounts to corporate entities; enforced by account provider and or regulatory authorities	• Corporate restriction limits flexibility for micro-finance group accounts. • The law cannot prevent group use of accounts – individual associated with the SIM bears responsibility for any issues. • Enforcement will focus on provider policy and investigation when criminal activity is suspected – implies enforcement costs.									
				3. Law / Regulations permits group registration with designated "signatory" SIM authority acknowledged by all members in written agreement.	• Increases documentation requirements and transaction costs, motivating for avoidance. • Ability to identify which actor within the group made a given transaction would require collaboration from the "signatory".									
				4. No regulatory action	• Account providers determine group use policy. • SIM card holder held accountable for transactions over the account motivating the SIM card holder to block illicit transactions by shared users. • Regulatory authority's ability to identify members of a group and which member of an informal group is the source/beneficiary of an illicit									

Mobile Financial Services Risk Matrix: Consumers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
					transaction will depend on collaboration by the SIM card holder whose account was used.									
1.19	Government decides to tax transactions to raise funds increasing the marginal cost of each transaction.	Governments in need of revenues may see the high transaction volume mobile payment system as an opportunity. If governments decide to institute a transaction tax on mobile payment system transactions, they would raise the marginal cost of each transaction to consumers (as account providers would pass this cost along), thus pricing out many of the consumers that the system most benefits. The high adoption rate of mobile payments in most communities, and the benefits for expanding access to financial services, are driven largely by the low cost.	Keep the marginal transaction cost to a minimum.	1. Government imposes a transaction tax	• Any transaction tax will reduce volume of the system. The consumers that leave the system will be the poorest, as they are the most price-sensitive. Thus, any transaction tax would be viewed by the public as anti-poor. • A transaction tax would complicate operations and accounting for account providers. • Some funds would inevitably be raised; but offset by the negative societal impact of decreased usage.		X					X	X	X
				2. Government does not impose a transaction tax.	• Mobile payment adoption rate, and expanded access to financial services, not inhibited by taxation.									

Mobile Financial Services Risk Matrix: Merchant

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
2.1	Merchants are unable to easily convert mobile money into cash, limiting their flexibility to run their business / store.	Merchants accepting mobile money may not be able to rely on regular, flexible, and consistent methods to exchange electronic money into cash or use electronic money to trade with their suppliers. If they take in mobile money, but their suppliers do not accept mobile money, their ability to restock efficiently may be limited. Merchants may refuse to accept mobile money in payment for goods and services if their ability to cash out is limited.	Merchants able to cash out as needed for liquidity management.	1. Regulatory authority requires account providers to maintain an "agent of last resort" within specific geographic areas to ensure liquidity for consumers.	• Such regulation likely unenforceable, since cannot dictate the composition of account providers' networks or related contracts. • It is in the interest of account providers to provide an efficient agent network to ensure market penetration, regulatory intervention is likely unnecessary.			X		X		X		X
				2. No regulatory action	• Merchants will adopt mobile payment capabilities into their business model when they can either use mobile money balances with suppliers, or when they can depend on agents to maintain liquidity. • It is in the interest of account providers to ensure an efficient agent network. Monitoring of complaints of inadequate access could feed into license considerations.									
2.2	Merchant could be restricted by a contract with an account provider from accepting payments for or from another account provider.	Merchants locked into exclusivity agreements may be precluded from offering their clients better and/or less costly services from other account providers. Exclusivity agreements may provide economic justification for market entry of the first provider, but then may perpetuate a monopoly.	Balanced exclusivity agreements that facilitate market entry economies of scale yet prevent unreasonable restrictions on competition.	1. Exclusivity agreements restricted by law or regulation to balance short term market entry facilitation against longer term market competition, possibly through time limitations.	• Allowing or not disallowing exclusivity agreements may encourage market entry, but then block longer term competition. • Blocking all exclusivity agreements could discourage first mover market entry. • Requires regulatory monitoring of account provider agreements with agents and associated regulatory costs.			X			X	X	X	X

Mobile Financial Services Risk Matrix: Merchant

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
				2. Regulatory authority requires interoperability of payment networks (through inter-provider links or switch)	• Requirement of interoperability would lessen the inconvenience of any exclusivity agreements with merchants as they would still be able to make a purchase, though a fee may be involved. • Requirement of interoperability would raise the cost for new entrants.									
				3. Competition agency empowered to investigate non-competitive behavior	• Requires a competition agency with the capacity to investigate and enforce non-competitive behavior. This is not a unique issue to mobile financial services. • Actions to restrict exclusivity agreements that harm consumers will discourage their use in mobile financial services too.									
				4. No regulatory action	• Exclusivity agreements are possible; however, experience with networked technologies (cell phones/ATMs) suggests that the market will move toward interoperability without regulatory action.									

Mobile Financial Services Risk Matrix: Agents

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
3.1	Agent is unable to easily liquidate e-money inventory when the agency relationship is terminated.	Agents that voluntarily or involuntarily lose their agent status must be able to convert their e-money inventory to cash or deposit in a bank account.	Cash out procedures are covered in the agency agreement. Contractual disputes between account provider and agents subject to court resolution.	1. Regulatory authority requires providers to facilitate agent cash-out upon termination.	• Requirement mitigates agent liquidity risk in case of termination. • Requirement removes a potential barrier for entry of new agents, if they are uncertain of the market or the account provider. • Enforcement may be limited to review of agent agreement templates.	X	X	X	X	X	X	X	X	X
				2. Provider sets contractual agent termination provisions with guidance from the regulatory authority.	• Provisions set expectation for agents upon contract initiation. (Provisions should enable liquidation within a timely manner.) • If provisions do not ensure a timely liquidation, this may constitute a barrier to entry for new agents.									
				3. No regulatory guidance	• Account provider has a commercial interest in enabling existing agents to exit: to reduce barriers to new agents. • Account provider sets own contractual obligations to liquidate agent's e-money inventory in a timely manner. • Agent may liquidate balances via other agents. • Lack of clear exit strategy at termination may constitute a barrier to entry for new agents.									
3.2	Agent receives cash from client but fails to	Agent receives funds from a service user but misdirects funds	Effectively constrain diversion of	1. Require that service users receive, and know they have a right to receive, clear	• Public confidence issue - in the account provider's interest to ensure			X	X		X	X	X	X

Mobile Financial Services Risk Matrix: Agents

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	provide/transfer the e-money	to the agent's own benefit. This situation could arise in one of two ways: The consumer could be an existing customer without their phone with them, so they would not receive the transaction confirmation while with the agent. The consumer may not be a customer but requests that the agent sends money to an existing customer, so does not receive independent phone confirmation of the transaction.	funds.	confirmation that funds have been received and where they have been directed. This may include a paper receipt, if the customer does not have a phone, or if the individual is not a customer.	that clients are not defrauded. • Police may need training on dealing with complaints of abuse. • Agents require protection from spurious claims of non-receipt.									
				2. Require that service users receive, and know they have a right to receive, clear confirmation that funds have been received and where they have been directed. This may include a paper receipt, if the customer does not have a phone, but would not apply to non-customers requesting 'informal remittance' service from an agent, (i.e. when the service is not formally offered by the provider).	• Public confidence issue - in the account provider's interest to ensure that clients are not defrauded. • Police may need training on dealing with complaints of abuse. • Agents require protection from spurious claims of non-receipt. • Non-customers receive no more protection in this situation, than if they asked any user on the network to provide the same service.									
				3. Require account providers establish a control environment that establishes some dual control feature or other mitigant to fraudulent practices by agents.	• In the account provider's own interest to protect its network and clients from fraud. • Implies regulatory review of account providers' control policies and procedures.									
				4. Raise public awareness that users should have their cell phone available to ensure receipt of transaction confirmations.	• Reduces the need for potentially costly and unenforceable rules to ensure agents are crediting the proper accounts.									
				5. No confirmation requirement	• Customers requesting cash-in or remittance service without their phone present are at risk of losing cash if the agent decides to misdirect									

Mobile Financial Services Risk Matrix: Agents

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
					the money, or not process the transaction.									
3.3	Agent is robbed.	Agents that hold both cash and e-money face a risk of robbery. The risk may be heightened if the volume of cash/e-money required follows a predictable remittance cycle, requiring a higher than normal cash on hand position. Agent may be forced to transfer all or part of its e-money inventory to the robber or other party. However, agents that are also merchants may find that accepting e-money as payment for goods and services sold reduces the need of cash on hand, and the risk of robbery.	Agent responsibility for cash security should be clearly outlined in the contract with the account provider. • If the payment system is e-money, cash is owned by its bearer so cash security is the responsibility of the bearer agent. • If the agent is *deposit*-collecting, the cash in the till may be the customers', in which case greater security measures may be necessary.	1. Regulatory authority requires agents to be insured (whether by provider or self-provided)	• Insurance provides protection in case of theft. • Insurance requirement may constitute a barrier to entry for providers and /or agents.			X			X	X	X	X
				2. Provider informally agrees to make the agent whole based on sufficient evidence of robbery.	• Agents will not view theft as a barrier to entry, as they will bear the theft losses. • Creates moral hazard that may encourage thefts.									
				3. No account provider or regulatory action - local police matter	• Agents bear liability for theft losses. • Agent liability may create a barrier to entry.									
3.4 **Refer to 1.9**	Agent threatened with individual customer demands or potentially larger group protests due to inability to perform cash-out transactions.	Agent unable to perform cash out transactions due to KYC/CDD policies, insufficient cash on hand to meet occasional heightened demand, and/or system/network outages. For example, the account provider's system may be down, preventing KYC/CDD and transaction verification. Customer may have lost ID, pin code or phone; an updated account provider policy may prevent agent from resetting pin without sufficient credentials,	Market access issue between account provider and its customers, impacting the account provider's market reputation. Only becomes a regulatory issue if customers cannot reasonably retrieve their funds through other agents. Otherwise, police/public orders issue.	1. Account agreement or regulatory requirement stipulates access requirements and service levels. (see 1.2, 1.7, 1.8 and 1.9)	• Account agreement or regulatory requirement mitigates unreasonable expectations. • If inability to meet service levels becomes a problem, customer's can take legal action. More likely, customers would simply switch providers.			X	X	X	X	X	X	X
				2. No regulatory action	• Local police relied upon to handle civil disorder issues.									

Mobile Financial Services Risk Matrix: Agents

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		thus excluding the cash-out transaction.												
3.5 **Refer to 5.17**	Agent takes in cash that proves to be counterfeit.	Counterfeiter manufactures false notes to pass through agent and to integrate into the money supply.	Responsibility for accepting counterfeit currency for transfers the same as for sale of goods - with the agent. Agent training on counterfeits, and other illicit financial instruments, to be modeled on bank teller training and provided commensurate to the perceived risk. Account provider training program for agents subject to regulatory assistance/verification.	1. Regulatory authority provides mechanism for reporting, retrieval, and criminal investigation of suspect counterfeit notes. Regulatory authority sets parameters for training material for use by account providers with their agents.	• May incentivize agent to report counterfeit activity. • Reporting facilitates identification of issues, investigation, and apprehension of counterfeiters. • Regulatory authority requires capacity/budget to support anti-counterfeiting training and enforcement.			X	X		X	X	X	X
				2. Account providers required, as part of AML/CFT/Fraud training programs, to institute and monitor agent compliance commensurate with perceived risk.	• Training facilitates identification of issues, investigation, and apprehension of counterfeiters. • Active program will deter use of agents to pass counterfeit notes.									
				3. No regulatory response to counterfeit currency in circulation.	• Increasing circulation of counterfeit currency. • However, agents have a vested interest in identifying and rejecting counterfeit notes since these would be rejected if deposited in the agent's bank account.									
3.6 **Refer to 5.18**	Agent pays out cash that proves to be counterfeit.	Agent may pay out counterfeit currency received from customers without realizing it is counterfeit. Agent may use cash-out payments to distribute counterfeit currency.	Passing counterfeit currency, whether as cash outs to e-payments or as change on trade purchases, is a criminal issue for the police, not a regulatory issue. However, account providers should provide agent training on	1. Regulatory authorities should provide mechanism for reporting, retrieval, and criminal investigation of suspect counterfeit notes.	• Reporting facilitates identification of issues, investigation, and apprehension of counterfeiters. • Regulatory authority requires capacity/budget to support anti-counterfeiting training and enforcement.			X	X	X	X	X	X	X

Mobile Financial Services Risk Matrix: Agents

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		Agents may "get rid of" counterfeit currency they realize they have taken in by passing it on.	counterfeits, as for 3.4.	2. Regulatory authorities to provide an incentive, or reward, system for reporting and retrieving counterfeit currency, possibly including cash payments.	• Financial incentives can increase cooperation of agent network in identifying and pursuing counterfeiters. • Regulatory authority requires budget to support incentive program. • Financial rewards may encourage agents to collaborate with counterfeiters; however, authorities will monitor agents more closely that consistently turn in counterfeits for reward.									
				3. Account providers required, as part of AML/CFT/Fraud training programs, to institute and monitor agent compliance commensurate with perceived risk.	• Training facilitates identification of counterfeit currency and deters acceptance/distribution. • Agents may recirculate counterfeit currency if not incentivized or required to report it.									
				4. Regulatory authority or account provider could reward agents for identifying counterfeit currency or providing information on counterfeiters.	• Reward could provide the incentive for identification and the disincentive for passing the currency along. • Agents with frequent identification would need monitoring to ensure they were not involved in a counterfeit scheme. • Cost/capacity to implement such a scheme would need to be evaluated.									
				5. No regulatory oversight or training by account provider of agent	• Increased circulation of counterfeit currency. • However, account providers and agents have a reputational interest in									

Mobile Financial Services Risk Matrix: Agents

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
					preventing counterfeit cash distribution. • Burdening account providers with probably unenforceable counterfeit note regulation could reduce the incentives for market entry.									
3.7	Provision of credit to agents by non-bank actors.	Network models allow super agents/master agents to extend liquidity in the form of e-money directly to agents, possibly with limited or no controls or oversight.	Liquidity needs of account providers should be balanced with consumer protection for agents so that extension of credit does not become a vicious cycle.	1. No regulatory action *Note: Agent liquidity requirements or service levels may lead providers to play a more proactive role in liquidity management, which could result in their providing credit to super-agents; employing super-agents and providing them with budget for liquidity management—see 1.9 for more on agent liquidity issues.*	• Agents and super-agents will manage their own credit needs and indebtedness, as any small business.			X		X		X		X

Mobile Financial Services Risk Matrix: Account Providers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
4.1 **Refer to 7.10 and 7.11**	Provider employee manipulates agent credit allowances, agent e-money balances, or customer e-money balances for financial gain.	An insider with access to financial systems manipulates balances for his/her own financial gain.	Account providers responsible for their own internal security as a cost of doing business. Not a regulatory issue unless a) defalcations threaten the financial viability of the service, possibly providing a systemic impact, or b) service providers' customers are impacted, in which case the regulator has a consumer protection interest.	2. Regulatory authority requires providers to • Obtain fraud insurance to protect against insider threats and • Maintain 1:1 e-money reserve requirement in trust account. Depending on the liability loss, enlist law enforcement.	• Insurance will mitigate the risk of providers and the financial system against significant fraud risks. • Legal system must have the authority to arrest and prosecute those who committed the fraud. • Fraud insurance may not be available or may price providers out of entrance into the market	X	X	X	X	X	X	X	X	X
				3. Providers implement institution specific fraud detection systems	• Fraud detection allows for issue identification, investigation and prosecution. • Variance across institutions may let criminals target weak systems; however, competition will allow for innovation.									
				4. No required regulatory response to insider employee provider fraud.	• Small-scale insider manipulation is unlikely to have much impact • Systemic fraud by insiders could damage the stability of the financial system and will significantly damage the reputation of the mobile system.									
4.2	Provider fails to adequately select, train and supervise agents and super agents.	Agents acting on behalf of an account provider can damage the account provider's business reputation, both with the public and with the regulator if they act improperly.	Account provider agent selection, training and supervision policies and procedures are acceptable to the regulator, subject to verification of compliance. However, this is primarily a business management issue rather than a regulatory issue unless agent performance problems become flagrant. Regulator may mandate	1. Regulatory authority trains and licenses agents to ensure capacity.	• Training and licensing can help to ensure a base capacity among agents. • Regulatory ownership or training licensing is high cost and requires capacity that the regulator is unlikely to have.		X		X			X	X	X
				2. Regulatory authority requires provider to institute an AML/CFT/anti-Fraud training program which incorporates	• Training helps to ensure greater competence among the agent									

Mobile Financial Services Risk Matrix: Account Providers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
			KYC/CDD as a component of sound AML/CFT programs.	KYC/CDD guidelines. Training, compliance monitoring, and registration of agents is required by account provider.	network, and thus a stronger, more stable mobile payment system. • The agent may not have sufficient training, resources or motivation to follow prescribed guidelines without threat of penalty or termination of agent relationship for non-compliance. • Regularity verification of training program is low cost and requires low capacity.									
				3. Provider institutes training program that certifies an agent according to policies and procedures of the company for KYC/CDD; may encourage agents to adopt sound business practices and follow government guidelines for KYC/CDD.	• Training helps to ensure greater competence among the agent network, and thus a stronger, more stable mobile payment system. • The agent may not have sufficient training, resources or motivation to follow prescribed guidelines without threat of penalty or termination of agent relationship for non-compliance. • No regulatory oversight of training program may allow sub-optimal programs.									
				4. No required training or licensing process for agents	• Agent selection entirely up to the account provider. • Lax screening and/or inadequate training could result in service quality problems.									
4.3	Account provider or provider's agent does not meet required regulatory	Depending on the division of responsibilities, some AML procedures could be carried out	Account providers complying with such regulatory oversight as provided in law and regulation, including	1. Require account providers to institute appropriate due diligence of agents to ensure compliance with AML	• Primary responsibility for compliance with AML requirements within the account provider's network rests	X	X	X	X		X	X	X	X

Mobile Financial Services Risk Matrix: Account Providers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	responsibilities for AML.	by agents. Agents are generally not employees of the account provider and thus are related only through contractual arrangements. If roles are not clearly stipulated and enforced, compliance can be difficult.	effective suspicious transaction reporting. Predictable and enforceable penalties for non-compliance sufficient to motivate routine compliance.	requirements.	with the account provider. • Implies regulatory review of account provider's due diligence process.									
				2. Regulatory non-compliance results in corrective action and fine. Repeated non-compliance or significant instances of non-compliance will lead to a cease and desist order to the account provider.	• Penalties will create disincentive for non-compliance. • Implies that the regulatory authority has sufficient staffing and financial resources available to demonstrate effective enforcement.									
				3. Provider's agent agreement allows for termination for non-compliance.	• Termination threat will create a disincentive for agent non-compliance. • Despite contractual obligations of the agents, ML/TF risks will remain if not appropriately monitored by account provider and enforced by regulatory authorities.									
				4. No civil or criminal penalties for provider or provider's agent for non-compliance	• Enforcement of AML problematic, increasing risk of FATF censure.									
4.4	Trust fund is inadequately funded.	The account provider fails to adequately fund the trust account, possibly through • A breakdown in the funding process or • Intentional diversion of funds received in transit to cover the provider's operating costs. A trustee's fund investment strategy fails to conserve the	Trust funds are regulated and supervised similar to insurance reserve accounts to ensure adequate coverage of trust liabilities.	1. Regulatory authority requires minimum1:1 reserve requirement which is monitored through daily/weekly reporting with tiered enforcement options, including fines for non-compliance.	• Reporting requirements allow banks/providers to demonstrate to regulators and consumers their stability and soundness by meeting their requirement. The frequency of the reporting creates greater assurance, and thus lower risk. • Reporting requirements will impose a cost on banks/account providers. • Frequent reporting requirements could create a capacity issue for	X	X	X		X		X	X	X

Mobile Financial Services Risk Matrix: Account Providers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		fund's value.			regulators that do not have the staff to review reports and monitor compliance.									
				2. Regulator requires trustee to be bonded to cover the performance risk.	• Bonding will diversify the exposure of stakeholders; however, the cost could create a barrier to entry. If the cost is passed on to customers, the adoption/usage rate might slow. • Bonding costs could be covered by the interest that the trust accounts generate. • Monitoring and enforcement will focus on the acceptability of the bonding (insurance) company and the coverage provided.									
				3. Regulatory agency creates a new type of deposit insurance at the payment account holder level.	• Not needed for bank account providers, since funds already on deposit in covered bank accounts. • For cell-phone based account providers with pooled trust funds, this would substantially expand deposit insurance beyond current global practices and dilute the incentive for service users to open a formal bank account.									
				4. No regulatory action.	• Customers may lose mobile money balances if account provider is not managing trust accounts appropriately.									
4.5	Agent fraud untraceable due to poor records.	Lax or non-existent record keeping of transactions by agents creates challenges for account	Agents able to document their mobile financial transactions.	1. Regulatory authority requires agents to maintain paper records for a time period (consistent with other financial records)	• Audit trail requirements will discourage fraud, but may increase operating expenses and may not be		X	X	X		X	X	X	X

Mobile Financial Services Risk Matrix: Account Providers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
Refer to 7.2, 7.4, and 7.5		providers trying to research fraud issues. Payment transactions may be commingled with other merchant transactions, masking any irregularities in the payment service.	Account providers able to support police investigation of complaints of fraud. Regulatory involvement only in cases of systematic failure of account provider to ensure its agent network operates within reasonable bounds.	to support account provider's electronic records for investigation purposes.	complied with, particularly if fraud is involved. • Account provider's electronic records may be sufficient and more reliable.									
				2. Account provider operating and record keeping procedures developed, in concert with regulators, to support investigation in case of agent fraud.	• Generally in account provider's own interests to ensure transaction audit trails. • Providers will determine the degree of fraud protection on an institution by institution basis.									
				3. Require account providers to institute appropriate record keeping by f agents to ensure verifiable audit trails.	• Primary responsibility for compliance with record keeping requirements within the account provider's network rests with the account provider. • Agent records may well be provided through transaction records within the account provider's system. • Implies regulatory review of account provider's agent record keeping process.									
4.6 **Refer to 7.9 and 7.15**	System availability not maintained by account provider.	System users may be denied access to their funds if the account provider is unable to consistently maintain access to its services.	Account provider's services reasonably consistently available during normal business hours. Continuation of operating license contingent on maintaining reasonable service.	1. Regulatory authority mandates system redundancy requirements and disaster recovery to ensure continued financial system access, particularly for significant account providers.	• Redundancy and continuity will mitigate the risk of system availability and limit the duration when a failure occurs. • Documented alternative access procedures in the event of system failures for providers. • Regulations that focus on achieving the objective rather than prescribing specific procedures will enable		X	X	X			X	X	X

Mobile Financial Services Risk Matrix: Account Providers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
					account providers to innovate to provide the least cost solution. • Implies the regulator has, or can procure, the technical expertise to validate account providers' contingency plans.									
				2. Regulatory authorities permit off-shore data hosting and/or backup.	• In some jurisdictions where the infrastructure is weak, hosting data records in a more developed jurisdiction may be necessary to ensure adequate data security and integrity. • Can reduce operating expenses (and service fees) by facilitating economies of scale. • May require availability of fiber optic connections to ensure adequate band width. • May require agreement with hosting country regulator to verify compliance with data safety and security requirements.									
				3. Providers establish their own redundancy requirements and disaster recovery to ensure continued financial system access.	• Redundancy and continuity planning will mitigate the risk of failure in system availability and limit the duration when a failure occurs. • Should be supported by documented alternative access procedures in the event of system failures for providers. • Lack of regulatory requirement will allow each institution to define the extent of their contingency planning,									

Mobile Financial Services Risk Matrix: Account Providers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
					which may leave some less protected than may be appropriate for a payment system. However, it will also allow individual institutions to innovate.									
4.7 **Refer to 1.9**	Agents are consistently out of cash.	Without effective cash forecasting mechanisms, agents may have difficulty managing their cash needs. Cyclical or unexpected demands may complicate cash flow forecasting. Agents may be too far removed from a cash supply point to respond quickly to an increase in cash demands.	Agents have sufficient cash on hand to support most cash-out requests. Account providers support agents with cash management and forecasting.	1. Regulator mandates liquidity requirements for providers. (by agent or by geographic region) The provider could be required to appoint an "agent of last resort" to ensure customer access.	• Requirement may enhance access to cash within a reasonable amount of time. • Consistent shortages decrease confidence in a provider's system. • Requirement could raise a cost barrier to entry as small players may not have cash forecasting/cash management capabilities. • Providers may decide to hire some agents as employees, as independent agents in high-volume areas may not be able to maintain balances or deal with security issues. • Forecasting and management capabilities are similar for ATM and Branch cash forecasting/ management. • Regulation implies monitoring and enforcement capacity.		X	X	X	X	X	X	X	X
				2. Providers forecast and manage liquidity of agent network to optimize service for consumers.	• Enhances customer access to cash within a reasonable amount of time, improving public perception of service. • Account providers may decide to hire some agents as employees, as independent agents in high-volume areas may not be able to maintain									

Mobile Financial Services Risk Matrix: Account Providers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
					balances or deal with security issues. • Forecasting and management capabilities are similar for ATM and Branch cash forecasting/ management.									
				3. Require account providers establish a contingency funding plan in case cash-out needs are inconsistent with liquidity forecasts.	• Account providers have a vested interest in minimizing cash shortages. • Implies regulatory review of contingency plans.									
				4. No oversight for agent liquidity	• Customers may be unable to withdraw cash from mobile money accounts from time to time, when agents run out of cash. • Market forces will improve liquidity management over time, as account providers keep reliable agents, take on some agent responsibilities, or partner with other institutions as agents of last resort.									
4.8	Agent contracted to multiple account providers (i.e. a cell phone provider and a bank) with different regulatory requirements (e.g. KYC) does not meet its responsibilities for one or more.	When an agent contracts with more than one account provider with differing regulatory requirements, the agent may confuse its responsibilities, meet the lower regulatory burden between the two, or not meet the regulatory requirements for either.	Account providers to hold agents responsible for their individual contractual agreements, whether exclusive or not.	1. Regulatory authority prohibits agents from representing multiple account providers.	• Restricting multiple agent relations may limit competition, particularly if the first mover has locked in the most suitable agents. • Agents may not achieve adequate volumes to justify being a paying agent is not able to link to multiple account providers. • Difficult and expensive to monitor.	X		X	X		X	X	X	X
				2. Providers do not permit agents to enter into contractual obligations with other account providers without prior	• Helps first mover justify market entry.									

Mobile Financial Services Risk Matrix: Account Providers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
				consent.	• Limits subsequent competition by locking in the most suitable agents. • May limit agent profitability below breakeven point, limiting service expansion.									
				3. No action is taken by regulatory authorities or account providers restrict agents to a single account provider.	• Agents may link to multiple account providers. • Ensures competition based on service quality. • May reduce incentive for first mover.									
4.9	Individual poses as agent to collect deposits or payments from unsuspecting customers.	If an individual poses as an agent for an account provider, they could accept deposits or payments from customers and pocket the funds. The risk is likely higher in remote areas where oversight is limited, and where financial literacy is lower.	Consumers able to avoid fraud through spurious agents.	1. Regulatory authority requires all account provider agents to be registered. This list of registered agents published, and all registered agents post evidence of registration.	• Increased public information of registered agents allows consumers to protect themselves by only frequenting registered agents. • Implies regulatory capacity for agent registration and the public information campaign. • Requires that account providers require each agent to post registration at its place of business. • Most susceptible consumers, those who are financially illiterate, will be the most difficult to reach with an information campaign.			X	X		X	X	X	X
				2. Regulatory authority requires providers to publish a list of official agents on a periodic basis to limit the potential for fraud.	• Account provider assumes responsibility for distributing and advertising list of its agents. • Increased public information of official agents allows consumers to protect themselves by only frequenting official agents.									

Mobile Financial Services Risk Matrix: Account Providers

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
					• Most susceptible consumers, those who are financially illiterate, will be the most difficult to reach with an information campaign.									
				3. Rely on the significant consumer protection built into the system through electronic receipts and account limits to mitigate fraud.	• During cash in, the agent will have to have enough e-money available to initiate the transaction and resulting confirmation to the service user. • Transaction limits inhibit service users from acting as informal agents. • Monitoring systems flag suspicious behaviour, enabling the account provider to shut down informal agents.									
				4. No regulatory action	• Public may not understand that Account providers are not accountable for actions of these bad actors. • Instances of fraud subject to normal police investigation.									

Mobile Financial Services Risk Matrix: Trust Account Holding Financial Institutions

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
5.1 Refer to 7.12	Liability concentration risk caused by an expanding trust account that may have a material impact on the trustee institution's balance sheet, particularly for those trust funds on deposit with the trustee bank.	Trust funds of a successful account provider could become significant to the point of representing a funding concentration risk for the trustee bank - liquidity risk - should there be a sudden reduction in the volume of items in transit through the account provider's system. This could be due to new competition, changes in regulation, account provider decision to diversify its own risks, or civil disturbances that cause a flight to cash.	Trustee banks limit the size of trust accounts they manage to what is reasonably manageable for that institution.	1. Bank regulators limit risk concentrations as a normal part of their supervisory activities - this process should include funds held in trust, so off-balance sheet unless held in deposit accounts.	• Concerns with managing risk concentrations may restrict bank interest in providing trust services. • Trust funds need investment opportunities that provide adequate liquidity in case of rapid disintermediation.									
5.2	The reputation of the financial institution which holds the trust account for the mobile financial account provider is damaged due to its mismanagement of the trust account.	The financial institution which holds the trust fund for the account provider takes on reputational risk. If the trust funds are invested in instruments that do not conserve their value, the liability coverage provided by the trust assets may become inadequate, potentially leading to a crisis in confidence in the service.	Preserve the value of the trust funds through prudent investment management, subject to regulatory oversight (as for insurance company reserves) The affiliation risk will be managed by the market. Banks should not enter into agreements with mobile financial account providers with which they have concerns.	1. Regulatory requirements govern the investment instruments in which trust account holding financial institutions may invest funds.	• Conservative investment strategies for the trust funds will preserve asset values but limit investment income which might otherwise be applied to offset account provider costs and keep transaction fees low.		X		X		X	X	X	X
				2. Regulators evaluate reputational risk of major trust relationships.	• Adverse selection may come into play - those banks most qualified to act as trustees may be the most reluctant to take on the risks of doing so.									
5.3	The reputation of the financial institution which holds the trust account for the mobile financial account provider is damaged due to its association with an	The financial institution which holds the trust fund for the account provider takes on reputational risk. If the account provider is poorly managed, the trustee's affiliation with an	Preserve the value of the trust funds through prudent investment management, subject to regulatory oversight (as for insurance company reserves) The affiliation risk will be managed by	1. Regulatory requirements govern the investment instruments in which trust account holding financial institutions may invest funds.	• Conservative investment strategies for the trust funds will preserve asset values but limit investment income which might otherwise be applied to offset account provider costs and keep transaction fees low.									

Mobile Financial Services Risk Matrix: Trust Account Holding Financial Institutions

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	account provider whose payment system is poorly run.	institution that loses the public trust could damage its own reputation.	the market. Banks should not enter into agreements with mobile financial account providers with which they have concerns.	2. Regulators evaluate reputational risk of major trust relationships.	• Adverse selection may come into play - those banks most qualified to act as trustees may be the most reluctant to take on the risks of doing so.									

Mobile Financial Services Risk Matrix: Payment Systems

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
6.1	Government mandated usage of government owned payment utility to process and clear all payment transactions regardless of type.	Government may have invested in a national payment system designed not just for inter-bank settlements but to reach down to the retail level, and may seek to protect its investment by blocking development or use of other payment systems. This risks blocking innovation to improve efficiency and lower payment costs.	Limit government involvement in payment systems to a) interbank settlements, and b) establishing an enabling environment for retail payments that encourages competition and innovation within accepted security standards.	1. Government ownership of the payment switch effectively requiring any existing and new account provider to connect to and use the system for its payment services.	• Interoperability creates benefits to consumers, as they can transfer to any other consumer regardless of network. • If government perceives a profit opportunity, rather than a public good, monopolistic pricing of the transaction could ensue. • There is no incentive for a new technology innovations since the government requires all transactions to be processed through the system		X	X	X				X	
				2. Mobile financial account providers allowed to use whatever payment system best serves the needs of their clients.	• Market pricing • Incentive to innovate processing systems and reduce transaction costs • Interoperability will be market driven.									

Mobile Financial Services Risk Matrix: National Regulators

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
7.1	Illicit financial activities enabled by weak KYC/CDD requirements/enforcement.	If the AML/CFT requirements do not apply to mobile financial services, illicit actors could leverage the mobile network for illicit means. If the party providing the financial service is held to these standards, but its ability to comply/enforce them is limited, the risk still remains. (The ability to enforce AML/CFT among a disparate agent population is a critical element.)	Risk-based supervision and enforcement of AML/CFT safeguards to enable authorities to focus on the highest priority risks.	1. Regulatory authority implements and enforces a point –based (stepped based on risk) AML/CFT system.	• Point-based AML/CFT system allows flexibility for consumers with various forms of identification; however, limits risk by embedding a standard due diligence requirement industry-wide. • Regulatory authority to implement/monitor/enforce can be costly, considering that agents are the implementers.	X	X	X	X		X	X	X	
				2. Account providers elect to have account opening conducted by employees rather than agents, so as to maintain stricter AML/CFT controls.	• Account providers can hedge risk by controlling account opening process. • Potential customers inconvenienced as account provider has limited footprint relative to agent network. • Cost of building a network to support would be costly.									
				3. Account providers institute institution specific KYC/CDD policy for agents, which should comport with sound AML/CFT standards.	• Point-based AML/CFT system allows flexibility for consumers with various forms of identification; while limiting risk by embedding a standard due diligence requirement network-wide. • Lack of regulatory guidelines will lead to variance in system strength which can allow for exploitation. • Implies regulatory capacity to monitor individual account provider policies and procedures, but allows for innovation in achieving the objective.									
				4. No regulatory action for mobile on	• Illicit actors leverage mobile									

Mobile Financial Services Risk Matrix: National Regulators

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
				AML/CFT.	networks for illegitimate financial purposes; illicit activity flourishes in economically disadvantaged regions/zones where provider enforcement mechanisms are weak									
7.2 **Refer to 4.5, 7.4, and 7.5**	Identification of illicit financial activities hampered by insufficient reporting requirements.	Reporting of large or suspicious transactions to appropriate authorities and/or the Financial Intelligence Units (FIUs) provides information on mobile financial transactions that exceed or are structured to avoid reporting requirements, as well as on trends and patterns of unusual mobile financial activity.	Risk-based supervision and enforcement of AML/CFT safeguards to enable authorities to focus on the highest priority risks.	1. Financial regulatory authority includes mobile providers in AML/CFT reporting requirements to appropriate authorities and/or the FIUs. Account providers file Suspicious Transaction Reports (STR) for transactions meeting specified criteria. 2. STRs for all reporting entities indicate the channel used, including mobile.	• Standardized reporting, in line with financial institutions, mitigates potential for illicit activities and facilitates investigation. • Reporting requirements impose a cost on the account provider, which would be reflected in usage fees. • Account provider may not have the technology to identify suspicious transactions, resulting in a dump of all transactions on the FIU. • FIU may not have the capacity or budget to analyze reports for mobile sector.	X			X		X	X	X	X
				3. Account providers are not included in STR reporting requirement.	• Mobile financial services could be used to channel large quantities of small payments in support of illicit activities.									
7.3 **Refer to 4.2**	Illicit financial activities facilitated by unlicensed/ unmonitored agent network.	As agents are a critical component of the mobile payment network, may facilitate fraud or criminal activity (e.g. if they do not comply with AML/CFT requirements, customers could conceivably set up accounts under false identities).	Risk-based supervision and enforcement of AML/CFT safeguards to enable authorities to focus on the highest priority risks.	1. Regulatory authority trains and licenses agents to ensure capacity.	• Training and licensing can help to ensure a base capacity among agents. • Regulatory ownership or training licensing is high cost and requires capacity that the regulator is unlikely to have.		X	X	X	X	X	X		
				2. Regulatory authority requires account provider to institute an AML/CFT/anti-	• Training helps to ensure greater competence among the agent									

Mobile Financial Services Risk Matrix: National Regulators

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
				fraud training program which incorporates AML/CFT guidelines. Training, compliance monitoring of, and registration of agents is required by account provider.	network, and thus a stronger, more stable mobile payment system. • Motivating agents o follow prescribed guidelines may be challenging. • Implies regulatory support for and verification of training program.									
				3. Provider institutes training program that certifies an agent according to policies and procedures of the company for AML/CFT; may encourage agents to adopt sound business practices and follow government guidelines for AML/CFT.	• Training helps to ensure greater competence among the agent network, and thus a stronger, more stable mobile payment system • Motivating agents to follow prescribed guidelines may be challenging. • No regulatory enforcement of training program may allow sub-optimal programs.									
				4. No required training or licensing process.	• Least direct costs for account providers and regulators. • May result in indirect costs through use of mobile financial services to support illicit activities.									
7.4 **Refer to 4.5, 7.2, and 7.5**	Inadequate transaction records impair investigation of fraud or criminal activity	Full transaction audit trails are essential to investigations to follow the money trail. Records retention should permit reconstruction of transaction details, including the identity of the transaction parties.	Regulatory framework follows international standards for financial records retention to mitigate risks, which sets 5 years to enable information requests from competent authorities.	1. All service users required to maintain an individual bank account through which all transactions flow.	• Cell phone company role limited to messaging - actual transactions occur in the bank. • Ensures that full transaction records exist within the formal banking system. • Acceptable to users who already have bank accounts, but represents a high cost barrier to users who have			X	X		X	X		

Mobile Financial Services Risk Matrix: National Regulators

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
					no need for a full banking relationship. • Would substantially restrict expanding access to financial services to the unbanked.									
				2. Regulator requires transaction level reporting and implements internal suspicious transaction identification process.	• Internal systems facilitate investigation • Lowers account provider costs by enabling a raw data dump on the FIU, without the need for analysis. • Implies FIU capacity to absorb and analyze large volumes of transaction data, essentially all of which will be routine.									
				3. Regulatory authority requires the account provider to maintain all payment transaction records for 5 years following the completion of the transaction. (Should mimic financial requirements)	• Record retention requirements will facilitate investigation. • Records retention responsibilities may be tiered to transaction amounts and type of services provided (e-money issuer, remittance services, Telco) • Retention requirements will impose a cost on providers, which would be passed on to service users. • Differs from normal cell phone call records, which may be subject to shorter record retention.									
				4. Provider sets internal policies and procedures for maintaining all records obtained through the CDD process and transaction records (Customer Detail	• Record retention requirements will facilitate investigation. • If the standards for retention are low, authorities may not be able to									

Mobile Financial Services Risk Matrix: National Regulators

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
				Records-CDRs) for a specified period following the completion of the transaction, failure of the account provider, and/or termination of customer relationship.	trace transactions within a payment chain from one provider to another or reconstruct sender/receiver identities in the prosecution of financial crimes.									
				5. No mandatory or implied records retention policies for mobile financial services	• Ability to reconstruct audit trail is dependent on business practices for records retention and retrieval capability of account providers and others in the account provider's network.									
7.5 **Refer to 4.5, 7.2, and 7.4**	National regulators and/or law enforcement authorities unable to effectively investigate fraud or criminal activity due to lack of operational support systems and human capacity.	Investigative officials are unlikely to have the human capacity to effectively regulate the network of providers, agents, trust accounts and customers necessary to mitigate the known risks. If the regulatory framework entailed licensing/supervising agents, as well as providers and banks, the number of regulators required for this activity would likely be well beyond that on staff for the regulatory authorities.	Risk based regulatory framework that minimizes the role of the regulator while providing an enabling environment that mitigates against risks to the customer, account provider network and the financial system. Regulatory capacity sufficient to provide a deterrent to illicit use of mobile financial services through heightened risk of discovery and prosecution.	1. Establish an FIU with sufficient resources to credibly investigate suspicious transactions and initiate prosecution of illicit activity. Establish specialized investigative, prosecutorial and judicial expertise within the legal system.	• Would enable the country to comply with FATF guidelines and participation in the Egmont group. • Would extend activities already in principle required for banking and insurance to mobile financial services. • Has cost implications - may require a fee regime on account providers, which would be passed on to users, reducing the financial incentives to use mobile financial services.		X	X	X		X	X	X	X
				2. Establish a risk-based framework that shifts the responsibility for monitoring compliance on behalf of the agent to the account provider.	• The regulatory authority can leverage the transactional level compliance efforts of the account provider by focusing on the control mechanisms and risk management programs from a system level.									
				3. FIU established but not adequately resourced, or no FIU established.	• No direct cost incurred, but • Not in compliance with FATF									

Mobile Financial Services Risk Matrix: National Regulators

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
					guidelines, potentially risking inclusion in the list of non-compliant countries, leading to restrictions of access to international financial markets.									
7.6	National regulators and/or law enforcement authorities unable to effectively investigate fraud or criminal activity due to lack of authority.	In many country contexts, the regulatory framework for mobile payment service provision has not been established. Thus, it is unclear whether the financial regulators have the authority to oversee the payment network, or if it is the responsibility of the telecommunications regulators, or if anyone has the requisite authority. Jurisdictional concerns may be exaggerated, since the service functions are distinct. For instance, in the United States, many grocery stores provide access to financial services (credit unions, etc) but their core business is selling groceries. Their financial activities are easily overseen by financial authorities and their core business is overseen by state food safety regulators.	Clearly defined centralized regulatory authority for mobile payment networks. Clearly defined authority to refer breaches of public trust or illicit activities to law enforcement authorities for prosecution.	1. Empower through law/regulation either the financial regulator or telecommunications regulator as the sole regulatory authority over mobile payment system.	• Sole authority limits confusion regarding investigative authority. • However, different issues may require different subject matter expertise which may not be resident in the sole regulator. • Capacity/Budget of sole regulator may need to be adjusted to accommodate increased responsibility.		X		X		X	X	X	X
				2. Harmonize enforcement and penalty authority framework across Communications and Financial Services regulatory authorities.	• Harmonization process defines which regulator is responsible for which tasks, mitigating risks of issues "falling between the cracks" or of overlapping or contradictory activities. • However, emerging risks may create confusion regarding responsibility. • Authorities may lack capacity to implement across institutional silos.									
				3. No Formal System (Ad hoc – on a case-by-case basis as determined).	• Lack of defined responsibility regarding specific risks will create confusion and uncovered areas, creating risk for the financial sector.									
7.7	Account provider may fail to institute appropriate	Mobile financial services are a dynamically growing market with	Regulators to ensure account providers monitor evolving new risks,	1. Regulatory authority, or financial intelligence unit (FIU), monitors emerging	• Emerging risk monitoring will help the providers be vigilant with regards		X		X	X	X	X	X	

Mobile Financial Services Risk Matrix: National Regulators

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	safeguards against newly emerging risks.	new account providers, new services and new vulnerabilities developing rapidly. Ensuring that information on the risk factors is disseminated and understood, and appropriate safeguards instituted, is a significant challenge.	and institute appropriate risk mitigation. Regulators routinely disseminating warnings of new risks as these are identified.	risk for financial sector, including mobile payment systems.	to emerging risk, so they can develop mitigation strategies early. • Would benefit from integration into the global FIU network. • FIU may not have the skills / capacity necessary to analyze risks associated with this new channel. • FIU may not have the budget to cover this area.									
				2. Association of account providers monitors emerging risk for financial sector, including mobile payment systems.	• Emerging risk monitoring will help the account providers be vigilant with regards to emerging risk, so they can develop mitigation strategies early. • Individual account providers generally linked to international institutions operating in multiple countries, allowing for cross fertilization. • There may be no association at the country level - but account providers linked to the GSM Association.									
				3. No oversight of emerging risks	• Emerging risks may not be spotted until the risk is has become a significant problem.									
7.8	The ability to track/investigate illicit transactions is made difficult by the number of financial intermediaries (e.g. agents, super agents, providers, banks managing the trust	Criminal elements can utilize the lack of standard processes in conducting transactions, particularly in commingled accounts and instances where it is difficult to identify the beneficial owner. This risk may be	Minimum standard audit trail for SMS/USSD (Unstructured Support Service Data) transactions to enable investigation through account providers' payment transaction processing system consistent with international standards, with accurate	1. Regulatory authority mandates inclusion of accurate and meaningful information with transfer or related message through the payment chain.	• Implies regulatory involvement in data standards and oversight over account provider data transmission and retention policies and procedures.	X		X	X		X	X	X	
				2. Regulatory authorities prohibit mobile	• Would limit the complexity of									

Mobile Financial Services Risk Matrix: National Regulators

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	accounts); and as these various actors are not vertically integrated, the lack of transparency between them exacerbates the challenge for regulators.	heightened with remote and non-face-to-face transactions, particularly in the cross-border context of some mobile financial service business segments.	and meaningful information that travels with each transaction. Contracts clearly identify the responsibilities of each party in the transaction and provide clear channels for sharing information.	financial services outside of the same account providers or bank.	transactions. • Prohibits the expansion of low cost mobile financial services and would inhibit service innovation and outreach.									
				3. No regulatory action	• Regulatory authorities would rely on account provider records.									
7.9 **Refer to 4.6 and 7.15**	Account provider suspends operations or collapses, disrupting service.	Temporary or permanent failure of a systemically important account provider could trigger loss of public confidence that could spread beyond the account provider, causing a general crisis of confidence among the public. As communication networks are relied upon for financial services, performance risk becomes concentrated in critical systems whose failure for technical or business reasons could impact a significant portion of the population.	Contingency response policies and procedures to ensure continuity of operations and rapid recovery in case of failure.	1. Regulatory authority mandates system redundancy requirements and disaster recovery policies and procedures to ensure continued public access.	• Redundancy and continuity will mitigate the risk of system availability and limit the duration when a failure occurs. • Documented alternative access procedures in the event of system failures for providers	X	X	X	X	X	X	X	X	X
				2. For cell phone based systems, regulator requires off-site storage of backup data in a format that would enable an orderly liquidation of the trust account(s) through repayment to system users. For bank based systems based on individual bank accounts, normal bank processes required.	• Implies an orderly liquidation process or transfer to an alternate account provider similar to that used for a failed financial institution.									
				3. Providers establish their own redundancy requirements and disaster recovery to ensure continued financial system access.	• Redundancy and continuity will mitigate the risk of loss of system availability and limit the duration when a failure occurs. • Documented alternative access procedures in the event of system failures for providers. • Lack of regulatory requirement will									

Mobile Financial Services Risk Matrix: National Regulators

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
					allow each institution to define the extent of their contingency plans, which will leave some less protected than may be appropriate for the payment system. However, it will also allow individual institutions to innovate.									
7.10 **Refer to 4.1 and 7.11**	Account provider's employee sets up accounts on the system with balances not backed by receipt of currency and funding of the trust account(s). Such an act would create a liability and related losses for the account provider	Generally, when a customer sets up a prepaid mobile payment account, they make a deposit of real currency for an equivalent balance of mobile money. However, an employee of the account provider with access to the backend systems could set up fraudulent new accounts that were not backed by currency. The employee could then either cash-out or spend their mobile money, depleting the trust funds, which could go unnoticed without proper internal safeguards. Since e-money is backed by real money deposited in the trust account (or the capital of the account provider, if deficient), creation of e-money may increase the velocity of money, but not the volume.	Account providers ensure sufficient internal controls and monitoring of the trust balances against the amount in transit to discourage such defalcations and rapidly identify them should they occur. Subject to regulatory oversight.	1. Regulatory authority requires account providers to conduct due diligence screening on key employees and obtain fraud insurance (bonding) to protect against insider fraud.	• Insurance will mitigate the risk to account providers and the financial system of fraud. • Fraud insurance may not be available or be expensive. • Bonding costs lower if the legal system has the capacity to arrest, prosecute and convict those who commit fraud.		X	X	X	X		X	X	X
				2. Providers implement institution specific fraud detection systems.	• Account providers have a vested interest in protecting themselves from internal fraud and in implementing appropriate internal controls. • Fraud detection allows for issue identification, investigation and prosecution. • Variance across institutions may let criminals target weak systems; however, competition will allow for innovation.									
				3. No required regulatory response to insider employee fraud.	• Small-scale insider manipulation is unlikely to have much impact. • Systemic fraud by insiders could damage the stability of the financial									

Mobile Financial Services Risk Matrix: National Regulators

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
					system and will significantly damage the reputation of the mobile system.									
7.11 **Refer to 4.1 and 7.10**	In economies where minutes are exchanged like currency, and could be cashed-out for currency, distributor of airtime vouchers or distributor employee could increase the amount of airtime on the market.	In some economies, mobile minutes have been used as a means of exchange. Generally, an account provider will provide mobile minutes as a service for a specific price. However, an account provider could increase the number of minutes on the market without compensation for various reasons, such as extra minutes to reward customer loyalty. The effect would be to discount the price of the cell phone company's service, just as any other product discount results in an increase in the product or service provided without an offsetting increase in revenue. If the additional minutes are cashed out at the original price, the cell phone company is in effect paying its clients a cash rebate.	The account provider's business model will determine the extent of service discounts they wish to provide to their customers. Not a regulatory issue.	1. No regulatory action	• Hopefully cell phone company "sales" that reduce the cost of airtime will result in increased business rather than losses.		X	X	X	X	X	X		
7.12 **Refer to 5.1**	Increasing reliance on mobile financial services may result in a concentration of deposits in one or a few trustee financial institutions, leading to disintermediation from smaller institutions and reductions in access to finance from those	Rather than having funds dispersed across the financial system, or outside of the financial system entirely, the uptake of mobile payment services will concentrate payment account funds in the trust funds held in only a few institutions. The financial institutions where	Application of prudential guidelines on risk concentrations/dependencies to account provider trust accounts. Expansion of larger financial institutions down-market as the technology lowers transaction costs and service break even points.	1. Law/Regulation that limits the size of a trust account or group of trust accounts from any account provider in any one trustee institution to a percentage of the trustee's risk weighted capital.	• Diversification of trust accounts holdings across multiple financial institutions reduces risk concentrations. • Spreading trust funds across multiple financial institutions will add complexity for account providers, increasing operating costs. • Implies regulatory oversight to		X					X		

Mobile Financial Services Risk Matrix: National Regulators

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	institutions.	some of these funds would have been deposited will have fewer resources with which to make loans. The institutions holding these funds could be restricted by regulations, or their own credit policy decisions, from using these funds for lending, thus reducing the level of loan funding available to the economy. This could lead to consolidation within the financial system resulting from those institutions that are not able to keep up with the technology having increasing difficulty competing. However, the conversion of cash in circulation to deposits in the trust accounts would increase the resources of the banking system as a whole.			ensure compliance. 2. No regulatory action • Account providers hedge their risk relating to concentration of deposits based on profit motive, which may not align with what is best for the market as a whole.									
7.13 **Refer to 1.12**	Single dominant player in a closed-loop environment abuses market power (predatory pricing).	A single telecom company can dominate the market in the absence of adequate competition. The first player to enter the market can create a monopoly, which can potentially lead to anti-competitive pricing and restricted services/innovation.	Fair competition among providers on products/services. No unreasonable barriers to the flow of funds between account providers. Predictable market entry for qualified applicants to ensure that the prospect of competition discourages predatory pricing. National and regional payment systems able to transmit payments between account providers and	1. Regulators require interoperability of payment networks (through inter-provider links or through a switch)	• Requirement of interoperability could raise a barrier to entry as the technology requirements could be more challenging than a simple closed network. Further, the requirement could stifle innovation in a new technology through keeping new entrants out. • Customers would benefit as there would be no network limitations on sending mobile money. • Providers would be forced to		X					X	X	X

Mobile Financial Services Risk Matrix: National Regulators

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
			between countries.		compete on cost, products, and service, rather than size of network which could represent a first mover advantage. • By reducing the first mover advantage, could discourage potential first movers from entering the market.									
				2. Competition agency empowered to investigate non-competitive behavior	• Implies a competition agency with the capacity to investigate and enforce non-competitive behavior, such as predatory pricing, to counteract the incentive for monopoly pricing, thus protecting the consumer. • However, may impede development of cross network transaction capability.									
				3. No regulatory action	• Predatory pricing and expanded monopoly power are possible. However, experience with networked technologies (cell phones/ATMs) suggests that the market will move toward interoperability without regulatory action. • Provided that account providers are given consistent market entry requirements, abuse of the first mover advantage will encourage competition to enter the market.									
7.14	Illicit actors conduct high volume transactions using	Because of the speed of the payment process using a mobile	Account providers flag and limit opening multiple accounts based on	1. Account providers required to flag and block multiple accounts with similar KYC/	• Monitoring systems implemented by	X		X	X			X		

Mobile Financial Services Risk Matrix: National Regulators

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	multiple accounts, bypassing monitoring systems before regulators can step in.	system, it is possible to make multiple transactions quickly, in a near real-time transaction environment. With reasonable preparation, large sums could be transferred simultaneously using multiple accounts.	similar KYC/ CDD data. Subject to regulatory oversight.	CDD data.	the account provider can deter most illicit activity. • Implies regulatory verification of account provider systems, policies, procedures and its capacity to comply.									
				2. Rely on account monitoring as another alternative to KYC.	• Multiple accounts of the same owner can be identified via pattern identification systems that recognize activity similarities (e.g. several account all sending money to the same place/agent/customer or e.g. an unusual level of transactions from one place to another in a given timeframe.) • Enables expanded access where national ID systems may be weak.									
				3. No regulatory action.	• Providers will institute risk mitigation systems in line with their perceived risk to abuse of their system.									
7.15 **Refer to 4.6 and 7.9**	Financial terrorists target payment network to disrupt financial system.	Financial terrorists hack into mobile payment network to disrupt the economy. The mobile payment network may be targeted, as the security is perceived as less than that of the financial system. Alternatively, terrorists may target the data center of the account provider to damage or destroy service capacity.	Mobile payment networks' security requirements, including possible redundancy, to be commensurate with the proportionate systemic importance of the account provider.	1. Regulatory authority mandates system redundancy requirements and disaster recovery to ensure continued financial system access, particularly for significant account providers.	• Redundancy and continuity will mitigate the risk of impaired system availability and limit the duration when a failure occurs. • Documented alternative data access and recovery procedures in the event of system failures for account providers	X	X	X	X	X	X	X	X	X
				2. Providers establish their own redundancy requirements and disaster	• Redundancy and continuity will mitigate the risk of impaired system									

Mobile Financial Services Risk Matrix: National Regulators

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
				recovery to ensure continued financial system access.	availability and limit the duration when a failure occurs. • Documented alternative data access and recovery procedures in the event of system failures for providers • Lack of regulatory requirement will allow each institution to define the extent of its contingency plans, which will leave some less protected than may be appropriate for the payment system. However, it will also allow individual institutions to innovate.									
7.16	Account provider fails / enters insolvency limiting customer access to funds and potentially destabilizing financial system.	Mobile payment account providers, like other companies, may fail / enter insolvency for a variety of reasons. However, unlike normal companies, their service provision is a component of the financial system and their insolvency can destabilize the economy if not properly managed.	Mobile payment account providers' insolvency procedures should mimic those of financial institutions. Established process for obtaining records of items in transit and enabling rapid cash out liquidation or transfer to another account provider using the trust funds. Clear regulatory policies and procedures to manage such events.	1. Incorporate winding up provisions in the Law / Regulation covering mobile financial account providers, particularly on assuring regulatory access to transaction records and trust funds that back items in transit.	• Protection of payment system assets and records in case of insolvency would minimize the systemic impact of a mobile payment system failure. • Assets of clients, as in customer funds in transit or temporary storage, should be kept out of the general pool of assets available to satisfy creditors. This is particularly important in countries under statute law that does not accommodate separation of assets into trusts.	X	X	X	X	X	X	X	X	X
				2. Insolvency handled like any other business.	• Financial system stability would be at risk depending on the size of the network. • Consumer protection for payment account holders would be a significant issue if the insolvency process did not protect these									

Mobile Financial Services Risk Matrix: National Regulators

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
					accounts differently from the general assets of the account provider.									
7.17 **Refer to 3.5**	Counterfeit funds accepted by an agent.	Agents will be targeted as an entry point for counterfeiters to unload money into the system. Counterfeiters will perceive agents as less knowledgeable than bank employees, the security/monitoring of agents to be less than banks, and yet still have a high enough transaction volume that they would be difficult to identify.	Agent training on counterfeits to be modeled on bank teller training and provided by account providers commensurate to the perceived risk.	1. Regulatory authority provides mechanism for reporting, retrieval, and criminal investigation of suspect counterfeit notes. Regulatory authority sets parameters for training material for use by account providers with their agents.	• May incentivize agent to report counterfeit activity. • Reporting facilitates identification of issues, investigation, and apprehension of counterfeiters. • Regulatory authority requires capacity/budget to support anti-counterfeiting training and enforcement.			X	X	X	X	X	X	X
				2. Account providers required, as part of AML/CFT/Fraud training programs, to institute and monitor agent compliance commensurate with perceived risk.	• Training facilitates identification of issues, investigation, and apprehension of counterfeiters. • Active program will deter use of agents to pass counterfeit notes.									
				No regulatory response to counterfeit currency in circulation.	• Increasing circulation of counterfeit currency.									
7.18 **Refer to 3.6**	Counterfeit funds distributed by an agent.	Counterfeiters may try to recruit agents into their networks to distribute counterfeit currency into the economy.	MNOs responsible for supervision of agents and collaborate with law enforcement authorities on investigation of counterfeit currency to enable criminal prosecution of agents.	1. Regulatory authorities should provide mechanism for reporting, retrieval, and criminal investigation of suspect counterfeit notes.	• Reporting facilitates identification of issues, investigation, and apprehension of counterfeiters. • Regulatory authority requires capacity/budget to support anti-counterfeiting training and enforcement.		X	X	X	X	X	X	X	X
				2. Regulatory authorities to provide an incentive, or reward, system for reporting and retrieving counterfeit currency, possibly including cash payments.	• Financial incentives can increase cooperation of agent network in identifying and pursuing counterfeiters. • Regulatory authority requires budget									

Mobile Financial Services Risk Matrix: National Regulators

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
					to support incentive program. • Financial rewards may encourage agents to collaborate with counterfeiters; however, authorities will monitor agents more closely that consistently turn in counterfeits for reward.									
				3. Account providers required, as part of AML/CFT/Fraud training programs, to institute and monitor agent compliance commensurate with perceived risk	• Training facilitates identification of counterfeit currency and deters acceptance/distribution. • Agents may recirculate counterfeit currency if not incentivized or required to report it.									
				4. Regulatory authority or account provider could reward agents for identifying counterfeit currency or providing information on counterfeiters.	• Reward could provide the incentive for identification and the disincentive for passing the currency along. • Agents with frequent identification would need monitoring to ensure they were not involved in a counterfeit scheme. • Cost/capacity to implement such a scheme would need to be evaluated.									
				5. No regulatory oversight or training by account provider of agent	• Increased circulation of counterfeit currency.									
7.19	Currency redenominated while in transit.	When a country redenominates its currency, often after a period of high inflation, service users should be paid out in the new units, adjusted for the redenomination.	Treat items in transit in the same was as deposits in the banking system are treated in case of redenomination of the currency.	1. Financial regulators include mobile payment system in any implementation plans for currency redenomination and handle them as they do deposits in the banking system.	• Implies account provider capacity to adjust the nominal value of items in transit during a redenomination. • Regulatory requirements mandating that capacity may send a message to the market that redenomination is likely, possibly undermining			X				X	X	X

Mobile Financial Services Risk Matrix: National Regulators

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
					confidence in the national currency. • May complicate the public education process during redenomination by bunching the impact for people who may be less financially sophisticated.									
				2. No regulatory action	• An incentive is created for moving money into or out of the mobile payment system around redenomination to benefit from arbitrage opportunity - could bankrupt the account provider and deplete the trust funds so that only the first to cash out could be paid.									
7.20	Regulator unreasonably blocks a particular service model.	The extraordinary success of some cell phone based systems have raised concerns in other countries based on "loss of control" over uncertain risks or resistance to competition with exiting formal financial institutions.	Enable all proven business models within a predictable legal and regulatory environment.	1. Limit mobile financial services to bank based models requiring users to pass all transactions over individual bank accounts	• Restricts usage to those who have reason to have a full bank account, effectively excluding the poor. • Little or no developmental impact.		X	X	X		X	X	X	X
				2. Allow both cell phone company and bank based services.	• Opens access to financial services to the poor through low cost payment services that do not require a full bank account – significant developmental impact. • Acts as a catalyst for building confidence in the financial system and in using formal financial services rather than dependence on cash.									
7.21	Interest income on service users' trust funds is improperly allocated to the detriment of service users.	The trustee will invest the trust funds in interest bearing instruments, such as government securities or interest bearing deposit or savings accounts with	Ensure that the benefit of income generated by the trust funds is most efficiently allocated back to the benefit of service users, based on the	1. Require that interest income be credited back to individual service user's accounts, based on the average amounts in transit during the period.	• Adds an additional level of complexity to the account provider's service by requiring calculation of the interest and crediting back to the service users' individual accounts,		X	X			X	X		

Mobile Financial Services Risk Matrix: National Regulators

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		financial intermediaries. So either the trustee, the account provider or the service users will benefit from this interest.	account provider's business model		adding to the cost of providing the service. • Complicates account reconciliation for service users by adding transactions not originated by service users. • Could encourage service users to leave funds "on deposit" in lieu of opening a formal savings account, reducing incentives to move savings into the formal financial sector.									
				2. Allocate some or all of the interest income to the trustee to cover trustee fees for managing the trust account.	• Motivates trustees to provide the trustee services. • Eliminates pass back of trustee fees to the account provider. • Implies monitoring by the account provider to avoid over-charging by the trustee. • May motivate trustee to reach for higher yield, higher risk investments, implying a need for regulatory oversight of investments.									
				3. Allocate some or all of the interest income to the account provider as additional revenue.	• Augments the revenue stream for the account provider, in principle enabling lower direct service fees to service users. • Benefit will vary with market interest rates.									

International Regulatory Issues

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
8.1	Heightened difficulty tracking and prosecuting illicit cross-border transactions given the new cross border payment capability with a national regulatory framework and enforcement mechanism.	Illicit financial activities, such as money laundering and the financing of terrorist activities, can be facilitated (and more difficult to prevent) when cross-border transactions are allowed where different regulatory systems are in place. Incompatible regulation can prevent, or make more complicated, identifying suspicious transactions, investigating the transactions, as well as prosecuting and convicting those involved in illicit transactions. This risk applies to any cross border payment system, not just those using mobile financial services.	Regional harmonization of the legal and regulatory framework for mobile financial services,	1. Regulatory authority harmonizes mobile financial service definitions in the context of FATF Special Recommendation VII (SRVII) within their own AML/CFT regimes.	• Harmonization with FATF standards facilitates tracking and prosecution. • New requirement imposes a new cost on stakeholders	X	X		X		X	X	X	X
				2. Harmonize information sharing among regulatory authorities.	• In order to track illicit cross-border transactions as geographic borders diminish in importance, the ability for law enforcement entities and regulators to work collaboratively is critical.									
				3. No regulatory action	• Continued, or possibly, increased ability of terrorist and/or criminal elements to leverage mobile payment network and avoid prosecution for illicit cross-border financial crimes. • However, transaction size and volume limits mitigate this risk, particularly versus other payment systems that can handle larger amounts.									
8.2	Small-scale traders face a theft risk due to their 'cash & carry' business.	Currently, in-country and regional traders conduct a cash and carry business that relies on cash settlement of trade transactions outside of any financial institution, with no audit trails and with theft risk to the traders.	Enable traders to use mobile payments to settle trade transactions involving larger amounts than are appropriate for personal remittances to reduce the theft risk and bring these trade transactions into the financial system. Enable the use of mobile payments for cross-border transactions.	1. Regulatory authorities prevent the larger transactions needed for traders or businesses via mobile payments.	• Regulatory authorities limit mobile payment system to small-scale personal transactions, limiting its usefulness for commerce. • Risk of mobile system use for ML/TF is limited by the small scale of transactions. • Traders continue to use cash for commerce and the risk of theft and lack of audit trails persists.			X						

International Regulatory Issues

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
				2. Regulatory authorities to allow for a separate user category for traders that allow for larger scale transactions.	• Regulatory authorities enable traders and businesses to use mobile payments through stepped user categories. • Implies higher level of KYC/CDD to contain the risk of mobile system use for ML/TF. • Risk of theft reduced by access to non-cash, mobile channel.									
				3. Regulatory authorities do not restrict transaction size.	• Regulatory authorities enable traders and businesses to use mobile payments as transaction limits do not restrict their capacity. • Risk of mobile system use for ML/TF increases, as large transactions enabled without segregated from general consumer transactions. • Risk of theft reduced by access to non-cash, mobile channel.									
8.3	Cross-border payments through a mobile financial service could be seen as bypassing a country's foreign exchange restrictions.	Convenience and safety may encourage cross-border traders to tap into a neighboring country's mobile payment system to settle trade payments. If both buyer and seller use the same system, then the funds will remain in the country hosting the buyer's system. The seller will either have to buy goods or services using the e-money from the system host country, or cash out through an exchange office	Enable use of mobile financial services in cross border trade transactions without unreasonable foreign exchange restrictions.	1. Regulatory authorities prohibit foreign exchange conversion using mobile financial services.	• Cross border traders limited to using cash or a currency both buyer and seller can use. • May encourage use of a larger neighboring country's currency, as for cash transactions, lowering acceptance of the domestic currency.	X	X	X		X	X	X	X	X
				2. Regulatory authorities specifically allow foreign exchange conversion using mobile financial services.	• Facilitates monitoring of foreign exchange flows. • Implies development of linkages between neighboring services that									

International Regulatory Issues

#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		that can use the buyer's currency of origin. If a foreign exchange conversion facility is built into the service, then transactions that otherwise would be settled in cash move into electronic form.			enable currency conversion.									
				3. No Regulatory Action	• Market for mobile financial services across borders may be impeded by lack of clarity on the potential regulatory response.									

Part III – Sample Transaction Flow Charts

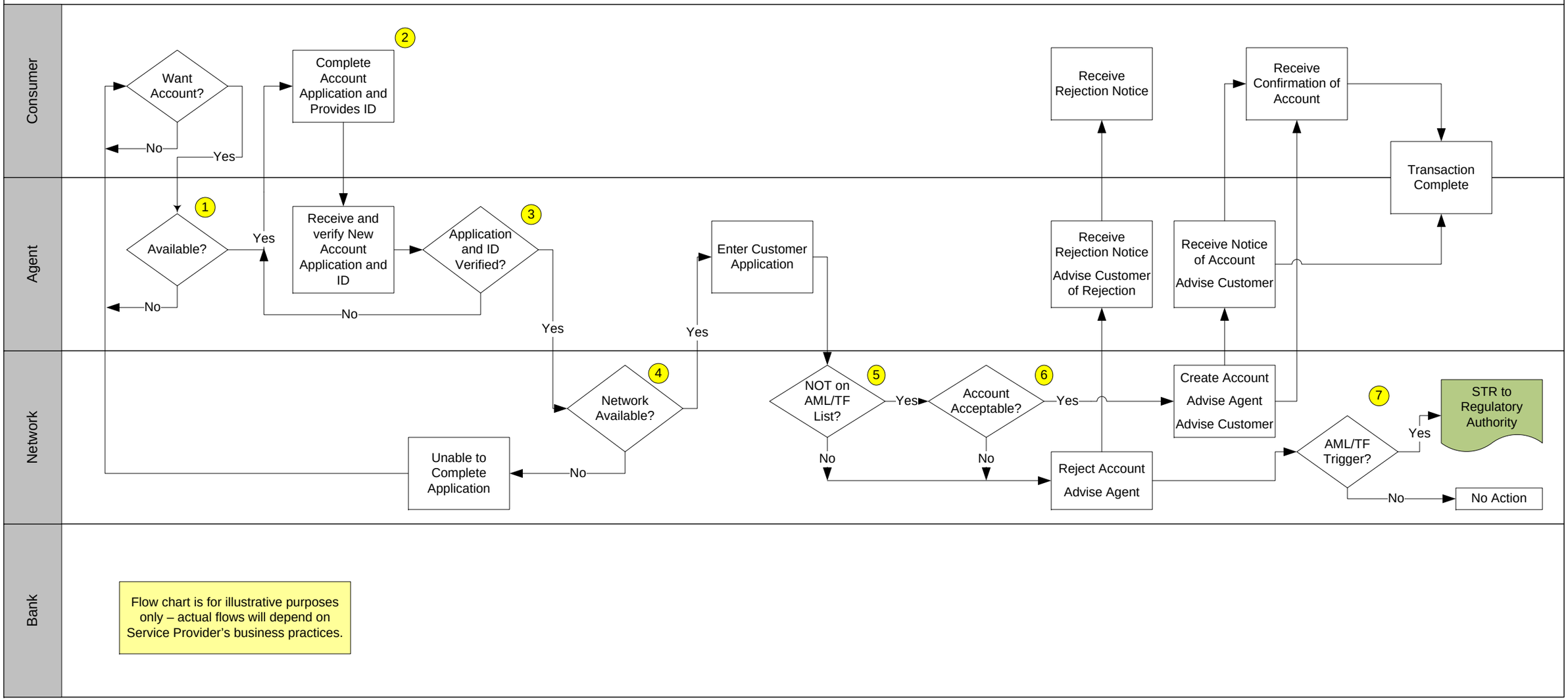
This Part II provides twelve sample transaction flows representing the most commonly used transactions in mobile financial services. The objective is not to be prescriptive on how these flows should be structured, since each account provider will have its own business model and its own transaction processing methodology. Rather, the intent of these samples is to show where in the most common transaction types the risks examined in Part I are likely to occur.

The samples provided are not exhaustive, nor do they necessarily reflect every risk involved - our understanding of the nature of these services and their implications to the regulator's risk management process is still evolving, and will continue to do so as the technology and the breadth of service offerings expands. The samples are:

1. Account Setup - MNO Model. This involves an individual with a cell phone applying through an agent for a payment account with a cell phone company that is providing payment services, such as Safaricom's M-PESA service in Kenya.
2. Cash In - MNO Model. This transaction flow represents an individual account holder buying e-money - depositing funds into his/her cell phone company based payment account - through the intermediary of a cell phone company agent.
3. Agent Cash In - MNO Model. Agents will typically have both sales and purchases transactions of e-money with cell phone clients, with corresponding cash transactions. This transaction flow represents an agent depositing the net surplus cash in the cell phone company trust account against purchase (re-stocking) of additional e-money to enable future sales to clients. The reverse transaction would be Agent Cash Out, where an agent sells back e-money to the cell phone company, in the process receiving the cash equivalent.
4. Cash Out - MNO Model, covers the situation where an account holder has received e-money, possibly as a gift from a relative, a salary payment, or a social subsidy payment from the government, and wishes to withdraw some or all of the funds through a cell phone company agent.
5. P2P In Network - MNO Model, shows how a payment from one cell phone account holder to another might work - for example from a family member working in a large town sending funds back to a family member in a rural area.
6. P2P in Network - Bank Model, demonstrates an account to account payment in a bank based system, where the cell phone is serving purely as a communications devise to transmit instructions and advices, but where the cell phone company is not involved in the execution of the underlying transaction. This example requires that both sender and recipient have established account relations with the same banking institution.
7. P2P Out of Network - MNO Model, shows how a payment would flow from a cell phone company client to a beneficiary who is a client of a competing cell phone company.
8. P2P Out of Network, No Account - MNO Model. In this example, an account holder of a cell phone company account provider initiates a payment to a beneficiary who does not have his/her own account, but can cash out through a cell phone company agent based on the cash out code provided.

The following four examples illustrate possible hybrid variations on some of the main transaction types in which a cell phone company serves as the communications vehicle, while a bank based agent network, including dedicated agents, retailers and/or branches of the bank, provide the customer interface.

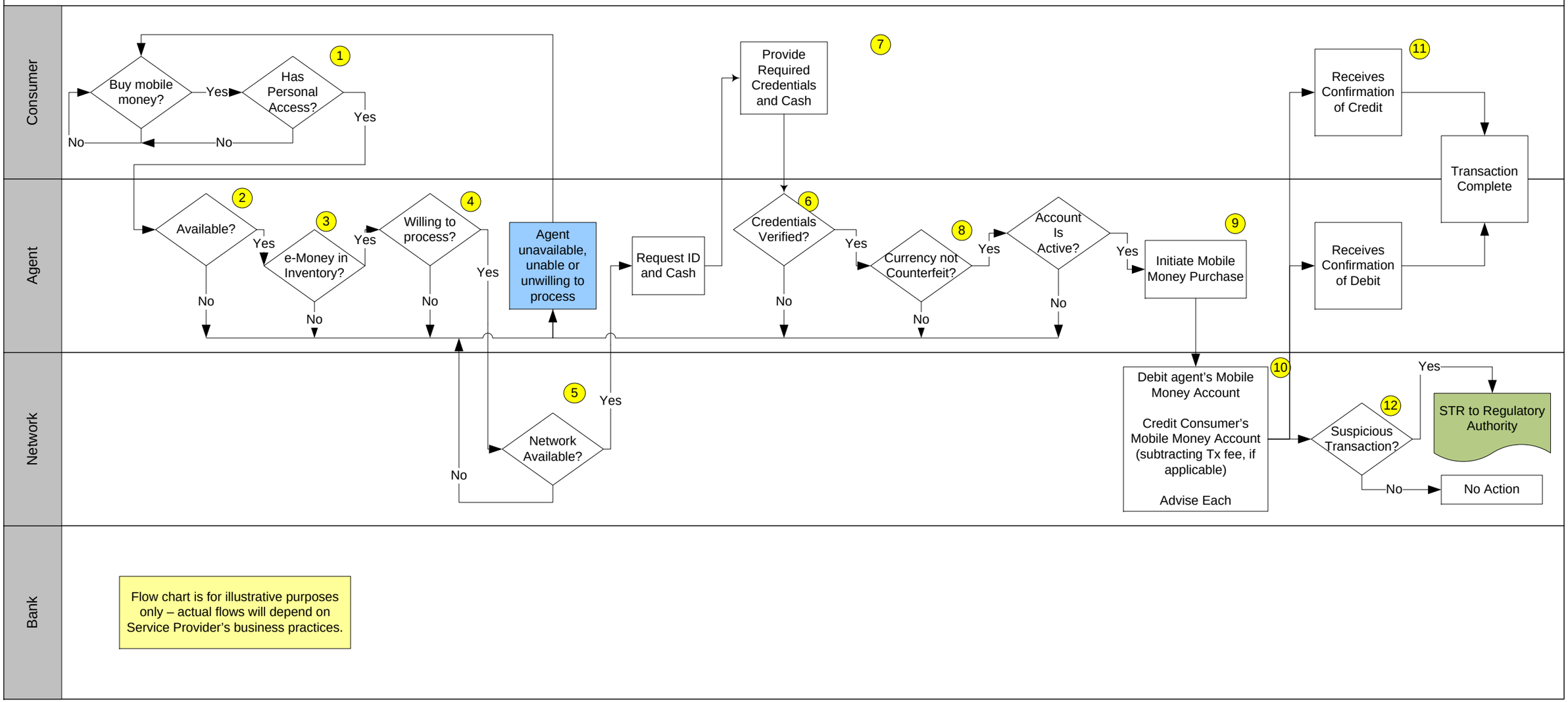
Account Setup – MNO Model



Risk Legend

1. 1.8 Agent unwilling to perform transaction for customer/Including
2. 1.18 Beneficial owners of stored value accounts cannot be determined in the event of illicit account activity when group accounts are used.
3. 1.1 Potential customer cannot access mobile payment services due to inability to prove his/her identity.
   1.6 Customer is charged unauthorized fee by agent.
   1.18 Beneficial owners of stored value accounts cannot be determined in the event of illicit account activity when group accounts are allowed.
   4.2/4.3/5.1/7.3 Including, provider fails to adequately select, train and supervise agents and superagents.
4. 4.6/7.9/7.15/7.16 System availability cannot be maintained by provider./Privately managed payment network suspends operations or collapses, disrupting service.
5. 1.3 Customer's identity is stolen and used to conduct fraudulent transactions
   4.2/4.3/7.1/7.3 Including, provider fails to adequately select, train, and supervise agents and super agents/Provider or agent failing to meet regulatory requirements/Illicit financial activities enabled by weak KYC/CDD requirements/enforcement.
   1.18 Beneficial owners of stored value accounts cannot be determined in the event of illicit account activity when group accounts are used..
6. 4.1/4.5/7.10/7.11 Including, service provider employee sets up accounts on the system with balances not backed by receipt of currency and funding of trust account.
7. 4.5/7.2/7.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.

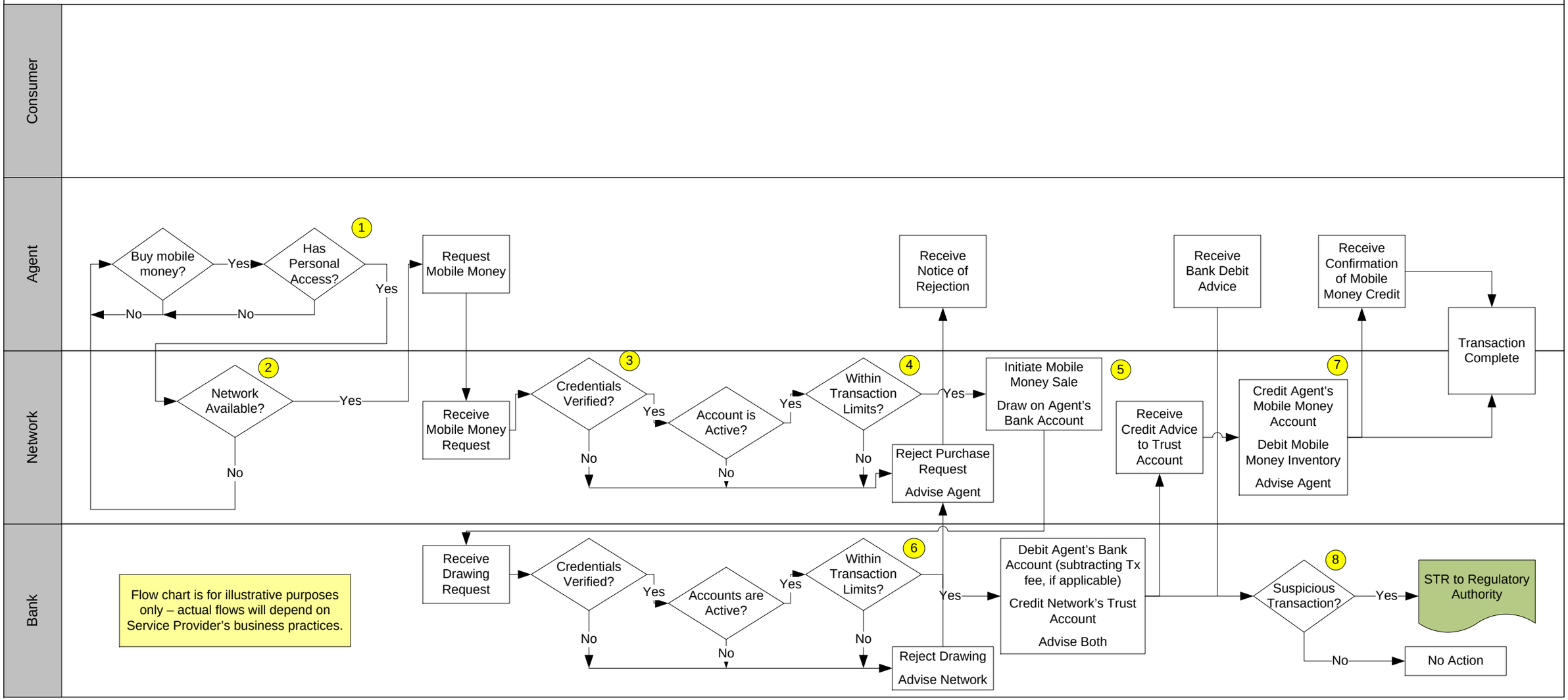
Cash in – MNO Model



Risk Legend

1. 1.10 Customer cannot purchase mobile money due to lack of personal access
2. 1.7 Customer cannot purchase mobile money due to lack of agent availability.
3. 1.9/4.7 Including, customer can't purchase mobile money due to lack of agent inventory of m-money.
   3.3 Agent is robbed.
   3.7 Provision of credit to agents by non-bank actors.
4. 1.8/4.2 Including, agent unwilling to perform transaction for customer.
5. 1.11/4.6/7.9/7.15/7.16 Including, customer cannot access account due to System availability cannot be maintained by provider/Privately managed payment network suspends operations or collapses, disrupting services.
6. 1.2 Existing customer cannot access mobile payment services due to inability to prove his/her identity.
   1.6 Customer is charged unauthorized fee by agent.
   4.2/4.3/7.1/5.3 Including, provider fails to adequately select, train, and supervise agents and super agents/Illicit financial activities enabled by weak KYC/CDD requirements/enforcement.
7. 1.16 Consumers have the ability to fund the transaction using a credit facility which will increase their debt.
8. 3.5/7.17 Including, agent takes in cash that proves to be counterfeit.
9. 1.16 Customer is charged unauthorized fees by agent.
10. 1.18/1.19 Including, government decides to tax transactions to raise funds, increasing the cost.
    4.1/ 4.5/7.10/7.11 Provider employee manipulates customer e-money balances for financial gain.
    4.5/7.2/7.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.
11. 3.2 Agent receives cash from client but fails to provide/transfer the e-money
12. 7.2/7.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.

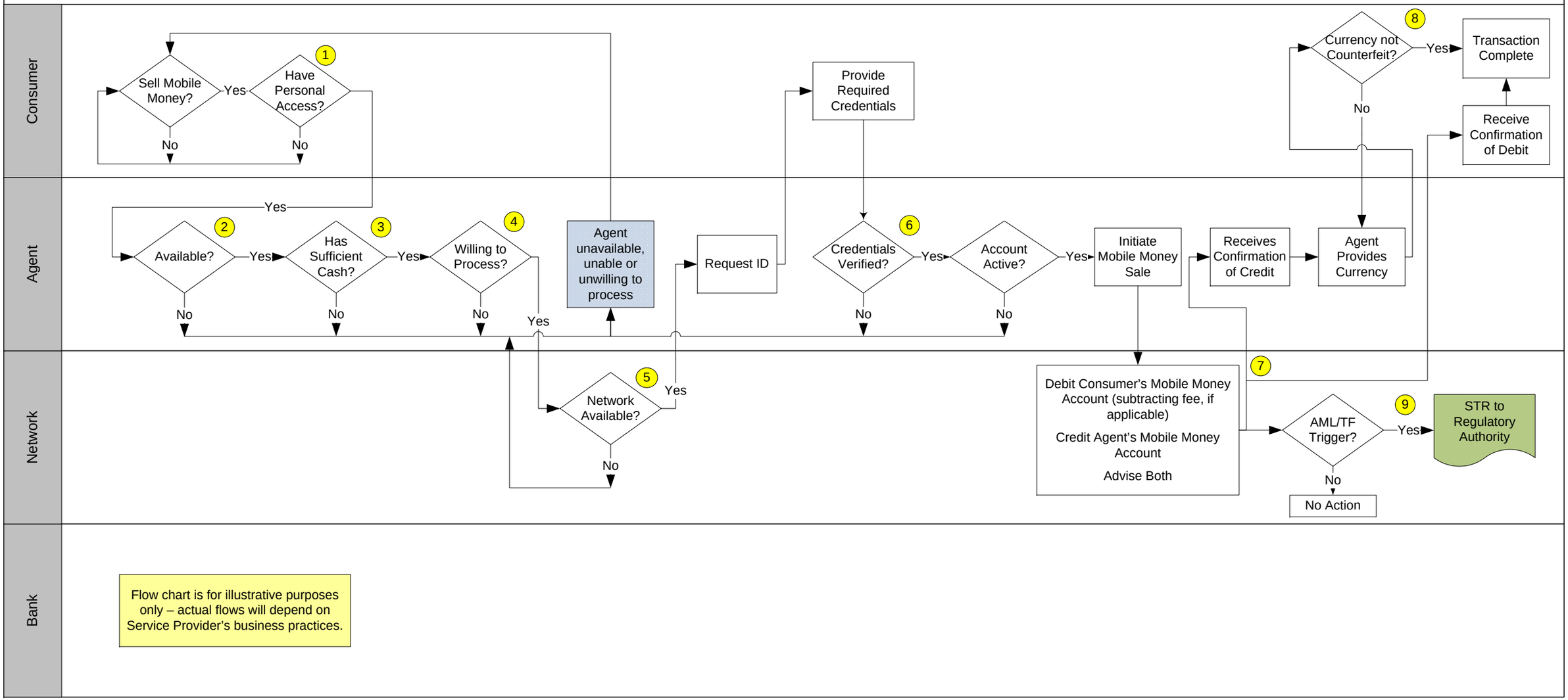
Agent Cash In – MNO Model



Risk Legend

1. 1.10 Agent cannot purchase mobile money due to lack of personal access
2. 1.11/4.6/7.9/7.15/7.16 Including, agent cannot access account due to system availability.
3. 1.2 Existing agent cannot access mobile payment services due to inability to prove his/her identity.
4. 7,14 Illicit actors conduct high volume transactions using multiple accounts, bypassing monitoring systems before regulators step in.
5. 3.7 Provision of credit to agents by non-bank actors.
6. 7,14 Illicit actors conduct high volume transactions using multiple accounts, bypassing monitoring systems before regulators step in.
7. 1.19 Government decides to tax transactions to raise funds, increasing the cost. 4.1/ 4.5/7.10/7.11 Provider employee manipulates customer e-money balances for financial gain. 4.5/7.2/7.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.
8. 7.2/7.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.

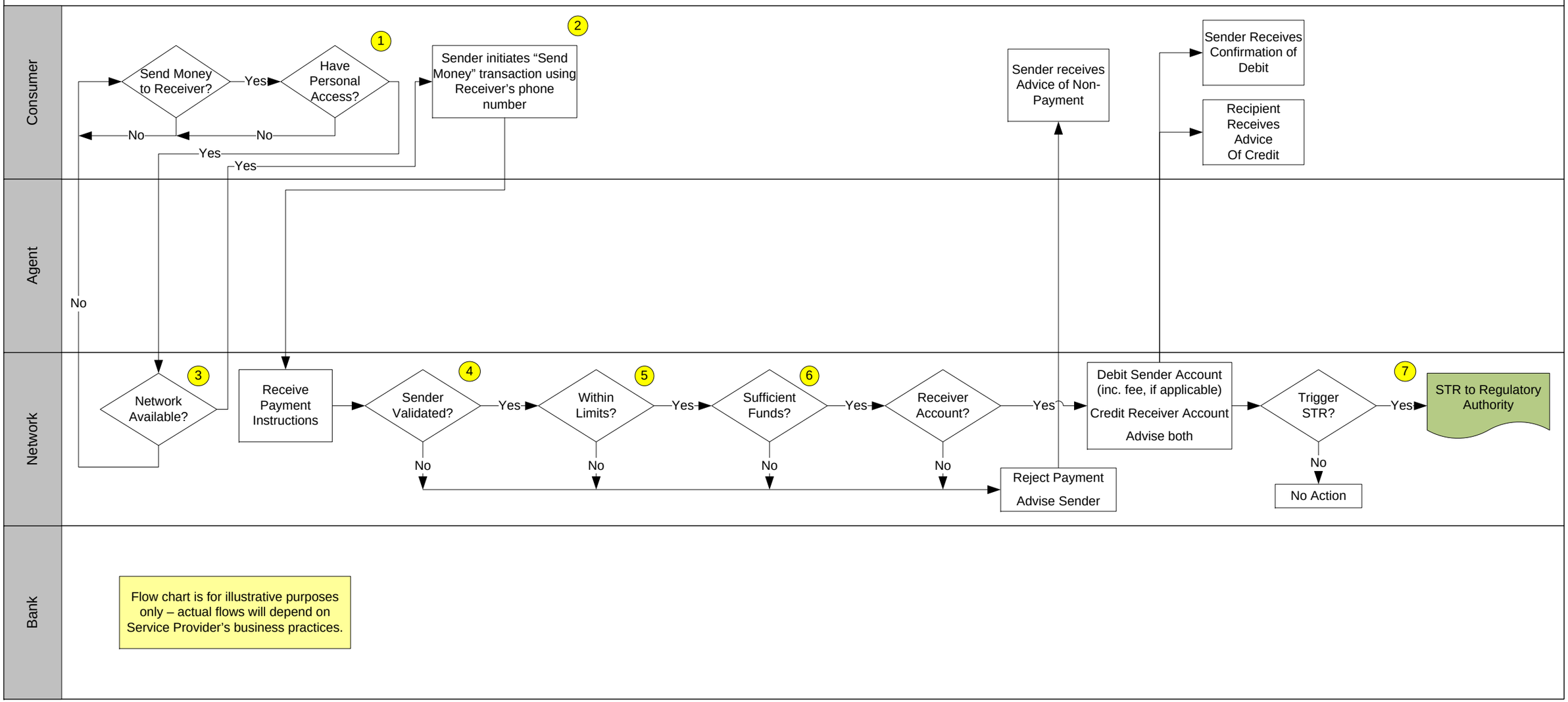
Cash Out – MNO Model



Risk Legend

1. 1.10 Customer cannot access cash from mobile money account due to lack of personal access.
2. 1.7 Customer cannot access cash from mobile money account due to lack of agent availability.
3. 1.9/4.7/5.2/5.3 Including, customer cannot access cash from mobile money account due to lack of agent liquidity (in mobile money).
   3.3/3.4 Including, agent is robbed.
   3.7 Provision of credit to agents by non-bank actors.
4. 1.8 Agent unwilling to perform transaction for customer.
   2.1 Merchants unable to easily convert mobile money into cash, limiting their flexibility to run their bus.
   4.2 Provider fails to adequately train and supervise agents and super agents.
5. 1.11/4.6/7.9/7.15/7.16 Including, customer cannot access account due to System availability cannot be maintained by provider/Privately managed payment network suspends operations or collapses, disrupting services.
6. 1.2 Existing customer cannot access mobile payment services due to inability to prove his/her identity.
   1.3 Customer's identity is stolen and used to conduct fraudulent transactions
   4.2/4.3/7.1/7.3 Including, provider fails to adequately select, train, and supervise agents and super agents/Illicit financial activities enabled by weak KYC/CDD requirements/enforcement
7. 1.4 Customer's account credentials are improperly released.
   1.13/1.14/1.15/1.16 Including, customer loses balance due to failure of a bank holding trust fund, or a similar situation where trust fund is compromised.
   1.6/1.19 Including, customer is charged unauthorized fee by agent
   4.5/7.2/7.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.
8. 3.6/7.18 Agent pays out cash that proves to be counterfeit.
9. 7.2/7.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.

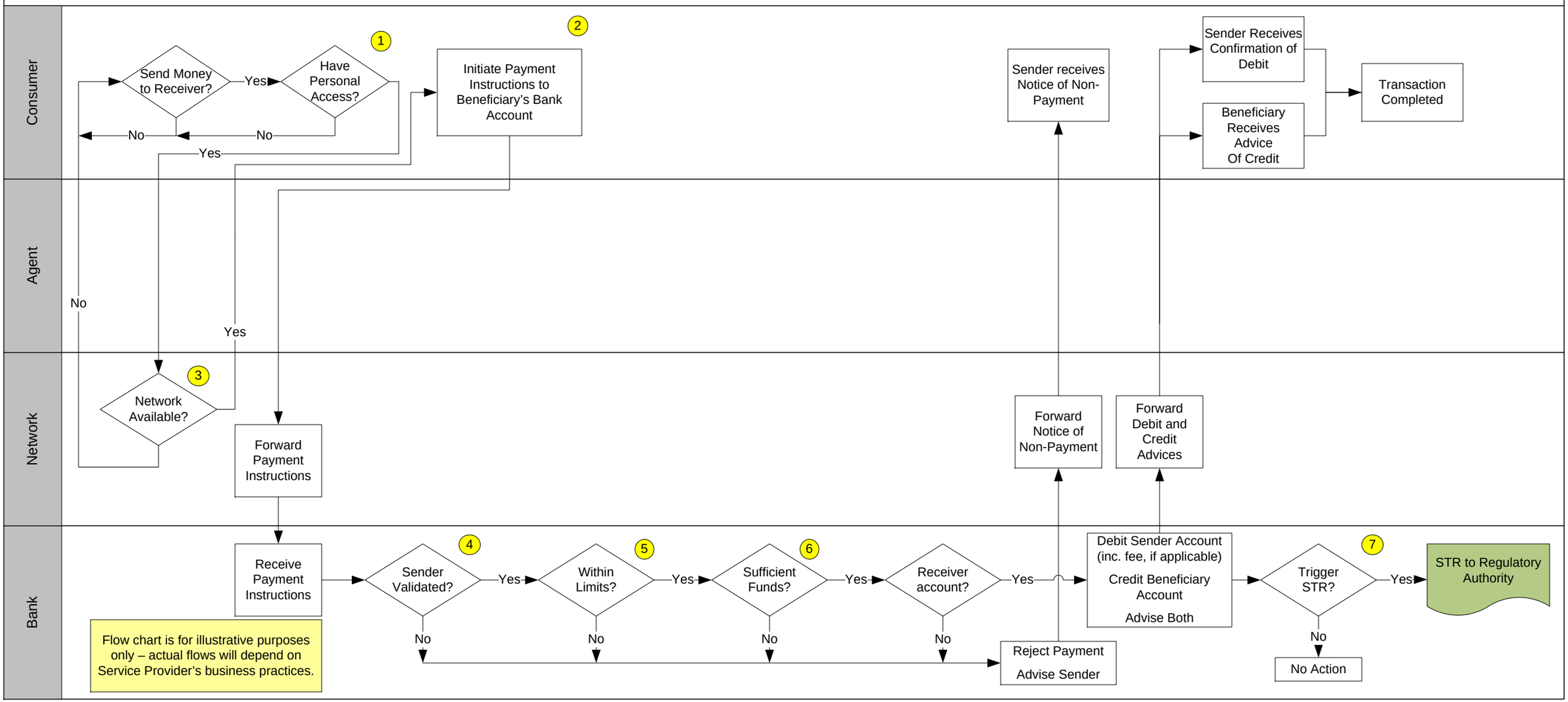
P2P – MNO Model, In Network



Risk Legend

1. 1.10 Customer can not access cash from mobile money account due to lack of personal access.
2. 1.16/8.2 Consumers may be pressured into drawing on credit lines to fund payments to relatives. Small-scale traders face a theft risk due to their 'cash & carry' business4.6/7.9/7.15/7.16 Including, customer cannot access account due to System availability cannot be maintained by provider/Privately managed payment network suspends operations or collapses, disrupting services.
3. 4.6/7.9/7.15/7.16 Including, customer cannot access account due to system failure, system availability cannot be maintained by provider, or privately managed payment network suspends operations or collapses, disrupting services.
4. 1.13 / 1.14/1.15 Including, customer loses balance due to failure of a bank holding trust fund, or a similar situation where trust fund is compromised
5. 1.4 Customer's account security credentials are released improperly
6. 7.14 Illicit actors conduct high volume transactions using multiple accounts, bypassing monitoring systems, before regulators intervene
7. 7.2/7.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.

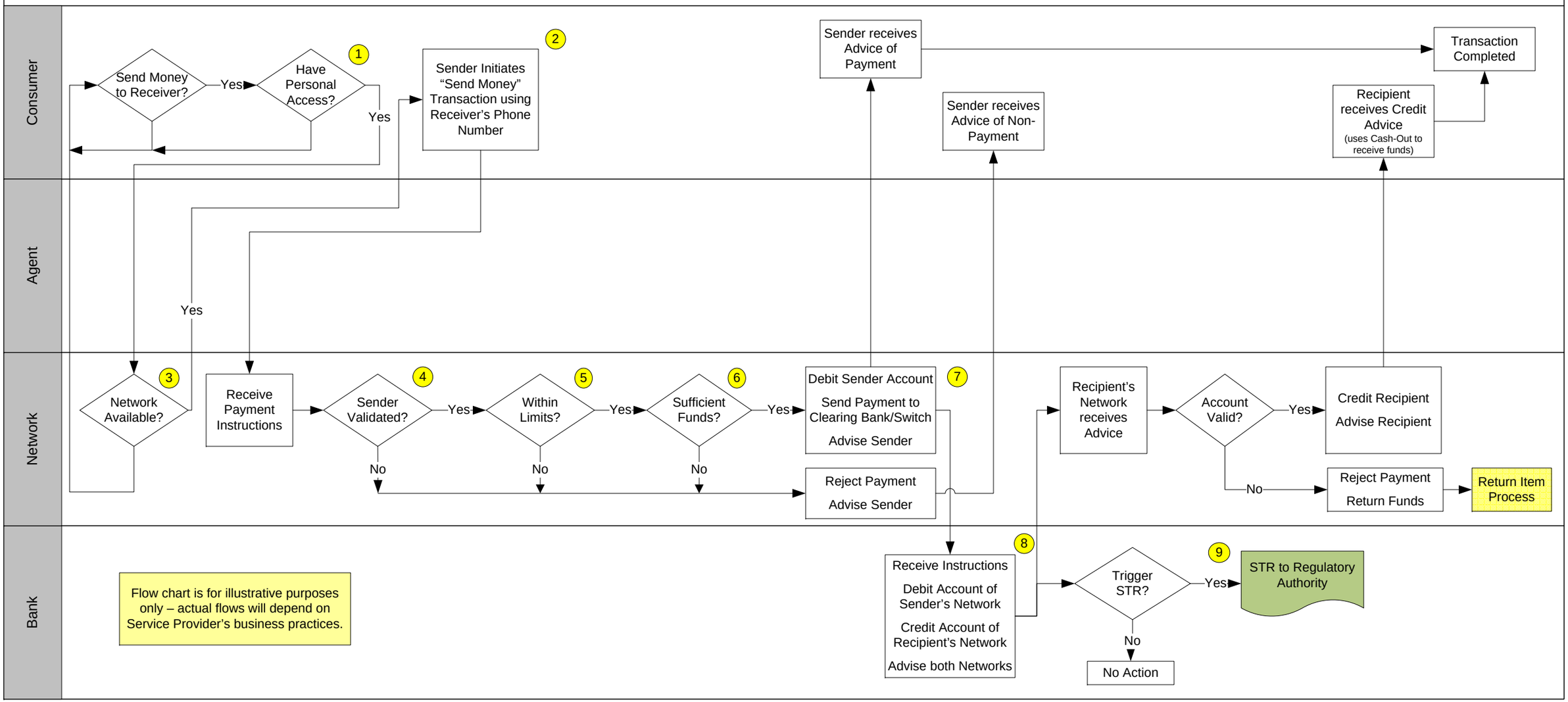
P2P – Bank Model, In Network



Risk Legend

1. 1.10 Customer can not access cash from mobile money account due to lack of personal access.
2. 4.6/7.9/7.15/7.16 Including, customer cannot access account due to System availability cannot be maintained by provider/Privately managed payment network suspends operations or collapses, disrupting services.
3. 8.2 Small-scale traders face a theft risk due to their 'cash & carry' business.
4. 1.13 / 1.14/1.15/1.16 Including, customer loses balance due to failure of a bank holding trust fund, or a similar situation where trust fund is compromised
5. 1.4 Customer's account security credentials are released improperly
6. 7.14 Illicit actors conduct high volume transactions using multiple accounts, bypassing monitoring systems, before regulators intervene
7. 7.2/5.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.

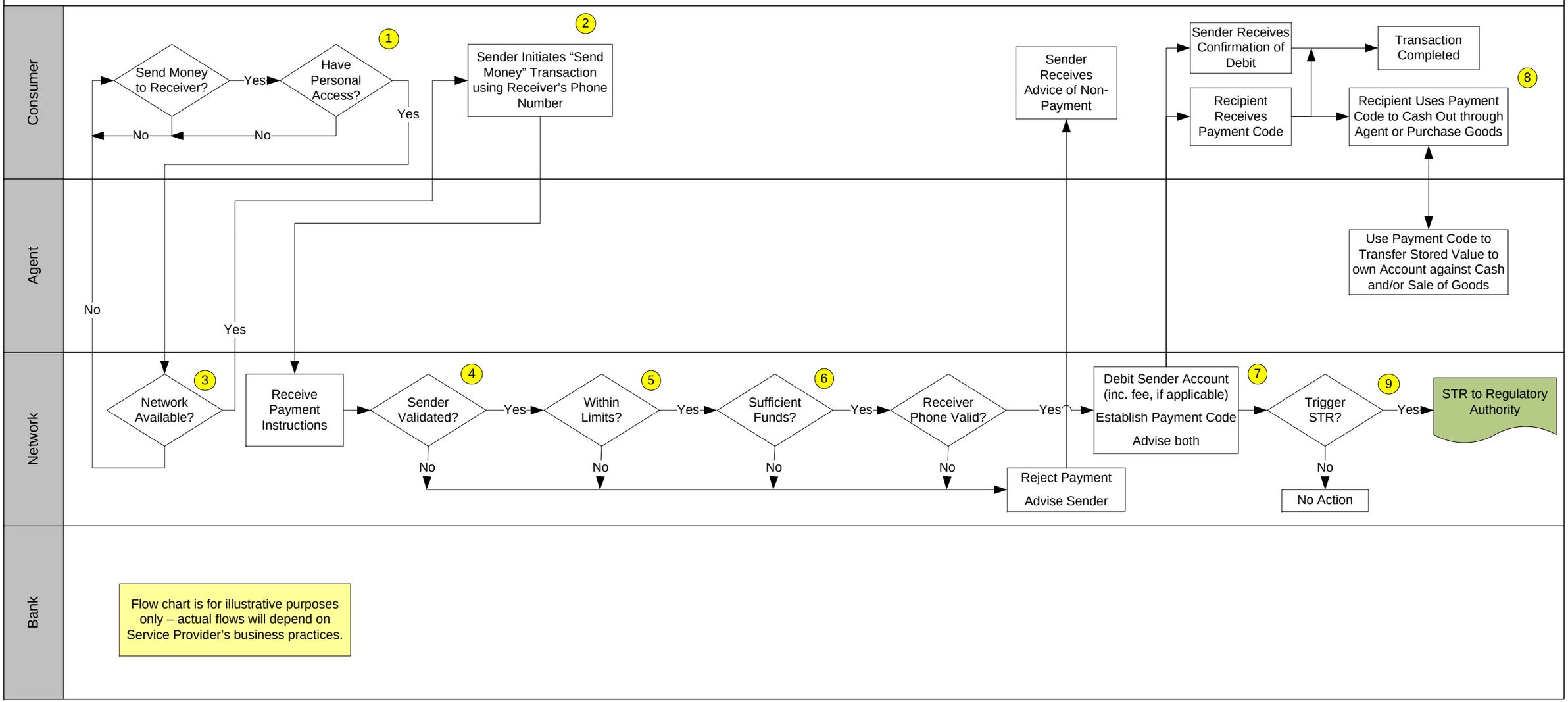
P2P – MNO Model, In Network Consumer to Out-of-Network Consumer



Risk Legend

1. 1.10 Customer cannot access cash from mobile money due to lack of personal access.
2. 8.2 Small-scale traders face a theft risk due to their 'cash & carry' business.
3. 1.11/4.6/7.9/7.15/7.16 Including, system availability cannot be maintained by provider / privately managed payment network suspends operations or collapses, disrupting services.
4. 1.4 Customer's account credentials are released improperly
5. 7.14 Illicit actors conduct high volume transactions using multiple accounts, bypassing monitoring systems before regulators can step in.
6. 1.13/ 1.14/1.15/1.16 Including, customer loses balance due to failure of a bank holding trust fund, or a similar situation where trust fund is compromised.
7. 1.12/5.13 Lack of network interoperability prevents consumers from transacting with desired party.
   7.2/5.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.
   7.19 Including, currency redenominated while in transit.
8. 1.6/1.19 Government decides to tax transactions to raise funds increasing the marginal cost.
   7.2/7.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.
   5.19 Currency redenominated while in transit.
9. 7.2/7.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.

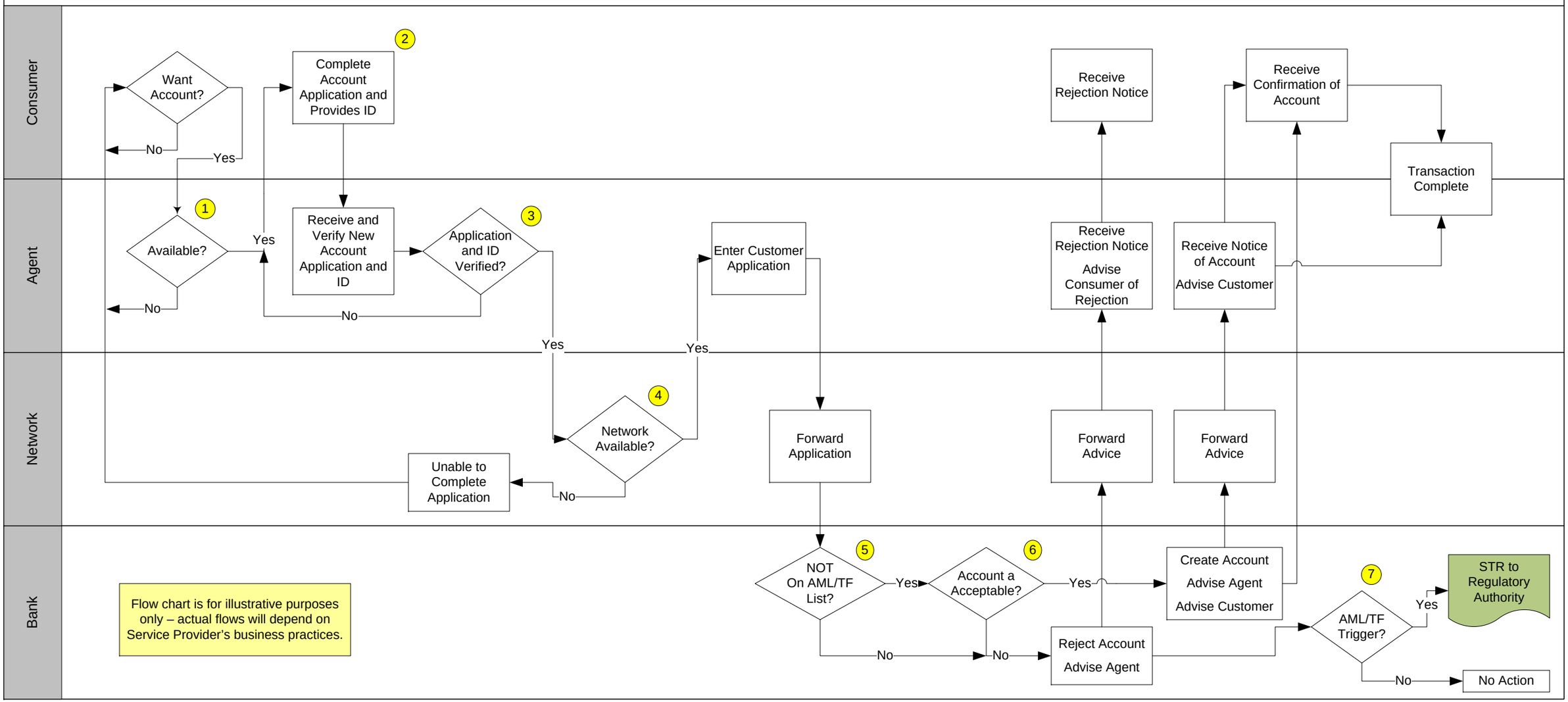
P2P – MNO Model, In Network Consumer to Out-of-Network Consumer – No Account



Risk Legend

1. 1.10 Customer cannot access cash from mobile money due to lack of personal access.
2. 8.2 Small-scale traders face a theft risk due to their 'cash & carry' business.
3. 1.11/4.6/7.9/7.15/7.16 Including, customer cannot access account due to personal access issues/ System availability cannot be maintained by provider/Privately managed payment network suspends operations or collapses, disrupting services.
4. 1.4 Customer's account credentials are released improperly
5. 7.14 Illicit actors conduct high volume transactions using multiple accounts, bypassing monitoring systems before regulators can step in.
6. 1.13/ 1.14/1.15/1.16 Including, customer loses balance due to failure of a bank holding trust fund, or a similar situation where trust fund is compromised.
7. 7.2/7.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.
   5.19Including, currency redenominated while in transit.
   1.6/1.19 Government decides to tax transactions to raise funds increasing the marginal cost.
   7.2/7.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.
   7.19 Currency redenominated while in transit.
8. 1.7 Customer cannot access mobile money account due to lack of agent availability
   1.9/4.4//4.7/5.2/5.3 Customer cannot access cash from mobile money account due to lack of agent liquitdity.
   3.7 Provision of credit to agents by non-bank actors
   3.3/3.4 Including, agent is robbed.
   1.8/4.2 Including, agent unwilling to perform transaction for customer.
   4.2/4.3/7.1/7.3 Including, provider fails to adequately select, train, and supervise agents and super agents/Illicit financial activities enabled by weak KYC/CDD requirements/enforcement.
   3.6/7.18 Agent pays out cash that proves to be counterfeit.
9. 7.2/7.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.

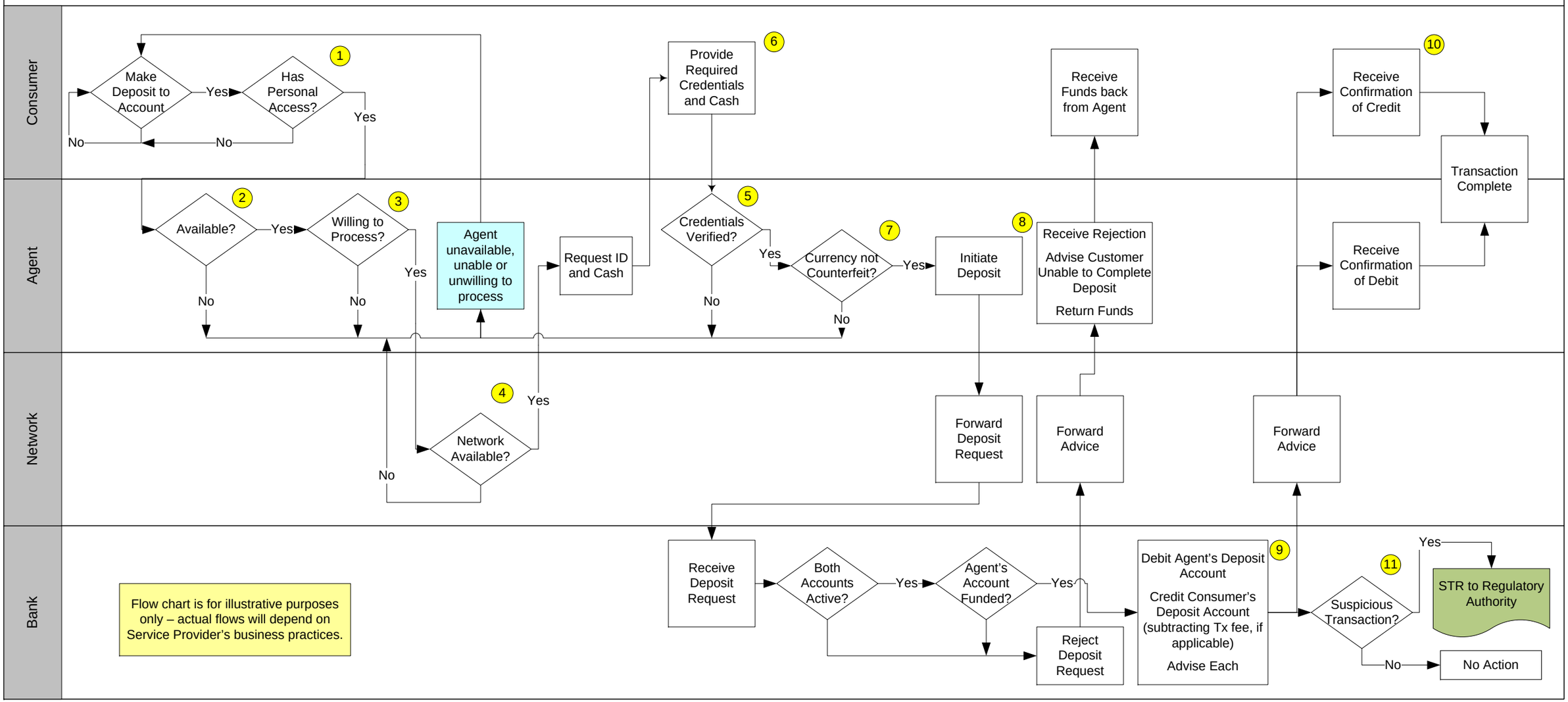
Account Setup – Hybrid Model



Risk Legend

1. 1.8 Agent not available or unwilling to perform transaction for customer.
2. 1.18 Beneficial owners of stored value accounts cannot be determined in the event of illicit account activity when group accounts are used.
3. 1.1 Potential customer cannot access mobile payment services due to inability to prove his/her identity.
   1.6 Customer is charged unauthorized fee by agent.
   1.18 Beneficial owners of stored value accounts cannot be determined in the event of illicit account activity when group accounts are allowed.
   4.2/4.3/5.1/7.3 Including, provider fails to adequately select, train and supervise agents and superagents.
4. 4.6/7.9/7.15/7.16 System availability cannot be maintained by provider./Privately managed payment network suspends operations or collapses, disrupting service.
5. 1.3 Customer's identity is stolen and used to conduct fraudulent transactions
   4.2/4.3/7.1/7.3 Including, provider fails to adequately select, train, and supervise agents and super agents/Provider or agent failing to meet regulatory requirements/Illicit financial activities enabled by weak KYC/CDD requirements/enforcement.
   1.18 Beneficial owners of stored value accounts cannot be determined in the event of illicit account activity when group accounts are used..
6. 4.1/4.5/7.10/7.11 Including, service provider employee sets up accounts on the system with balances not backed by receipt of currency and funding of trust account.
7. 4.5/7.2/7.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.

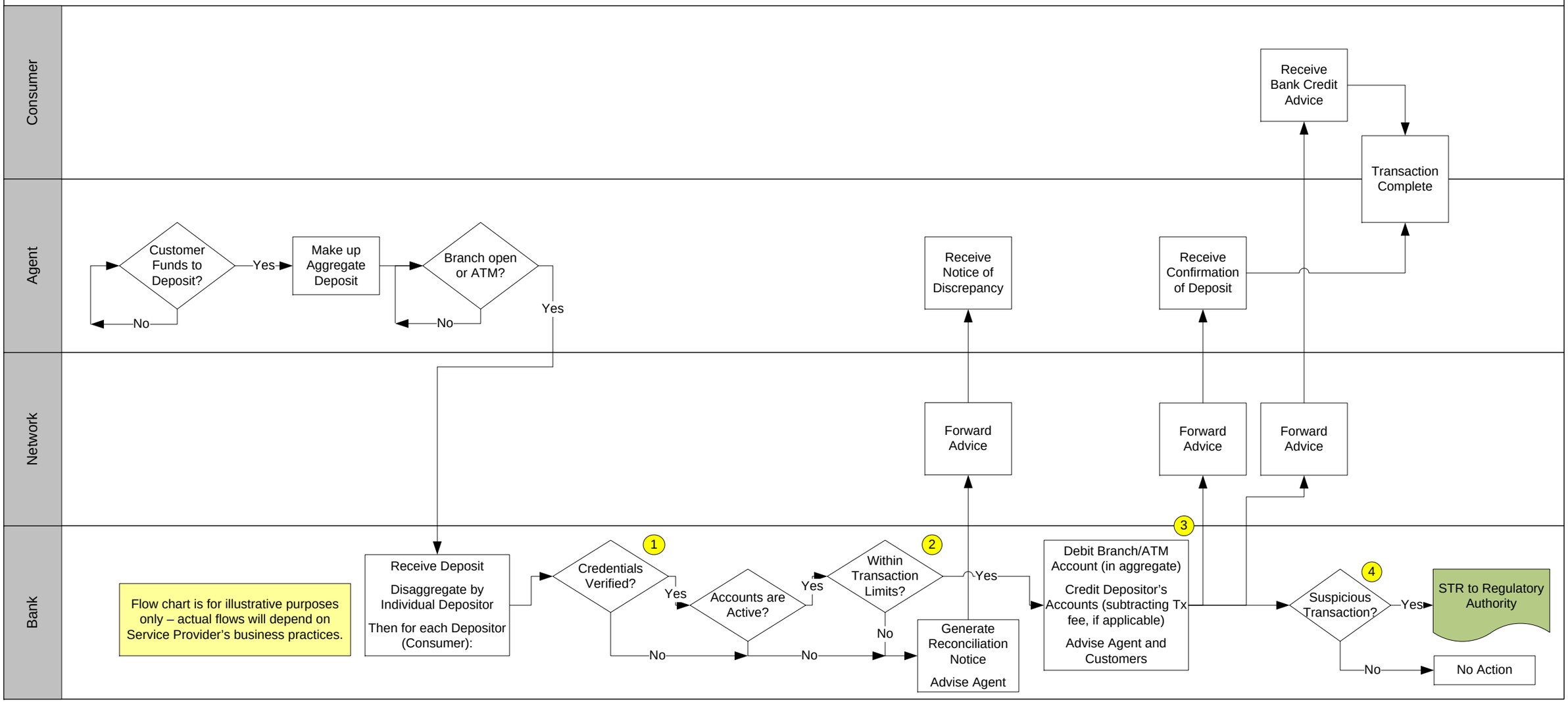
Cash In – Hybrid Model



Risk Legend

1. 1.10 Customer cannot purchse mobile money due to lack of personal access
2. 1.7 Customer cannot purchase mobile money due to lack of agent's availability.
3. 1.8/4.2 Including, agent unwilling to perform transaction for customer.
   Agent may know it does not have sufficient funds on deposit or credit line with the bank
4. 1.11/4.6/7.9/7.15/7.16 Including, customer cannot access account due to System availability cannot be maintained by provider/Privately managed payment network suspends operations or collapses, disrupting services.
5. 1.2 Existing customer cannot access mobile payment services due to inability to prove his/her identity.
   1.6 Customer is charged unauthorized fee by agent.
   4.2/4.3/7.1/5.3 Including, provider fails to adequately select, train, and supervise agents and super agents/ Illicit financial activities enabled by weak KYC/CDD requirements/enforcement.
6. 1.16 Consumers have the ability to fund the transaction using a credit facility which will increase their debt.
7. 3.5/7.17 Including, agent takes in cash that proves to be counterfeit.
8. 1.16 Customer is charged unauthorized fees by agent.
9. 1.18/1.19 Including, government decides to tax transactions to raise funds, increasing the cost.
   4.1/ 4.5/7.10/7.11 Provider employee manipulates customer e-money balances for financial gain.
   4.5/7.2/7.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.
10. 3.2 Agent receives cash from client but fails to provide/transfer the e-money
11. 7.2/7.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.

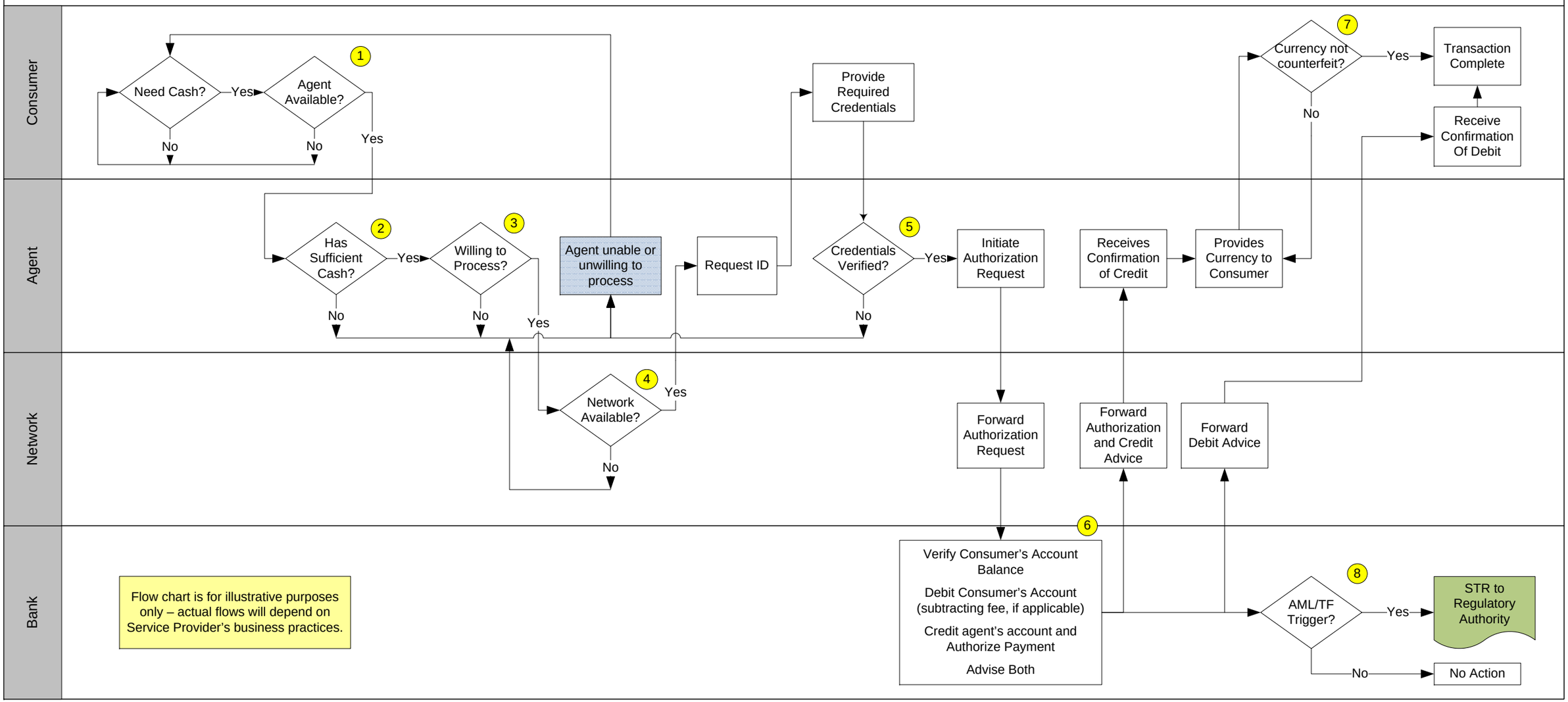
Agent Cash In – Hybrid Model



Risk Legend

1. 1.2 Existing agent cannot access mobile payment services due to inability to prove his/her identity.
2. 7,14 Illicit actors conduct high volume transactions using multiple accounts, bypassing monitoring systems before regulators step in.
3. 1.19 Government decides to tax transactions to raise funds, increasing the cost.
   4.1/ 4.5/7.10/7.11 Provider employee manipulates customer e-money balances for financial gain.
   4.5/7.2/7.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.
4. 7.2/7.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.

Cash Out – Hybrid Model



Risk Legend

1. 1.7 Customer cannot access cash from mobile money account due to lack of agent availability.
2. 1.9/4.4/4.7/5.2/5.3 Including, customer cannot access cash from mobile money account due to lack of agent liquidity (in mobile money).
   3.3/3.4 Including, agent is robbed.
   3.7 Provision of credit to agents by non-bank actors.
3. 1.8 Agent unwilling to perform transaction for customer.
   2.1 Merchants unable to easily convert mobile money into cash, limiting their flexibility to run their bus.
   4.2 Provider fails to adequately train and supervise agents and super agents.
4. 1.11/4.6/7.9/7.15/7.16 Including, customer cannot access account due to System availability cannot be maintained by provider/Privately managed payment network suspends operations or collapses, disrupting services.
5. 1.2 Existing customer cannot access mobile payment services due to inability to prove his/her identity.
   1.3 Customer's identity is stolen and used to conduct fraudulent transactions
   4.2/4.3/7.1/7.3 Including, provider fails to adequately select, train, and supervise agents and super agents/Illicit financial activities enabled by weak KYC/CDD requirements/enforcement
6. 1.4 Customer's account credentials are improperly released.
   1.13/1.14/1.15/1.16 Including, customer loses balance due to failure of a bank holding trust fund, or a similar situation where trust fund is compromised.
   1.6/1.19 Including, customer is charged unauthorized fee by agent
   4.5/7.2/7.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.
7. 3.6/7.18 Agent pays out cash that proves to be counterfeit.
8. 7.2/7.4/7.5/7.6/7.8/8.1 Including, inadequate transaction records impair investigation of fraud or criminal activity.

Risk-based Policy Matrix – Appendix

PART III - Appendix

Part III, the appendix to the policy matrix, incorporates a policy narrative and market examples to accompany each risk. The policy narrative provides some context to the select policy options noted. More importantly, the appendix presents market examples of how different countries are approaching these risks from a policy perspective. These examples provide insight into the diversity of policy actions, and how policies must be shaped to the environment of a given country.

Clearly, this document is a work in progress, as policies are constantly being implemented and modified around the world. We hope this effort helps to provide insights into the policy landscape for mobile financial services, and we welcome recommendations for additions or edits.

Risk-based Policy Matrix – Appendix

1.1. Risk (Consumers)

"Potential customers cannot access mobile payment services due to inability to prove his/her identity."

Description:
When initially registering for mobile financial services (MFS), the inability of the account provider or its agents to adequately verify the identity and personal information of applicants may block approval or access to mobile payment services.

National authorities may standardize national public identification (ID) to facilitate documentable measures to verify the customer and/or beneficial owner's identity when conducting transactional activity or establishing customer relationships. Financial institutions should implement risk management systems, in addition to normal due diligence measures, to determine if a customer is a politically exposed person (PEP). In the absence of a national customer ID, national authorities may provide for alternative ID instruments to comply with these requirements. All ID requirements should pay special attention to money laundering (ML) and terrorist financing (TF) threats that may arise from the anonymity of new or developing technologies.

According to the Financial Action Task Force (FATF), "the general rule is that customers should be subject to the full range of customer due diligence measures. However, there are circumstances in which it would be reasonable for a country to allow its financial institutions to apply the extent of the customer due diligence measures on a risk sensitive basis."[1] Since these recommendations do not elaborate the methods for establishing customer identity verification, mobile financial Account Providers with low-income clients have adopted a variety of regulatory approaches in different jurisdictions to insure financial inclusion. Regulatory approaches vary from those traditionally applied to branch banking clients to non-face-to-face alternatives, including biometrics. One risk to consumers could conceivably be that the very innovative ID methods employed for financial inclusion in the absence of a national ID, or with implementation of a national ID, is that it may be used in a manner to subvert privacy of the individual by authoritarian state regimes or their designees.

Objective:

- Know Your Customer (KYC)/Customer Due Diligence (CDD) guidelines to be set commensurate with the risk of the service.
- Subject to regulatory approval and verification of implementation.

Policy Table:

Options	Implications
1.National ID system: Authorities issue universal IDs, which are used for access to financial services	• Universality removes potential for exclusion of those desiring service. • Burden on national authorities to institute universal ID program may be unaffordable or beyond the existing infrastructure's legal, technical or political capacity to enforce.
2. Financial ID system: In the absence of universal ID, financial account providers (as a consortia) offer a financial ID with similar characteristics as a universal ID, but only issued to customers after meeting standard sector KYC requirements (e.g. a customer's phone # and SIM could be used as basic form of identification) Could link in with an industry ID system established for ensuring certainty of identity in credit bureaus, or with a tax ID system.	• With no universal national ID, the financial sector must rely on other forms of identity, which all customers may not have access to; however, they can set risk-based tiers to ensure access. • Coordination of various private actors in the financial sector could work through the bankers association and/or MFI association, possibly with leadership from the central bank.
3. Regulated KYC Requirements which leave implementation to institutions	• Each institution can interpret the requirements, which may allow various combinations of identification. Banks can set risk-based tiers to ensure access. • Each individual bank must establish a policy that meets regulatory requirement. • Reliance on existing forms of identification keeps cost low, but difference in policies across institutions creates some risk
4. No regulatory KYC requirements	• Each institution will determine requirements for account opening based on their perception of risk. Lack of regulatory requirement should keep barriers to access low. • Lack of requirement opens cross-organization risk for criminal activity.

Policy Narrative:
Policy makers should consider measures to strengthen and standardize the national identification systems. This single policy initiative will not only improve all financial Account Providers' ability to perform CDD/KYC as an effective tool for financial inclusion but, concomitantly, serves as a cornerstone of AML and CFT compliance measures. In lieu of national IDs, alternative instruments, such as financial IDs, should be considered and enumerated by appropriate State authorities. As World Bank authors aptly stately recently on this subject, "IDs cannot be linked to extensive verification procedures that increase the cost of compliance as a surrogate activity that belongs to the State. If the public infrastructure for IDs is not sufficiently secure, policy makers face the challenge of identifying which IDs could complement or substitute public IDs."

Risk-based Policy Matrix – Appendix

Market Examples:

- **Ghana:** at birth, national ID/financial ID include a 10-finger print scan, retinal scan, with data embedded in a passport ID. Each individual is assigned a national ID card and a bank account to receive all social services from cradle to grave. Rescanning/printing is done at age 16.
- **Zambia:** Universal National Registration Card (NRC) is available to all individuals at age 16 and used for all social service programs.
- **Tanzania –** "Corporate"- style registration of SIM cards for Village Savings and Loan program participant groups was verified, with group members designating an "officer" to act as the SIM disbursal authority for the group.
- **Korea:** a customer must be a bank account holder and visit the bank branch in person. To establish service, the customer must provide identification and fill in a form, including predefined details for funds transfers. The customer receives an e-banking password and ID. The financial institution issues a letter permitting the customer to obtain a SIM card from the TelCo; service is available only to post-paid individual subscribers. Foreign citizens must present a valid passport. TelCos retain a copy of the letter.
- **Hong Kong SAR of China**: customers register their SIM card face-to-face with the mobile phone operator in order to use mobile phone remittance services and are required to present their national ID. This ID is equipped with security features, such as a chip with biometric information.
- **Brazil**: known as Procon, an active network of government entities, rather than a consumer protection body, enforces Consumer Protection Codes in the financial sector. Additionally there is a newly created Ombudsman of the Central Bank of Brazil, which has the power to require prompt correction for non-compliance with the codes.[2]
- **South Africa**: non-face-to-face acquisition is permitted, but the m-FS provider must verify identity through other means, such as via confirming customer information with a third party data base.[3] A potential complicating factor is the Regulation of Interception of Communication-Related Information Act (RICA), which facilitates interception of information passed over electronic communications channels, such as mobile phones for combating crime. This act would require full KYC by operators and distributors of mobile phones to any individual to whom they provide a phone or a SIM card. Those provisions were suspended; the proposed implementation highlights differing and conflicting regulatory approaches that may affect an individual even within the same jurisdictions.
- **India**: The Reserve Bank of India allows for non face-to-face customer identification requirements, if there is certification of all documents presented and the first payment is effected through the customer's account with another bank. This may create barriers for remote account opening.[4]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		x	x		x	x	x	x

Risk-based Policy Matrix – Appendix

1.2. Risk (Consumers):

"Existing customer cannot access mobile payment services due to inability to prove his/her identity."

Description:
Verifying identity and personal information to protect customers when using mobile payment services may block access if the customer is not able to adequately prove his/her identity.

Objective:

- Restrict access to mobile financial services to those who can meet the same KYC requirement as account opening
- Ensure that appropriate risk based service access requirements are established at account opening
- Require that funds transferred to recipients who do not have established KYC credentials are returned to sender
- Require that Account Providers have acceptable procedures in place for replacing PIN and other provider ID

Policy Table:

Options	Implications
1. Restrict access to mobile financial services to those who can meet the same KYC requirement as account opening	• Requiring that agents repeat the same KYC requirements at the transaction level that are required at account opening is not practical. It would place an enormous time requirement on agents, and should not be necessary if the account opening procedure is implemented. (This would be the equivalent of requiring a photo ID check at the ATM.) • Regulatory authorities would not be able to effectively police such a requirement.
2. Ensure that appropriate risk based service access requirements are established at account opening	• Strict KYC requirement for agent transactions will create inconveniences for customers and create more bureaucracy for agents. • Expecting agents to conduct this due diligence for transactions of existing customers, especially during busy times is impractical. • Risk-based allowances ensure customers still have some access even without full KYC; yet the limits protect against fraud. (Option enables customers who have lost their ID to maintain some access) • Lower requirements for small, or low risk, transactions reduce regulatory burden for agents
3. Require that funds transferred to recipients who do not have established KYC credentials are returned to sender	• Risks unwarranted returns if agents do not want to complete pay-outs for non-KYC reasons
4. Require that account providers have acceptable procedures in place for replacing PIN and other provider	• Balance protection of customers against theft of funds against inconvenience of denial of service for legitimate transactions

Policy Narrative:
The primary obligation of the account provider and its agents is to ensure that a consumer's funds are protected against improper diversion. KYC procedures that require that funds can only be withdrawn based on proper identification of the beneficiary are intended to protect the owner of those funds, but may inhibit legitimate access if the owner is subsequently unable to provide adequate identifying information. It is important that proper KYC procedures be established when an account is opened to ensure difficulties in withdrawing funds later are avoided. Laws, such as the recent Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) in South Africa, require operators and distributors of mobile phone or SIM card (including existing clients) to perform full KYC procedures on any person to whom they provide a mobile phone or SIM. Customers are, therefore, required to visit agents in person and produce personally identifying information (full name, identity number, and address), which will be verify by a current national identity document, identity card, temporary identity certificate, or a valid passport. As the national ID cards and passport reliability are questionable, the risk is great that many will be excluded not due to criminality, but lack of stipulated documentation. [5]

Market Examples:

- **Jordan**: As a member in the UN International Convention for the Suppression of the Financing of Terrorism and the Arab Treaty for the Combating of Terrorism, Jordan issued an Anti Money Laundering Law (AML Law) in 2007, and in 2008, and the Central Bank of Jordan (CBJ) issued Instruction 42 under the AML Law.
  KYC for bank-based model. Instruction 42 stipulates that banks must identify and verify customer identity. In order to comply, customers must present their national ID, as well as a proof of address, in person to bank officials for verification in order to open an account. However, the ability to open an account without face-to-face verification greatly facilitates extending access to finance beyond the reach of traditional bank branches. KYC can be conducted remotely by an agent faxing documentation to the bank. Anecdotal evidence indicates that compliance with these KYC procedures does not pose an obstacle to low income population segments. The vast majority of poor people are able to provide a national ID and to give satisfactory proof of their address. Instruction 42 exempts wire transfer transactions below JD 700 (USD 980) from KYC procedures.[72] However, it does not offer relaxed KYC procedures for the opening of low value accounts.

Risk-based Policy Matrix – Appendix

KYC for nonbank-based model. It is unclear if e-money schemes would fall under the AML Law. The AML Law stipulates that financial companies which, inter alia, provide payment and collection services, must comply with Article 14 (compliance with KYC procedures, reporting suspicious transactions and complying with all instructions issued by competent regulatory parties).[73] Even if the operation of an e-money scheme is interpreted to be a "payment and collection service", the application of the law still requires it to be provided by a financial company. Since MNOs are not considered financial companies, the wording of the AML Law currently would not cover mobile banking. However, MNOs are themselves required to conduct KYC procedures including verification of client identity.[74] The KYC requirement was implemented after many mobile subscriptions had already been sold, forcing MNOs to conduct retroactive KYC procedures. In some cases, where it is impractical or otherwise difficult to conduct a face to face verification, MNOs are permitted to obtain missing ID information over the telephone and verify such information against the national database.

- **Indonesia:** The Bank of Indonesia's Circular Letter 10/49/DASP outlines requirements for money transfer services conducted by nonbanks, requiring that individuals and entities apply for a money transfer license to provide not only their risk management procedures, including KYC. KYC must include verification of both sender and recipient at the time of the funds transfer (via government issued ID, driver's license, or passport). Additionally, the sender and recipient must be re-verified in the event the transfer exceeds IDR 100,000,000 (approximately USD 8,600), any suspicious transactions are detected, and there is concern as to the veracity of sender/receiver provided information.[6]
- **El Salvador:** Mobile banking is still in the embryonic stages and available only to those with a bank account. Financial institutions are required to maintain both systems and policies that provide access to both the identity and transaction profiles of their clientele. In order to open a bank account, a customer must provide their name, date and place of birth, nationality, address, profession, and marital status, in addition to presenting an identity card. The Banking Law, however, does not stipulate which identity documents are acceptable.[7]
- **Pakistan:** The Branchless Banking Regulations, dated March 31, 2008, outlines a risk-based approach to customer due diligence. Level 1 account customers must fill out and sign the account opening application, provide a photocopy of the computerized national ID card (CNIC), and engage in a face-to-face exchange with the designated financial institution account opening employee or undergo a biometric fingerprint scan and a digital photo at the agent location, which is sent to the designated financial institution. For Level 2 branchless banking accounts (top level and unrestricted) and level 3 (merchants, agents, businesses, banking agents, or third party account provider accounts), these are subject to the full range of KYC and regulations applicable to all accounts.[8]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		x	x		x	x	x	x

Risk-based Policy Matrix – Appendix

1.3. Risk (Consumers):

"Customer's identity is stolen and used to open a mobile payment account fraudulently."

Description:

The risk of stolen identity can have multiple ramifications, including:

- Customer's identity could be used to access other services
- Customer is held accountable for fraudulent transactions made in his/her name
- Customer is unable to access mobile services because an account using his/her name/identity has already been established fraudulently.

Objective:

- Protect service users against results of identity theft
- Subject to regulatory approval and verification of implementation.

Policy Table:

Options	Implications
1. Biometric national ID, or financial ID, system with biometric validation required for account opening	• Though biometric ID and validation reduces the possibility that a stolen ID could be used to fraudulently open an account in a customer's name, the cost of implementing such a program can be high. • Different biometric options have varying cost associated with them (e.g. voice tends to be less expensive as it can occur over the phone, whereas fingerprinting and retinal scans are more costly) • Biometric ID program may be beyond the technical capacity of a regulator to implement and maintain, as the infrastructure for capture and validation will require maintenance.
2. Account providers provide an effective process for blocking accounts when notified of fraudulent activity.	• Requiring a rapid block procedure to stop fraudulent activity once recognized is a simple and pragmatic way to deal with stolen identity. • The procedure can be easily validated by regulators.
3. Develop of best practices for enhancement of fraud detection systems. Provider reports suspicious or fraudulent activity to central authorities (Central Bank/Financial Intelligence Unit or FIU).	• KYC mechanisms, which could include point-based multiple ID requirement, limits potential for fraudulent account opening. • Reporting helps target systemic fraud, thus reducing risk. • Enforcement mechanisms for reported illicit activity may not exist or may be weak. Creating or enhancing such mechanisms will require investment.
4. With adequate account opening protections, including both policies above, providers can limit the liability of fraudulent activity in account agreement	• Consumer protections embedded in contracts will reduce barriers to adoption, and should not be terribly costly with adequate fraud controls. • Contract enforcement could be required to ensure customer protection which would require an effective court system.
5. No regulatory KYC/CDD requirements or provider-based consumer protection against fraudulent account opening.	• Lack of KYC/CDD requirements open financial system to fraud risk, whether through ID theft or ID fraud. • Lack of protection represents a potential cost for consumers and thus a barrier to entry.

Policy Narrative:

Development of an identification infrastructure, either at the federal level or through private databases for financial verification purposes, should be of paramount concern to government authorities. As outlined in a recent report, there are a variety of options that might be taken to ensure either linkages to existing databases, incentives for creation of new electronic databases for identity and AML/CFT purposes, and introduction of smartcard-based national ID systems which facilitate identity verification using biometric information. In the interim, duplicative efforts should not be imposed on financial institutions and system designers should be cognizant of the tradeoff between the barriers to adoption for financial institutions versus the need for developing an adequate customer profile using alternative or tiered ID requirements for AML/CFT in the absence of a national ID.[9]

Market Examples:

- **El Salvador:** Regardless of the type of delivery channel used, bank customer data is protected by the bank secrecy rule. However, interviews by CGAP for a recent Branchless Banking assessment indicated work remained in the areas concerning the use of agents by banks and nonbanks, as well as the protection of funds deposited into stored value instruments (prepaid cards and mobile banking). Consumer protection issues regarding branchless banking regulations remained deficient.[10]
- **General:** In consideration of the three parties to a transaction: the customer, the agent's employee who operates the POS device, and the bank, each should authenticate itself before initiating any transaction, preferably with two factors of security. Namely, these would be the personal attributes of "something you own, something you know, and something you are." The customer and the agent might each have a personal card (embedded in their phones) in addition to a secret PIN (agent employee may have only a name and password to the POS terminal – something you own). To avoid fraudulent POS terminals, the bank could also announce a unique secret key to its customers before each transaction.[11]

Risk-based Policy Matrix – Appendix

- **General:** A new cloud-based service allows retailers to instantly set up and run their online business, processing transactions using voice biometrics to authenticate/authorize their online and mobile-based electronic payments. According to the voice biometrics-driven e-commerce platform is a step-by-step process that allows retailers to quickly set up and build a fully functioning store that will process Level 1 PCI compliant payments through its voice transact payment network. As well as accepting payments from major credit card companies, the firm claims that retailers can also automatically deploy its biometric payment system to process secure mobile payments. The company's voice biometrics service is billed as allowing consumers to set up their own voice biometric as an authenticator for use over the phone or mobile phone.[12]
- **General:** "Unique information about the customer's handset (IMEI) and SIM card (IMSI) may be used as a second factor authentication mechanism. This will create confidence that the customer is using his/her device/SIM (something they have), and their PIN (something they know). [13]
- **India:** In 2009, the Government of India launched a new initiative in conjunction with Nandan Nilekani, an Indian Minister of State and one of the founders of the technology firm Infosys, to deploy a unique identification (UID) number. The UIDs will voluntarily offer Indian residents a biometric finger print scan which could be associated with a unique ID number and further utilized for such services as branchless banking efforts and transactions.[14]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
			x		x	x	x	x

Risk-based Policy Matrix – Appendix

1.4. Risk (Consumers):

Customer's account security credentials and / or account information and transaction history are improperly released (e.g., PIN biometrics, and stolen phone/subscriber identity module [SIM]).

Description:
If a customer's account credentials, account information and transaction history are not adequately protected, the customer's account can be illegally accessed to steal funds or to process illicit activities. Customers may also be subject to identity theft or blackmail.

Objective:

- Account providers maintain a rapid account block process for customers if customer/MNO believes the account has been compromised.
- Development of best practices for enhancement of fraud detection systems.
- MNOs mitigate risk of unauthorized/ inappropriate access to customer transaction data.
- Subject to regulatory review and verification of implementation.

Policy Table:

Options	Implications
1. Strong privacy legislation / regulation require institutions to institute controls to reduce the likelihood for unauthorized release, or theft, of personal information.	• Regulatory requirement reduces likelihood for improper release. Standard requirements for all institutions limit criminal targeting of weak institution policies. • Burden on national authorities to institute and enforce; may be unaffordable or beyond the existing infrastructure's legal, technical or political capacity, or authority, to implement and enforce. • Requirement will impose a cost on providers.
2. Provider led controls instituted to mitigate the likelihood of unauthorized release or theft of customer information.	• Institutional policies reduce likelihood for improper release. Lack of standard requirements for all institutions allows for criminal targeting of institutions with weaker policies. • Institutional programs will impose a cost on providers; however, lack of a regulatory requirement allows institutions to determine the level of mitigation.
3. Providers institute a "disaster plan" to notify customers impacted by breach, Plan could include procedures to block transactions on all impacted accounts and to issue new credentials to customers.	• Can result in denial of access to services, resulting in hardship for funds recipients until problem resolved. • Quick action can limit operational, systemic, and reputation risk.
4. No formal regulatory requirement or provider policies for customer protection or disaster recovery plan	• Lack of policy raises the systemic fraud risk. • Ineffective response to a breach of privacy could undermine public confidence in the financial system and its regulators.

Policy Narrative:
With respect to consumer data integrity and security, the challenges in the mobile ecosystem involve the integration of both the technological and operational components under the purview of the various actors in the financial services and telecommunications industries. "Who is responsible for data security and authentication, and how does that credential or certainty get passed along the mobile payment supply chain? Who resolves the customer's problem if a mistake is made? What consumer protection rights exist in case of error or fraud, and do those rights change depending on whether a traditional payment system is used to settle the transaction?"[15] In lieu of formal regulation, voluntary provider-led controls may satisfy market demands, particularly if associations or alliances of providers mitigate systemic fraud risks targeting sector-specific operational weaknesses.

Market Examples:

- **General:** According to a study by Mobey Forum, potential security measures for the mobile ecosystem depend not only on the targeted market scope (niche, national, or international), but also the inter-sector relations of the market actors, in particular those in the financial services and the telecom sectors. According to Mobey, the two key functional roles are the hardware based security element (SE) issuer and the Platform manager. The Platform Manager owns the cryptographic keys used to control the SE platform. The master key is generated during the chip personalization process by the personalization bureau. And the mobile business ecosystem is defined by which industry players act in which roles and by the relationship between them.
  -"The highest international potential lies within the ecosystem scenario, where global personalization bureaus take the role of Platform Manager": the SE may be an embedded chip or Secure Memory Card (SMC) sold through independent retailers, requiring a strong drive from personalization bureaus.
  -"National solutions can be based on the ecosystem scenario where mobile operators act both as SIM issuers and Platform Managers: this scenario may occur in markets where the key players maintain trusted business relations, but incurs difficulties when market relationships become more intertwined. MNOs are the key business drivers.
  -"Niche solutions can be based on banks or other Account Providers acting as Platform Managers: banks or other providers desiring to launch mobile independently may prefer this scenario, but it is unlikely that they will achieve mass market penetration.[16]
- **General:** In writing on one of the concerns of Information and Communication Technology (ICT) policy makers, David Porteous noted that "m-payments require the accepted use of electronic signatures," up to and potentially including biometric identifiers, to validate and authorize

Risk-based Policy Matrix – Appendix

transactions. If this is not an accepted and legally recognized practice, then there is a payment repudiation risk to both payment agents and payees. In many countries, there is no legislation enabling e-commerce; while PINs are used as a mobile phone security feature, e-signatures are not, creating a need to provide the same status to electronic transactions/signatures as physical signatures.[17] Such a provision was established in Part II, Section 6 of the Zambian Draft Electronic Communications and Transactions Bill (2009): "(1) Where the signature of a person is required by law and such law does not specify the type of signature, that requirement in relation to a data message shall be met only if an advanced electronic signature is used. Subject to subsection (1), an electronic signature shall not be without legal force and effect merely on the grounds that it is in electronic form."[18]

- **General:** Consumer protection and privacy laws should be concerned with, and customers should be similarly apprised and consent to, the use of location based services on mobile phones (LBS). Customers should consent to these services during the registration process for financial services when they authorize a bank, MNO, or card issuer to identify their location as a security feature (for instance, to red flag a transaction that is initiated outside of the scope where the customer would not typically conduct transactions.)[19]
- **Zambia:** Voucher scratch cards used in conjunction with mobile payment programs may be fraudulently manipulated at the agent level. There have been instances of consumers being tricked or coerced into revealing the scratch card PIN to the agent or agency staff when the consumer is reliant on a single mobile phone used at an agent location to obtain the payment due to lack of access. The result is that the consumer is defrauded of all or part of the payment. Screening the agent is important, as is consumer education regarding PIN security.[20]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x	x	x		x	x	x	x

Risk-based Policy Matrix – Appendix

1.5. Risk (Consumers):
"Customer is unable to efficiently dispute a transaction or account charge."

Description:

Customers are not able to resolve disputes with a account provider and recourse to a government body or regulatory authority to arbitrate disputes is weak or non-existent.

Note: The dispute requiring resolution could be a transaction that is initiated by a customer on the customer's phone, as well as a transaction that an agent makes on behalf of a customer who does not have his/her own phone.

Objective:

- MNOs provide an efficient dispute resolution process.
- Clear, published service standards to minimize the cause of disputes.
- Subject to regulatory review and verification of implementation.

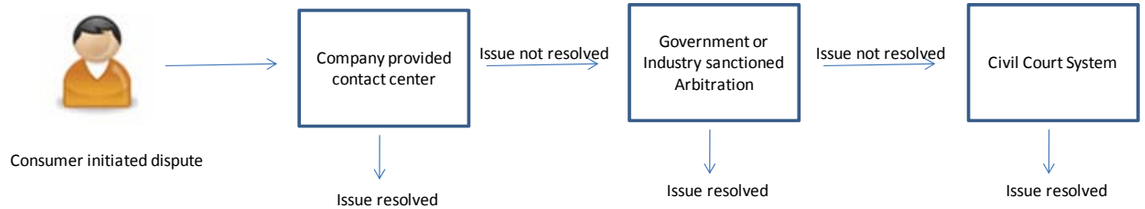
Policy Table:

Options	Implications
1. Regulatory oversight authority refers disputes back to the account provider but verifies account provider dispute resolution process.	• Licensing authority needs to set an "acceptable level of disputes" above which continuation of the account provider's license may be put in question. • Regulatory authority may not have capacity to handle complaints of disputes
2. Association of providers, or NGO, provides dispute resolution process.	• Association ownership could be perceived as biased toward providers, but less biased than a provider run system. An NGO focused on consumer protection could be preferable. • Allowing other providers in the association (or NGOs with other motivations) to interact with customers could create provider animosity • Association may not have capacity to support, or the budget to develop, this function.
3. Individual providers provide dispute resolution process	• Provider management could be biased toward provider; however, competition should enhance customer position.
4. Independent alternative dispute resolution (ADR) function developed to handle appeals to other processes.	• Existence of an independent ADR function provides consumer protection against industry bias in other processes.
5. No dispute resolution process	• Lack of consumer protection raises cost for consumers, thus creating a barrier to adoption. • The only incentive for resolving customer disputes will be customer retention and reputation, which will be stronger in competitive environments, and environments with an active business press corps.

Policy Narrative:

As with any banking/transaction service disputes between consumers and the account provider, between consumers, and between consumers and merchants is inevitable. The ability to quickly resolve such disputes in what is perceived to be an equitable manner is critical for consumer confidence and the eventual success of the service.

Lessons are available from existing banking, payment, and telecommunications models. As illustrated in Exhibit x-x, the typical dispute resolution flow involves a company specific customer service mechanism, a government or industry sanctioned arbitration body, and eventually, civil court mechanisms.



In the United States, debit card issuers and everyone else that electronically transfers money to or from a "bank account" is bound by a Federal law known as Regulation E (Reg E). Reg E clearly defines rules for banks that issue debit cards and, in particular, the strict processes which must be applied when a cardholder disputes a transaction. These rules include, as examples, the length of time within which the bank must provide "provisional credit" to the cardholder, the total length of time within which the dispute must be resolved, and how long a transaction can be disputed after it has posted against the bank account.

Since Reg E restricts the term "bank account" to mean demand deposit instruments such as checking accounts, however, Reg E does NOT apply to credit card transactions. While credit card issuers generally use Reg E as a guideline for handling disputes, it is the issuer's cardholder agreement and the issuer's policies that actually dictate how disputes are handled. The "zero liability" policy of Visa, as an example, is a business rule which all Visa card issuers must follow. That rule ensures cardholders that they will not be held liable for any

Risk-based Policy Matrix – Appendix

fraudulent transactions, provided that such fraud is properly reported within the timeframes dictated by the issuer.

Stored value (aka "prepaid debit") is a relatively new concept within the financial services industry but has quickly grown to be one of the single largest sources of payment transaction volume (and card issuance) in the US and throughout much of the world. In fact, Visa estimates that the total prepaid debit opportunity (a view of the future, not the current reality) is as much as $1 Trillion annually. Despite this, transactions performed on prepaid debit/stored value are largely unregulated at the federal level in the US and abroad.

An added complexity is that disputes can also arise through use cases other than traditional merchant transactions (e.g., peer to peer transfers). In all cases, platform record keeping capabilities and data retention requirements will underpin any dispute resolution process and influence any regulatory requirements.

Market Examples:

- **El Salvador:** Ley de Proteccion al Consumidor is the general consumer protection law, which has provisions for areas such as requiring banks to develop and publicize policies for products and pricing, bankruptcy protection for deposits over the bank creditors, etc. There is a Consumers Defender, which ensures compliance to the law, but no specialized agency or comprehensive regulatory framework dealing with financial consumer protection and payments via electronic channels.[21]
- **Indonesia:** The Bank of Indonesia's E-Money Circular addresses consumer protection-related complaints regarding e-money. It specifies that issuers must provide the following information to customers in clear and easily comprehensible Bahasa Indonesia:

a) information that e-money is not considered a deposit in the sense of the Banking Law and hence not guaranteed by Indonesian deposit insurance,
b) E-money usage procedure, such as cash in, transfer of funds, cash withdrawal, and redemption, as well as risks that may arise using e-money,
c) rights and obligations of a customer, which include:
   - -validity period of e-money (expiry),
   - -loss due to issue affecting customer, systemic failure, or other reasons,
   - -type and size of costs charged
   - procedure of submitting a claim in connection with e-money and estimated length of time for processing a complaint;
   - procedure of product use including for redeeming the entire e-money balance."[22]

- **U.S. and European Union:** The Electronic Funds Transfer Act and Regulation E in the United States and the Payments Directive in the EU set legal limits for consumer liability and procedures for dispute resolution. Depending on the time frame of consumer notification to the financial institution of an unauthorized transaction, the legal limit for the consumer's liability may be capped at $50-$500. In the EU, this limit is 150 Euros. In an effort to resolve disputes outside the court system, timelines for dispute resolution are likewise established, typically based on a number of working days from when the provider receives the consumer's complaint.[23]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x				x	x	x	x

Risk-based Policy Matrix – Appendix

1.6. Risk (Consumers):

"Customer is charged unauthorized fees by agent."

Description:

Agent may overcharge or have a side transaction that is not authorized that they impose on the consumer.

Customers may not understand the complexity of the contract signed, making it possible for him/her to face additional fees/services without being

Objective:

- Account Providers use clear contracts that fully disclose all fees to be charged, tailored for various customer situations, including different languages and illiteracy (i.e. pictogram-based contracts).
- Service charges clearly posted at each agent's location. Disclosures reasonably comprehendible to all customer groups (i.e. major language disclosures and potentially pictograms)
- Subject to regulatory review and verification of implementation.

Policy Table:

Options	Implications
1. Regulatory authority requires full disclosure of all fees in account agreement.	• Full disclosure of all fees limits potential for consumer exploitation by providers. • Regulators may lack the capacity/budget to monitor and enforce the requirement, especially considering the abuse is more likely to happen at the agent level than the corporate level.
2. Account providers required to ensure fee structure is posted in all service locations in a format understandable to the broad population. (i.e. major language disclosures and potentially pictograms) Account providers required to discipline or expel consistently non-compliant agents.	• Account provider disclosure mitigates potential for consumer exploitation, • Account providers may have difficulty ensuring reasonable compliance throughout their agent network.
3. No fee disclosure policy	• Account providers may not fully disclose fees, and/or agents may violate terms of service, undermining public satisfaction with the service, potentially resulting in complaints to the regulator.

Policy Narrative:

Fees for services should be disclosed to the customer in a clear and conspicuous manner at Agent locations, as well as posted in the major languages of the consumer groups being served and depicted pictorially. Given the channel of the service provided, the form of disclosure could be deployed electronically via the mobile handset or the Internet, but should also be made publically available at the Agent locations at the time the service is performed. The provider should inform the consumer of the potential for any third party fees and how to obtain further information regarding itemization of such additional fees (by type and amount).

Market Examples:

- **General**: Zain adopted the tiered model for its Zap service, with differences that are quite different from Safaricom and M-PESA with its agents. Zain charges customers for both cash in and cash out. Zain also permits agents to retain 100% of the tariff they charge the customer for each transaction. While Zain recommends a fixed tariff for cash ins/outs and communicates the same to its customers, they do recognize that agents will modify these and have limited recourse to restrain this practice. As a result, Zain agents will adjust rates depending on their availability of e-money and customer demand. They will negotiate rates with different customers and customers will pay cash fees to the agent. By allowing its agents to set their own commissions, customers may view this as predatory pricing versus transparent. [24]
- **Philippines**: An important feature of the mobile payments implementation in the Philippine market was the low user charges for purchase of and transfers of airtime and cash, which typically ranged from US 2-4 cents, though cash deposits and withdrawals were higher at 19 cents or 1%. In a 2006 study, which included markets in Southern Africa, South Africa, and Kenya, some networks charged upwards of 5-10 times these values for similar transactions. The Philippine charges, as a result, initially generated a much higher level of usage. The report did not even mention additional fees that might have been levied above and beyond base transaction charges. [25]
- **Tanzania:** Vodacom gives agents a commission each time a customer whom they registered buys airtime using M-PESA. The commission was established to reduce resistance to M-PESA by agents and aggregators, who were concerned that their customers would stop buying airtime from them directly. If the provider reduces agent commissions or otherwise does not adequately compensate them, they risk alienating the agents whom they rely on to deliver and promote their mobile money service. By allowing agents to set their own commissions for airtime and/or mobile money services, the operators risk the loss of transparency in pricing.[26]
- **Kenya:** Guideline on Agent Banking –CBK/PG/15: 4.5.1 Mandatory provisions to be included in the contract between an institution and an agent x) Prohibition from charging the customer any fees. [27]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		x	x		x	x	x	x

Risk-based Policy Matrix – Appendix

1.7. Risk (Consumers):

"Customer cannot access cash from mobile money account due to lack of agent availability."

Description:
Insufficient numbers/availability of mobile money and/or bank correspondent agents in a given geography results in consumers not being able to access cash or imposes excessive travel costs and inconvenience on consumers.

Objective:

- Providers responsible for market coverage
- No unreasonable regulatory constraints on expansion of agent networks

Policy Table:

Options	Implications
1. Regulatory authority mandates minimal geographic coverage as part of financial access/inclusion interests.	• Requirement raises the cost for account providers so that the service may not be profitable. Also, the requirement raises barriers to entry for smaller players. • Account providers may agree to collaborate in areas where population density does not justify multiple service access points.
2. Regulatory authority mandates community reinvestment by account providers to extend agent coverage	• Coverage would improve in rural areas • Requirement is a cost for providers; however, it has positive reputation benefits and could be scaled based on network size.
3. Regulatory authority requires disclosure of agent network coverage in service-level agreements (SLAs)	• Customer expectations are set at account opening. • Cost of compliance is low for providers and the cost of oversight is minimal. • Agent network will expand with market demand.
4. Regulatory authority allows account providers to appoint agents at their discretion, but with registration at the regulatory authority and subject to inspection as deemed necessary.	• Allowing account providers to determine the type and distribution of its agent network maximizes market efficiency. • The registration of agents and potential to inspect them provides the regulatory authority with a degree of oversight. • Agent network will expand with market demand.
5. Treat as internal account provider issue - no regulatory oversight of extent of agent network or required disclosure.	• Customer expectations may not be reasonable due to lack of transparency regarding network coverage and SLAs. Customer complaints may rise. • The reputation of the service may suffer. • Agent network will expand with market demand.

Policy Narrative:
The primary service a mobile money agent provides for its customer is to perform the cash in/cash out function. These transactions cannot be executed without adequate reserves of both cash and electronic value. If the agent is either physically unavailable to the customer or lacks liquidity in either stock of inventory, the reputation of the service necessarily suffers.

Market Examples:

- **Africa:** "Is there provision for agencies for cash withdrawal and deposits? For the foreseeable future, cash will remain the most widely used transaction medium in developing countries. It is therefore necessary there be sufficient points at which bank money (i.e. in a bank account) or e-money (e.g. at a TelCo) can be deposited or cashed out. Traditionally, these transactions happed via a bank teller, but branches are expensive to set up and run; extending branch networks into lower income or less dense areas is unlikely to be a viable means of increasing access to cash…for developing countries, ATMs are still relatively expensive, and typically require secure premises and ongoing servicing. Therefore, there is a need to use existing businesses which carry cash anyway, as bank agents or correspondents."[28]
- **Brazil:** It is not uncommon that retail agents can be employed in areas where transaction volumes and/or numbers may be too sparse to support a brick-and –mortar branch. If these agents are in locations where there is little or no banking presence, then cash management may pose operational issues. Not surprisingly, agents find it both costly and time consuming to deposit excess cash at bank branches where they frequently must travel into urban areas and risk theft of cash en route. In Brazil, Banco Brandesco partnered with the national post office to create national coverage using post office locations as agents, creating Banco Postal.[29]
- **Thailand:** The banking infrastructure permits instantaneous intrabank transfers, so that an agent can buy electronic value by transferring money from its bank account to its e-money account (a transaction that is completed via the mobile handset). After this is done, the agent's account is immediately credited with e-money value. True Money Express enables this functionality by holding bank accounts a more than a dozen banks throughout the country. The agent incurs a transfer fee of 1%. The agents also do not facilitate the cash out, which would require accumulating e-money from customers and reselling it back to True Money Express.[30]
- **Kenya and Tanzania:** In most markets, it is unrealistic for agents to travel to an operator-owned outlet or the branch of the operator's bank partner to facilitate instantaneous transfers or purchase electronic value. In these cases, operators appoint intermediaries that act like wholesalers in other distribution systems and earn lower commissions than regular agents since they deal in bulk. For a fee, these "superagents" agree to buy and sell electronic value in exchange for cash. Safricom signed

Risk-based Policy Matrix – Appendix

agreements with several banks in Kenya to perform this role. While banks commonly play this role, figures called "masteragents" who act as aggregators and manage liquidity may also buy value from the super agent and then resell it to agents under his umbrella. Vodacom in Tanzania issued its master agents toll-free mobile numbers to communicate their liquidity needs without concern as to airtime costs incurred.[31]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		x	x	x		x	x	x

Risk-based Policy Matrix – Appendix

1.8. Risk (Consumers):
"Agent unwilling to perform transaction for customer."

Description:

The agent may be unwilling to perform a large transaction because it is more profitable to the agent to perform multiple small transactions. Agent is unwilling to serve customer due to discrimination (race, tribe, religion, sex, etc).

Agent may wish to conserve cash by restricting large transactions to more profitably service a larger number of smaller transactionsAgent is instructed by super agent not to perform transactions during specific hours of the day due to cash pickup and deposit burdens.

Objective:

- Adoption of payment services best practices including optimization of agent and super-agent compensation models for cash distribution, cash pick up, and deposits.
- Standards for agents barring discriminatory practices, with regulatory review and verification of compliance.

Policy Table:

Options	Implications
1. Regulatory authority establishes anti-discriminatory policies with verification of compliance.	• Motivates account providers to encourage agents to serve the "customer in front of them" • Regulatory authority may lack capacity and/or authority for consumer protection oversight; Discrimination complaints are the task of other agencies
2. Account providers set institutional anti-discrimination policies and monitor agent behavior/compliance	• Institutional policies mitigate discrimination likelihood by setting up a disincentive for agents. • Providers may be more reactive in preventing discrimination if there is no regulatory cost. • Providers may lack the capacity, to monitor and enforce policy.
3. No regulatory requirement or provider policies requiring agents to complete transactions	• Relies on existing general anti-discrimination statutes and practices.

Policy Narrative:

In adopting best practices for agent compensation, it is critical to structure commissions to avoid instances where either the consumer or agent may abuse systemic loopholes. For instance, if commission structures are set to reward agents by maximizing their incentives for transaction volumes, they may structure a single customer deposit or withdrawal into multiple transactions to maximize commissions. On the other hand, agents may be disincentivized to perform small value transactions depending on their incentive and their liquidity at any given time.[32] It may be difficult in some instances, for example, to discern whether denial of service to minority groups who may have difficulties in obtaining a national ID card due to the registration process is a result of discrimination, lack of proper ID, or both. Registration for citizenship may be dependent on birth, decent, registration, or naturalization; registration and birth typically determined by the birth certificate. Decent may prove more difficult in some countries; women may not be allowed to pass nationality to their children or the homeless child may be "stateless."[33]

Market Examples:

- **Uganda and Cambodia:** Paying full-time customer registration agents on commission is possible, though it is important to pay a sustainable wage, given both their skills sets and economic conditions. If this does not occur, customer churn wipes out the investment the operator makes in the agent training.[34]
- **Zambia:** According to a GSMA report, the most common alternative to paying commissions based on tiers is to pay agents the same percentage of value transacted regardless of the size of the transaction. This eliminates the incentive to split transaction into multiple, small value transactions for a higher commission, and can be supplemented by minimum cash in and cash out, ensuring that agents are incentivized even for low value transactions.[35] In fact, two agent locations visited were observed to structure the lowest transaction tier for mobile money transfers with the highest fees and, when approached regarding transfers, indicated that no e-money was available.[36]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		x	x		x	x	x	x

Risk-based Policy Matrix – Appendix

1.9 Risk (Consumer):

"Customer cannot access cash from mobile money account due to lack of agent liquidity."

Description:

Customer cannot perform cash-out transaction because the agent does not have sufficient cash on hand to perform the transaction.

Agent may be experiencing unusually high cash-out requests due to special events, including public events, public disturbances, or loss of public confidence.

Super agents providing physical cash distribution to individual agents are not able to manage cash stocks effectively.

Objective:

- Account providers are responsible to customers for providing cash-out services in a timely manner, including contingency plans to deal with liquidity crises,
- Subject to regulatory review and verification of implementation.

Policy Table:

Options	Implications
1. Monitor complaints of unavailability of cash - factor the level of instances into license extension discussions/decisions.	• Forecasting and management capabilities are similar for ATM and Branch cash forecasting/ management. • Only a regulatory issue if account provider performance egregious - impact on license extension. • Account providers face a reputation risk if they cannot manage liquidity well.
2. Account providers forecast and manage liquidity of agent network to optimize service for consumers.	• Requirement ensures customers access to cash within a reasonable amount of time. • Forecasting and management capabilities are similar for ATM and Branch cash forecasting/ management. • Market forces will improve liquidity management overtime, as providers keep reliable agents; providers take on some agent responsibilities, or providers' partner with other institutions, as agents of last resort.

Policy Narrative:

This risk refers to the amount of capital (both cash and e-money) held by agents, available for cash in/cash out transactions. In many mobile financial services systems, agents are the primary human interface with the consumer. Initial consumer confidence in a MFS system is, to a large degree, contingent on their ability to conduct cash-in/cash-out transactions. Consequently, maintaining a viable agent infrastructure is an important element of a strong MFS system.

To date, MFS providers have used commercial practices (e.g., commission structures, agent vetting processes, prepaid e-money reserves) to drive the proliferation of cash in/cash out agents. Market forces have determined which agents remain viable. MFS providers generally have not developed service level agreements (SLAs) with agents requiring them to maintain cash balances.

Recent MFS conferences (e.g., M-Banking 2009, Kenya School of Monetary Studies, May 2009) have raised the issue of an unregulated, ad hoc, cash in/cash out infrastructure and the impact this has had on consumer confidence. While the issue is viewed as significant, most experts agree that a regulatory solution would be difficult to craft and implement. The current view is that consumer demand and market forces will dictate the number of agents and the operating principles that govern agent conduct (e.g., availability of cash, hours of operation, etc.) Further, similar to branch and ATM channels, the market will provide cash forecasting solutions to minimize liquidity issues.

Market Examples:

- **El Salvador:** Under Article 1 of the Banking Law, deposit-taking, financial intermediation, and "other activities carried out by banks", permit the Central Reserve Bank (BCR) to authorize other operations and services. Banks are subject to regulation ranging from prudential to management and ownership rules, with licensing by the Superintendence of the Financial System (SupFin). However, a different framework governs member-based financial institutions, most of which were not subject to supervision by SupFin. This financial sector, comprised of savings and loan societies and cooperative associations, recently pushed for a new law allowing deposit-taking from the general public. While there is no specific regulation on the issuance of e-money by non-banks, the activity by this sector is defined as taking deposits and intermediating those deposits. According to a recent CGAP Branchless Banking Assessment, it is widely assumed that Salvadoran regulators would strictly apply this definition to e-money schemes and deem such activity to be banking activity, particularly if funds are to be intermediated. [37]
- **India:** Acknowledging the development of the mobile channel, The Reserve Bank of India (RBI) issued the Operative Guidelines for Mobile Banking Transactions (2008) pursuant to the Payment and Settlement Systems Act (2007). Only banks licensed, supervised and with a physical presence in India may offer mobile banking to their existing customers. These institutions must obtain prior approval of RBI before launching their service offering. MNOs and nonbank financial institutions may not offer mobile banking services. Cross-border and foreign remittances are not permitted. Daily transaction limits are set at Rs 5,000 for transfers and Rs 10,000 for goods and services purchases. Two factor authentication, including a PIN is required on all transactions, with a limit of Rs 50,000.[38]
- **Kenya:** A recent study on the community level effects of M-PESA on local economic activity indicated that money circulation was the most highly ranked of all effects. It was consistently identified by respondents (being ranked most important by men and no. 3 by women) as infusing cash into the community via remittances where they appeared to be needed most. The higher and faster

Risk-based Policy Matrix – Appendix

circulation, in turn, contributed to expansion of businesses, food security, human capital accumulation, and rescue money (emergency funds), as well as increased employment opportunities.[39]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x		x	x	x	x		x

Risk-based Policy Matrix – Appendix

1.10 Risk (Consumers):

"Customer cannot access cash from mobile money account due to lack of personal access."

Description:

Customer cannot receive cash from agent or perform cash-out transaction during regular "business hours" due to one of the following situations:

- Customer has exhausted his/her pre-paid minutes.
- Customer's cell phone battery is dead.
- Customer has lost his/her cell phone.

Objective:

- Customer's responsibilities and process for regaining access to cash spelled out in contracts and in account provider's operating procedures.
- Simple remedies to each situation spelled out and available to users.

Policy Table:

Options	Implications
1. Provider ensures alternative access procedures in the event of customer notification of access failure; terms and conditions of each party's responsibilities outlined in account agreement.	• Customers responsible for maintaining their access. But failure to resolve access problems could undermine public acceptance by increasing the user's risk.
2. No alternative access measures exist	• Customer must pursue through dispute resolution if they can not reestablish connectivity.

Policy Narrative:

The two core components of customer education on mobile financial services should center on the customer's level of understanding of the service (e.g. methods and procedures for access) and the level of customer confidence in the service, including his/her perception of device security. Banks offering mobile banking generally do so as an alternative delivery channel for existing banking customers, with the model covered by an existing transactional and regulatory framework. Alternative access measures for the client have typically been established and are enumerated in customer account agreements. In the event an agent or correspondent network is developed in conjunction with traditional banking, such as in Brazil and India, regulations are adapted for consumer protection and access. In the case of non-banks offering mobile financial services, customers typically do not interact with a bank nor have a bank account; they may instead interact with an MNO or a prepaid card issuer; regulations or dispute resolution through customer agreements governing non-banks, e-money, and stored value, as well as the recourse for the consumer may either not exist or may be in conflict with traditional methods with which the consumer is familiar.

Market Examples:

- **Philippines:** "Circular No. 649, Series of 2009, Section 4. Provisions for All EMIs (Electronic Money Issuers). G. EMIs shall disclose in writing and its customers shall signify agreement to the information embodied in item C above upon their participation in the e-money system [note: Section C, in part, states that "E-money may only be redeemed at face value" and "…is not considered a deposit hence it is not insured with the Philippine Deposit Insurance Corporation."]. In addition, it shall provide clear guidance in English and Filipino on consumer's right of redemption, including conditions and fees for redemption, if any. Information on available redress procedures for complaints together with the address and contact information of the issuer shall also be provided." [40]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x	x	x			x	x	x

Risk-based Policy Matrix – Appendix

1.11 Risk (Consumers):

"Customer cannot access cash from mobile money account due to lack of system availability. "

Description:

Customer cannot receive cash from agent or perform cash-out transaction during regular "business hours" because of one of the following situations:

- Agent and/or customer cannot access the system to execute the transaction.
- The communications account provider is experiencing a temporary system outage.
- A record of complaints may indicate questionable business practices, or a lack of complaints could mean there is no established avenue for consumer remediation. Unscrupulous businesses or business may change names and locations to hide complaint histories once the business ceases operations.

Objective:

- Providers are responsible to customers for providing cash-out services in a timely manner.
- Account Providers post realistic access standards and area coverage to ensure appropriate client service expectations.
- Subject to regulatory review and verification of compliance.

Policy Table:

Options	Implications
1. Regulatory authority requires system availability service levels. Business continuity plans must be clearly stipulated in terms and conditions of customer agreements. Significant complaint levels will impact license extension.	• Required service levels and continuity plans mitigate system availability risk. • High system availability requirement will impose a cost to some providers and raise a barrier to entry for potential providers. • Regulatory authority capacity/authority to regulate and enforce system availability may not be practical. (Whether the regulatory authority in this situation is financial or telecommunication is debatable.)
2. Regulatory authority monitors system availability service levels. Significant complaint levels could impact license extension.	• Any new market entrant is likely to take time to fully roll out its service, particularly if competition is entrenched. Failure to do so within a reasonable time could lead to failure of the service, resulting in the regulator having to ensure an orderly withdrawal. • Regulatory capacity to monitor system availability may be limited. • Lack of a regulatory requirement keeps barriers to entry low, relative to this issue.
3. No system availability requirement by regulators or commitment by providers	• Adoption rates will be low if customers cannot depend on system availability.

Policy Narrative:

As the population begins to rely on the mobile network infrastructure for their financial service needs, any interruption of service will have a negative impact on the economy, beyond the impact associated with the ability to make calls. With payment volumes between individuals increasing, businesses integrating mobile payments into their operations, and governments leveraging the innovation to pay civil servants and make transfers to citizens, regulators must consider the availability requirements that private actors must maintain. In the policymaking process, regulators must balance raising barriers to entry and innovation with safeguarding the economy and consumer protection. As such, there is a continuum of policy options, of which we present three examples. First, the regulatory authority can set regulatory requirements for operators of mobile network infrastructure for system availability, redundancy, and continuity planning. Such requirements would be a precursor to licensing, and inability to maintain system availability would result in fines and negatively impact renewal of license. Second, guidelines could be provided and regulatory authorities could monitor availability and investigate issues as they arise. Lastly, regulators could leave system availability up to the market. Customers would likely flock to those with the best reputation for service. Variations to each of these options still exist. For example, regulators could tier requirements relative to customer base transaction volume so that the regulatory burden is proportional to the risk that failure presents to the economy.

Market Examples:

- **Philippines:** The Philippines is noted as the world's leader in the use of text messaging (SMS). Current estimates place usage at seven SMSs per customer per day, with the Philippine networks having had to equip two data channels in place of the usual one to control the traffic. Despite this, the introduction of SMART Money and Globe's G-CASH reported not system overloads, though exact transaction loads are not available (estimates are two calls per customer per day for SMART).[41]
- **Philippines:** "Circular No. 649, Series of 2009, Section 4. Provisions for All EMIs (Electronic Money Issuers). D. EMIs shall ensure that e-money instruments clearly identify the issuer who is ultimately responsible to the e-money holders. This shall be communicated to the client who shall acknowledge the same in writing."[42]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
x	x	x	x	x	x	x	x	x

Risk-based Policy Matrix – Appendix

1.12 Risk (Consumers):

"Lack of network interoperability prevents consumer from transacting with desired party."

Description:

Closed loop networks with no capability to transfer funds between account holders of different Account Providers' payment networks due to lack of interoperability. Among providers or their non-participation on a national payment platform block payments outside of the account provider's network. The first player to enter the market can gain monopoly power, limiting competition, but can help justify initial market entry into virgin markets.

Objective:

- No protectionist barriers to transfer funds between systems.
- Intra- account provider transfers conducted within the account provider's system.
- Inter-account provider transfers conducted through a national switch, either directly or through correspondent clearing accounts, without unreasonable usage fees or penalties.

Policy Table:

Options	Implications
1. National regulators require interoperability of payment networks (through inter-account provider links or through a switch)	• Requirement of interoperability may raise a barrier to entry as the technology requirements could be more challenging than a simple closed network. Further, the requirement may stifle innovation in a new technology through keeping new entrants out. • Consumers might benefit as there would be no network limitations on sending mobile money. • Account providers might be forced to compete on cost, products, and service, rather than size of network. • Limits first mover advantage, potentially discouraging initial market entry.
2. Competition agency empowered to investigate non-competitive behavior	• Requires a competition agency with the capacity to investigate and enforce non-competitive behavior, such as predatory pricing.
3. No regulatory action	• Predatory pricing and expanded monopoly power are possible; however, experience with networked technologies (cell phones/ATMs) suggest that the market will move toward interoperability without regulatory action.

Policy Narrative:

This risk focuses on the concept of interoperability among competing national and international MFS systems. Universal acceptance by all consumers, regardless of mobile network operator or MFS platform affiliation, will impact penetration growth and the overall sustainability of MFS.

In markets where MFS services are being led by mobile network operators (MNOs) interoperability is limited to peer to peer transfers to rival MNO subscribers through a mechanism that requires cash out, switching to and registering with the sender's service.

In markets where a third party is the dominant MFS provider (e.g., Wizzit) specific MNO affiliation is not a requirement. However, all transactions must be made through the third party platform and connectivity to other MFS providers is not possible.

In markets where banks are the leading players, the existing financial sector clearing processes act as a catalyst for interoperability. However, to date this has not translated into an effective interoperable MFS system.

In other fields, consumer demand typically drives the development of industry standards and interoperability (e.g., GSM operations). With respect to MFS, financial regulators are positioned to regulate interoperability, but thus far, have not done so.

Market Examples:

- **El Salvador:** According to a CGAP interview with the Central Reserve Bank (BCR), limited interoperability for retail payments hampers customers from cash-based deposit and withdrawal services in bank branches, as well as transferring funds from bank-to-bank using the Internet channel. Mobile banking is in the embryonic stages, and similar to Internet banking, is available only to those who already have bank accounts.[43]
- **Pakistan:** The State Bank of Pakistan (SBP) considered several branchless banking models before initially deciding to allow only bank-led models. In all cases, the customer has an account relationship with the bank through establishment of a branchless banking account. The many-to-many model involves a central transaction processing system or switch, providing total interoperability. Though not yet implemented, this is the preferred model of SBP and allows multiple banks to offer services to customers of multiple agent networks or MNOs. The switch must be controlled by the bank, an agent or a subsidiary of the bank or group of banks. Banks can purchase access to the switch, similar to access to an ATM network, which would reduce the technology investment burden placed on any single bank.[44]
- **Indonesia:** Article 27 of the E-Money Regulation mandates that e-money providers must offer systems that are interoperable with other e-money systems.[45]
- **South Africa:** WIZZIT, founded in 2004 by two entrepreneurs and operating in partnership with the Bank of Athens, offers mobile banking services to approximately 300,000 customers. The company is mobile phone agnostic, so that customers can use phones operated by any of South Africa's mobile operators, for services ranging from transferring money to third parties, loading

Risk-based Policy Matrix – Appendix

electricity with prepaid cards, and buying airtime for prepaid mobile phone subscriptions. Since WIZZIT has no brick and mortar branches of its own, it operates 3,500 deposit taking sites in conjunction with the Post Office and ABSA Bank. Customers are issued a Maestro-branded debit card, which they may use for cash withdrawals at any South African ATM.[46]

- **Spain:** Mobipay, was launched as mobile payments platform, as a result of a joint venture between Spain's largest TelCo, Telefonica, and a bank, BBVA. At the time this venture, the Spanish Competition Authority (SDC) was concerned that m-payments would affect not only e-commerce but also mobile telephony; it approved the JV with certain stipulations:

-other mobile operators must be allowed to participate;
-the interoperability of any mobile operator and any financial institution had to be technically possible;
-customers could not be limited in their choice of other MNOs or financial Account Providers by the service contract;
-SDC had approval authority for interchange fees.
While initially slow to market in Spain, BBVA, took the product to Mexico and North Africa in 2005.[47]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		x			x	x	x	x

Risk-based Policy Matrix – Appendix

1.13 Risk (Consumers):

"Customer loses balance due to failure of a bank holding trust fund, or a similar situation where trust fund is compromised."

Description:

Should the trustee fails or goes into insolvency, trust accounts that are not legally segregated from the general pool of bank assets available to satisfy creditors may be pulled into the bankruptcy process.

Trust funds deposited by the trustee in an account with the trustee bank or other banks are pooled deposits that may not be fully protected under bank closing/insolvency/deposit insurance rules.

- Deposit insurance is at the account level, and the trust account is viewed as a single account, rather than many.
- Trust accounts are not covered as deposit accounts.
- There may not be deposit insurance in the country.

The value of trust funds invested in other financial instruments or institutions may be impaired.

The trust account may be technically protected, but no rapid procedure for transferring funds held in trust to another trustee may exist, preventing access to the funds

Objective:

- Trust funds holding the value of items in transit are legally segregated from the trustee's own assets in bankruptcy.
- Trust accounts are divisible (to spread risk) and transferable (in case of failure of the trustee to perform).
- Management and investment of trust funds regulated similarly to insurance company loss reserves to limit risk of impairment of value.

Policy Table:

Options	Implications
1. Law / Regulation relating to bank failure or insolvency segregates assets held in trust accounts from the general pool of assets of a trustee in the bankruptcy process.	• Requires trust law - normal in common law systems but typically difficult in statute law systems. • Requires a court system that both understands trust law and is empowered to enforce it.
2. Law / Regulation on trust funds that provides for: • Transferability of the trust to another trustee in case of non-performance or failure of the trustee. • Investment guidelines for trust funds that limit risk concentrations for funds not invested in marketable or short maturity government securities. • Clear segregation of trust funds covering customer funds from the operating funds of the account provider. • Periodic regulatory verification of the adequacy of trust funds	• Diversification of trust accounts spreads risk across multiple financial institutions thus reducing the exposure of providers. Holding across multiple institutions will create a bit more complexity for payment providers in managing several bank relationships. • Monitoring and enforcement of trust account diversification should be possible through periodic reporting.
3. No regulatory action	• Deficiencies in the trust account, if leading to the inability of a account provider to cash out for clients, could have systemic impact through weakening of public confidence in the financial system.

Policy Narrative:

When a customer makes a deposit to their mobile payment account, the funds do not remain with the mobile network operator, but are held in a trust account, along with all other deposits, at a given financial institution. If the bank holding the trust fails or becomes insolvent, the customers, who may have no relationship with the failing institution, may risk financial loss if regulatory measures are not in place to limit the risk. Two key policy measures are noted that focus on modifying the legal / regulatory framework to ensure consumer protection. The first focuses on insolvency. If the law / regulation relating to insolvency segregates trust account assets from general assets, then mobile customers would have some protection of financial loss. The second focuses on the regulation of the trust fund itself. As noted, this law or regulation would focus on limiting risky investment, the segregation of assets, and monitoring. These two policies work together. If a financial institution has a policy of segregating entrusted funds from operating funds and maintains a low risk investment strategy with these funds, then these consumers should be protected in case of insolvency.

Market Examples:

- **European Union (EU): DIRECTIVE 2000/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 September2000** "The issuance of electronic money may affect the stability of the financial system and the smooth operation of payments systems. Close cooperation in assessing the integrity of electronic money schemes is called for. Electronic money institutions shall not have any holdings in other undertakings except where these undertakings perform operational or other ancillary functions related to electronic money issued or distributed by the institution concerned… 2. Electronic money institutions ***shall have at all times own funds which are equal to or above 2 % of the higher of the current amount or the average of the preceding six months' total amount of their financial liabilities related to outstanding electronic money.*** 3. Where an electronic money institution has not completed a six months' period of business, including the day it starts up, it shall have own funds which are equal to or above 2 % of the higher of the current amount or the six months' target total amount of its financial liabilities related to outstanding electronic money. The six months' target total amount of the institution's financial liabilities related to outstanding electronic money shall be evidenced by its business plan subject to any adjustment to that plan having been required by the competent authorities.[48]
- **Jordan:** The Deposit Insurance Corporation in Jordan was established pursuant to the Deposit Insurance Corporation Law of 2000. Deposit insurance applies only to banks, as well as local

Risk-based Policy Matrix – Appendix

branches of foreign banks, and covers up to a maximum deposit of JD10,000 (USD 14,000). The fees charged to banks include (i) a JD100,000 (USD 140,000) fee paid upon establishment of the bank and (ii) an annual fee equal to 0.25 percent of the bank's aggregate deposits.[49]

- **General (Microfinance):** The field of microfinance may include not only credit transactions, but also micro-savings, micro-insurance, remittances, and other payments, which though fractionally small in overall payment streams, greatly impact the lives of the poor. A recent CGAP research study noted that there exist financial institutions excluded from microfinance definitions that are nonetheless providing services to more than 750 million account holders worldwide in low income range.[50]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x	x	x	x	x	x	x	x

Risk-based Policy Matrix – Appendix

1.14 Risk (Consumers):

"Pooled deposits within a trust account can create a funding concentration risk which would not protect individual customers if trust is impaired."

Description:

Trust impaired: Trust funds deposited by the trustee in an account with the trustee bank or other banks are pooled deposits that may be significant compared to the size of the bank, representing a funding concentration risk, and may not be fully protected under bank closing/insolvency/ deposit insurance rules.

- Even if available, deposit insurance is at the account level, and if the trust account is viewed as a single account, rather than many, the cap would be insignificant compared to the size of the trust account.
- The value of trust funds invested in other financial instruments or institutions may be impaired by a decline in market value of the investments.
- Significant and unusual outflows could present the trust with liquidity difficulties if investments cannot be unwound.

Objective:

- Trust funds holding the value of items in transit are legally segregated from the trustee's own assets in bankruptcy.
- Trust accounts are divisible (to spread risk) and transferable (in case of failure of the trustee to perform).
- Management and investment of trust funds regulated similarly to insurance company loss reserves to limit risk of impairment of value.

Policy Table:

Options	Implications
1. Law / Regulation relating to bank failure or insolvency segregates assets held in trust accounts from the general pool of assets of a trustee in the bankruptcy process.	• Requires trust law - normal in common law systems but typically difficult in statute law systems. • Requires a court system that both understands trust law and is empowered to enforce it.
2. Law / Regulation on trust funds that provides for: • Transferability of the trust to another trustee in case of non-performance or failure of the trustee. • Investment guidelines for trust funds that limit risk concentrations for funds not invested in marketable or short maturity government securities. • Clear segregation of trust funds covering customer funds from the operating funds of the account provider. • Periodic regulatory verification of the adequacy of trust funds	• Diversification of trust accounts spreads risk across multiple financial institutions thus reducing the exposure of providers. Holding accounts across multiple institutions will create a bit more complexity for payment providers in managing several bank relationships. • Monitoring and enforcement of trust account diversification should be possible through periodic reporting. • Excessive risk concentrations in a trust fund could heighten systemic vulnerability should a loss of public confidence in the account provider result in disintermediation with consequent demand to liquidate investments by the trust.
3. No regulatory action	• Deficiencies in the trust account, if leading to the inability of a account provider to cash out for clients, could have systemic impact through weakening of public confidence in the financial system.

Policy Narrative:

When a customer makes a deposit to their mobile payment account, the funds do not remain with the mobile network operator, but are held in a trust account, along with all other deposits, at a given financial institution. If the bank holding the trust fails or becomes insolvent, the customers, who may have no relationship with the failing institution, may risk financial loss if regulatory measures are not in place to limit the risk. Two key policy measures are noted that focus on modifying the legal / regulatory framework to ensure consumer protection. The first focuses on insolvency. If the law / regulation relating to insolvency segregates trust account assets from general assets, then mobile customers would have some protection of financial loss. The second focuses on the regulation of the trust fund itself. As noted, this law or regulation would focus on limiting risky investment, the segregation of assets, and monitoring. These two policies work together. If a financial institution has a policy of segregating entrusted funds from operating funds and maintains a low risk investment strategy with these funds, then these consumers should be protected in case of insolvency.

Market Examples:

- **Philippines**: "Circular No. 649, Series of 2009, Section 4. Provisions for All EMIs (Electronic Money Issuers). B. EMIs shall put in place a system to maintain accurate and complete record of e-money instruments issued, the identity of e-money holders, and the individual and consolidated balances thereof. The system must have the capability to monitor the movement of e-money transactions and link e-money instruments issued to common e-money holders. The susceptibility of a system to intentional or unintentional misreporting of transactions and balances shall be sufficient grounds for imposition by the BSP (Bangko Sentral ng Pilipinas) of sanctions, as may be applicable."[51]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x	x	x	x	x	x	x	x

Risk-based Policy Matrix – Appendix

Risk-based Policy Matrix – Appendix

1.15 Risk (Consumers):

"Customer loses balance due to bank/provider not maintaining a 1:1 coverage requirement in the payment account trust fund."

Description:

If the financial services provider or bank holding the trust fund does not maintain a balance equal to the total value of all pre-paid accounts (payments in transit or float determination), the customer may not be able to access his/her funds if there were a "run on the bank."

The risk is particularly severe if the account provider is experiencing operating losses or cash flow strains due to network expansion or other operating or investment costs and may see client funds in transit as a source of operating funding.

Objective:

- Prevent co-mingling of account provider operating funds and customer funds in transit.
- The sum of the lower of cost or market value of trust funds in account provider trust accounts must at least fully cover the value of all transfer items in transit or funds stored in mobile phone accounts that are defined as funds paid in by customers into payment accounts and not yet withdrawn.
- Subject to regulatory supervision (this is probably the dominant systemic risk issue).

Policy Table:

Options	Implications
1. 1:1 trust account balance requirement.	• Requires periodic reporting by banks/providers to regulators. • Reporting requirements Regulators will need the capacity to effectively monitor and verify reports.
2. No regulatory action	• Failure to ensure that items in transit are fully covered by corresponding funds held in trust could result in a messy winding up of a failed account provider, with systemic impact on financial markets.

Policy Narrative:

To mitigate risk, financial institutions are responsible for maintaining capital requirements in line with regulatory provisions. Such requirements help to protect consumers by ensuring banks keep enough cash on hand to ensure liquidity even in the case of high demand periods, such as a "run on the bank" during a financial crisis. In an MNO model, the regulatory requirements of financial institutions may not apply to MNOs offering mobile payment accounts. Without regulatory requirements and monitoring, an MNO could leverage mobile payment account funds to cover operating expenses, or even to make investments. Given the high demand nature of mobile payment accounts, the policy option notes a 1:1 trust account balance requirement.

Such a requirement would disallow any risk to customers by misuse of their account balance. Clearly, less restrictive capital requirement levels could be set, yet these will expose customers to risk. As mobile payments remains a fairly nascent technology / financial service, more historical data would be required to provide policymakers the ability to safely set lower thresholds.

Market Examples:

- **Indonesia:** The Bank of Indonesia (BI) issued both an E-Money Regulation (11/12/2009) and a related Circular Letter 11/11/DASP, specifying that both banks and non-banks could issue e-money. Both types of issuers are required to obtain licenses from BI; nonbank issuers must place 100% of the float in a commercial bank, with funds being placed either in a savings, current account or a time deposit account. Float funds may only be used to fulfill the issuer's obligations to customers and agents. Bank issuers are required to report the float as an immediate liability. Further, both types of issuers are prohibited from issuing e-money with values other than that (higher or lower) deposited by the holder. Definitionally e-money funds are not considered to be deposits under the E-money Regulation or Circular Letter and, therefore, are neither protected by Indonesian deposit insurance nor are interest bearing.[52]
- **Philippines:** "Circular No. 649, Series of 2009, Section 5. Provisions for EMI-Others (note: these are non-bank financial institutions which are registered as money transfer agents with Bangko Sentralng Pilipinas). D. To further protect the e-money holders and ensure that e-money redemptions are adequately met at all times, the entity should have sufficient liquid assets equal to the amount of outstanding e-money issued. The liquid assets should remain unencumbered and may take any of the following forms:
  1. Bank deposits separately maintained for liquidity purposes;
  2. Government securities set aside for the purpose; and
  3. Such other liquid assets as the BSP may allow.

  Records pertaining to the above liquid assets shall be made available for inspection by BSP at any time and the confidentiality of bank deposits and government securities shall be waived."[53]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x		x		x	x	x	x

Risk-based Policy Matrix – Appendix

1.16 Risk (Consumers):

"Consumers may respond to social pressures by drawing on credit lines to fund payments, risking over indebtedness."

Description:

Increasing the ease with which funds may be transferred to family members may increase social pressures for such transfers, possibly leading remitters to tap credit lines to supplement payments. This may increase the risk of remitters increasing their debts to unsustainable levels.

Objective:

- Public awareness of the risks of over indebtedness.
- Lender policies and procedures that protect against over indebtedness.
- This is a general (not cell phone specific) consumer protection and portfolio quality issue that should be already under regulatory oversight, although may not be in place in many countries.

Policy Table:

Options	Implications
1. Regulatory authority prohibits use of credit facilities for funding mobile money accounts.	• Not implementable since money is fungible. • Financial institutions will reject regulators limiting how credit facilities can be used on a situational basis.
2. Regulatory authority may provide general consumer protection guidelines for over indebtedness, but otherwise take no action	• Requires support from the on-site examination of regulated institutions' lending policies and procedures, as a normal part of market supervision.

Policy Narrative:

As mobile money is a rapid way to send money long distances, individuals remitting money via mobile payments may face increased pressure to support family and friends. If mobile payment accounts could be funded via a credit facility, consumers could rapidly indebt themselves in response to such pressure. Though consumer debt is a valid concern, regulators will face challenges if they attempt to restrict the use to which approved credit lines can be used. The regulatory authority, instead, should focus their attention on the credit policies of the institution that extended the credit line.

Market Examples:

- **Jordan**: Currently there is no consumer protection regulation for MFI clients. Consequently, the only recourse available to MFI clients (and MFIs themselves) is an often lengthy and costly court system. The Central Bank of Jordan (CBJ) has a consumer complaint division for customers of licensed banks only (and consequently available to clients of Cairo Bank of Amman's microcredit program). However the CBJ's consumer complaint division minimally staffed office does not engage in any substantial effort to educate financial consumers of their rights. The Ministry of Industry and Trade (MIT) only supervises market conduct to the extent such conduct addresses fair pricing; MIT does not address consumer protections related to —free market services.[54]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
x				x	x	x	x	x

Risk-based Policy Matrix – Appendix

1.17 Risk (Consumers):

"Customer's family is unable to access account funds if the customer dies."

Description:
If account providers have not established escheatment guidelines for customer mobile payment accounts in case of death, customer's families will be unable to access the balances and the account will remain dormant on the provider's system.

Objective:

- Escheatment guidelines to mimic the guidelines for demand deposits accounts.
- Subject to regulatory oversight and verification of compliance.

Policy Table:

Options	Implications
1. Regulatory authority mandates establishing beneficial owners for stored value fund balances payable on death of the owner	• Account opening complicated, increasing operating costs and potentially deterring usage. • Regulation implies enforcement capacity and costs.
2. No regulation, but account providers establish beneficial owners for stored value fund balances in the event of death or incapacity of the owner	• Account opening complicated, increasing operating costs and potentially deterring usage.
3. Service users protect themselves by sharing access codes with trusted family member(s)	• Could result in misallocation of funds by overly trusted family member(s)
4. Institute "abandoned property" regulations that transfer unclaimed funds to the state after a prescribed period.	• Requires an accounting process for abandoned funds and may require a process for responding to claims received after the prescribed period.

Policy Narrative:
A "Payable On Death" or POD option for a mobile financial services account would involve filling out additional forms for the bank-led or hybrid MFS models and allow for the transfer of all assets to the named beneficiary or beneficiaries upon, for instance, presentation of a death certificate of the sole owner or the last to die of all multiple owners on an account and the proper ID of the named beneficiary or beneficiaries. POD has no effect on ownership of the funds in the account until the owner's death; the owner may change the beneficiary designation at any time without the beneficiary's knowledge or consent. There may still be challenges for the financial institution, however, in KYC of the named beneficiary and a risk-based approach would be prudent in responding to claims. In the event the account is opened with an MNO-based model, the account provider may follow precedent for e-money funds in the absence of existing regulation, but in all likelihood funds may revert to the MNO in the absence of knowledge be survivors of the account or a regulatory requirement for notification for abandoned property.

Market Examples:

- **Kenya:** M-Kesho is a bank account accessible by M-PESA registered users who are Equity bank account holders. They need a mobile phone and must fill out an application form at selected outlets, producing an original ID, a copy of the ID and 2 passport size photos. Funds may be transferred from Equity bank accounts or through M-PESA, though inter-account transfers are not allowed (e.g. transfers to those who do not have an M-KESHO account.). Other features include micro credit facilities through M-PESA and micro credit insurance insurance and accident coverage.[55]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x				x	x	x	x

Risk-based Policy Matrix – Appendix

1.18 Risk (Consumers):

"The beneficial owner(s) of stored value and transactional accounts (e.g., mobile money) cannot be determined by authorities in the event of illicit account activity or determining credit worthiness of individual members when group accounts are allowed."

Description:

Village based solidarity and small group lending programs jointly open a non-bank mobile money account making regular deposits with an intention to "share out" funds to individual group members as micro-loans. As the account is associated with multiple individuals, authorities have difficulty identifying specific actor when illicit activity occurs.

Objective:

- Responsibility for any transaction passing through a mobile account clearly defined.

Policy Table:

Options	Implications
1. Law / Regulation prohibits group registration for transactional accounts.	• The law cannot realistically prevent informal group use of accounts – individual associated with the SIM card bears responsibility for any issues. • Enforcement will focus on provider policy and investigation when criminal activity is suspected – implies enforcement costs
2. Law / Regulation limits group registration for transactional accounts to corporate entities; enforced by account provider and or regulatory authorities	• Corporate restriction limits flexibility for micro-finance group accounts. • The law cannot prevent group use of accounts – individual associated with the SIM bears responsibility for any issues. • Enforcement will focus on provider policy and investigation when criminal activity is suspected – implies enforcement costs.
3. Law / Regulations permits group registration with designated "signatory" SIM authority acknowledged by all members in written agreement.	• Increases documentation requirements and transaction costs, motivating for avoidance. • Ability to identify which actor within the group made a given transaction would require collaboration from the "signatory".
4. No regulatory action	• Account providers determine group use policy. • SIM card holder held accountable for transactions over the account motivating the SIM card holder to block illicit transactions by shared users. • Regulatory authority's ability to identify members of a group and which member of an informal group is the source/beneficiary of an illicit transaction will depend on collaboration by the SIM card holder whose account was used.

Policy Narrative:

While any policy option should be cognizant of the size and scope of transactions currently flowing through mobile financial services, those responsible for potential operational security risks should remain cognizant of the underlying concerns linking these services to the broader realm of financial services where illicit actors seek to actively conceal ownership structures. As the complexity of financial options offered via the mobile channel increases, so to must the recognition that illicit actors will increasingly employ the most convenient methods available that entail the least perceived risk. The term "beneficial ownership" refers to the control over funds versus mere signature authority. This reflects the fact that the person whose name is on an account may not necessarily be the person entitled to such funds or controlling the movement of such funds. For the purposes of anti-money laundering guidelines, identifying the person controlling the movement of funds is a critically important step in determining the source of funds .[56] Use of shared accounts is not permitted under FATF due to AML/CFT concerns, since such accounts effectively permit anonymity of most of the beneficial owners of the account.

The FATF framework generally requires the beneficial owner(s) of an account to be known to the financial institution so using one person to send/receive money on behalf of a community is not permitted.

Market Examples:

- **Tanzania:** A micro finance institution indicated that a corporate resolution was successfully used for group registration of SIM cards. A letter identifies and attests all registered owners of the SIM and a corporate "officer" is designated for cash ins/cash outs. The PIN code is split for security purposes.[57]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		x	x		x	x	x	x

Risk-based Policy Matrix – Appendix

1.19 Risk (Consumers):
"Government decides to tax transactions to raise funds increasing the marginal cost of each transaction."

Description:

Governments in need of revenues may see the high transaction volume mobile payment system as an opportunity. If governments decide to institute a transaction tax on mobile payment system transactions, they would raise the marginal cost of each transaction to consumers (as account providers would pass this cost along), thus pricing out many of the consumers that the system most benefits. The high adoption rate of mobile payments in most communities, and the benefits for expanding access to financial services, are driven largely by the low cost.

Objective:

- Keep the marginal transaction cost to a minimum

Policy Table:

Options	Implications
1. Government imposes a transaction tax	• Any transaction tax will reduce volume of the system. The consumers that leave the system will be the poorest, as they are the most price-sensitive. Thus, any transaction tax would be viewed by the public as anti-poor. • A transaction tax would complicate operations and accounting for account providers. • Some funds would inevitably be raised; but offset by the negative societal impact of decreased usage.
2. Government does not impose a transaction tax	• Mobile payment adoption rate, and expanded access to financial services, not inhibited by taxation.

Policy Narrative:
Bucketed –price plans, which are designed for low-income consumers, allow either unlimited text messages or a predetermined number of these SMSs over a defined period of time. In mobile financial services, the SMS is frequently used as the instruction message to convey a funds transfer or other type of mobile financial service. Regulatory authorizes levying a tax on this component of mobile financial services may be seen as stifling market expansion if the tax is not passed on to consumers or be accused of being "anti-consumer" if such a revenue-generating tax is passed on.

Market Examples:

- **Philippines:** Considered the text messaging capital of the world, the country averages 10-12 SMSs a day per its 70 million mobile subscribers. Government authorities recently proposed a 5 centavo ($0.001) tax, which was not to be passed on to consumers. The country's three largest telecommunications companies opposed the measure, claiming that it would be a burden on low income consumers. The head of the Philippine Long Distance Telephone regulatory affairs and policy office noted that 92% of SMS traffic is in the country is generated from bucket-priced plans. The ways and means panel of the 264-member House of Representatives approved the proposed tax to raise 36 billion pesos ($744.5 million) after Congress was reluctant to pass a proposal on alcohol and tobacco products.[58]
- **Turkey:** The tax burden on mobile users is higher than in any of the other 49 countries in a GSMA study from 2006. The study stated that 43% of the total cost of owning and using a phone in Turkey was a result of the taxes levied, in comparison to 18% in 50 other countries studied. Among the taxes noted were a Special Communication Tax (25%), the Treasury Share Premium (15%) and Value Added Tax (18%) on each mobile call made. When initially subscribing, users paid US $18, a Wireless License Fee of US $7.5, and Usage Fee of US &.5 per annum, in addition to the then proposed new Environmental Contribution Fund tax of US $9. The GSMA, a global trade association for mobile operators globally, concluded that economic growth in the mobile channel was being limited in Turkey as a result of the tax burden on the mobile users.[59]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
			x			x	x	x

Risk-based Policy Matrix – Appendix

2.1. Risk (Merchants):

"Merchants are unable to easily convert mobile money into cash limiting their flexibility to run their business / store."

Description:
Merchants accepting mobile money may not be able to rely on regular, flexible, and consistent methods to exchange electronic money into cash or use electronic money to trade with their suppliers. If they take in mobile money, but their suppliers do not accept mobile money, their ability to restock efficiently may be limited.

Objective:

- Merchants able to cash out as needed for liquidity management.

Policy Table:

Options	Implications
1. Regulatory authority requires Account Providers to maintain an "agent of last resort" within specific geographic areas to ensure liquidity for consumers.	• Such regulation likely unenforceable, since cannot dictate the composition of account providers' networks or related contracts. • It is in the interest of Account Providers to provide an efficient agent network to ensure market penetration, regulatory intervention is likely unnecessary.
2. No regulatory action	• Merchants will adopt mobile payment capabilities into their business model when they can either use mobile money balances with suppliers, or when they can depend on agents to maintain liquidity. • It is in the interest of account providers to ensure an efficient agent network. Monitoring of complaints of inadequate access could feed into license considerations.

Policy Narrative:
Merchants are unlikely to adopt a product as a critical part of their business infrastructure, until the infrastructure itself has proved reliable to meet their needs. A merchant, thus, will not adopt mobile payments as a payment option if they do not believe they can readily cash-out when needed. Regulators can require an "agent of last resort" within specific geographies to ensure availability and liquidity, yet the market is likely to drive this change more quickly, as the reputation of the service would be at risk.

Market Examples:

- ***Please Note:*** *A market example of a policy action associated with this risk was not identified during the literature review or the in-country consultations included in this project's scope. We welcome your suggestions of relevant examples for inclusion in subsequent versions.*

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		x		x		x		

Risk-based Policy Matrix – Appendix

2.2. Risk (Merchants):

"Merchant could be restricted by a contract with a payment provider from accepting payments for or from another account provider."

Description:

Merchants locked into exclusivity agreements may be precluded from offering their clients better and/or less costly services from other account providers.

Exclusivity agreements may provide economic justification for market entry of the first provider, but then may perpetuate a monopoly.

Objective:

- Balanced exclusivity agreements that facilitate market entry economies of scale yet prevent unreasonable restrictions on competition.

Policy Table:

Options	Implications
1. Exclusivity agreements restricted by law or regulation to balance short term market entry facilitation against longer term market competition, possibly through time limitations.	• Allowing or not disallowing exclusivity agreements may encourage market entry, but then block longer term competition. • Blocking all exclusivity agreements could discourage first mover market entry. • Requires regulatory monitoring of account provider agreements with agents and associated regulatory costs.
2. Regulatory authority requires interoperability of payment networks (through inter-provider links or switch)	• Requirement of interoperability would lessen the inconvenience of any exclusivity agreements with merchants as they would still be able to make a purchase, though a fee may be involved. • Requirement of interoperability would raise the cost for new entrants.
3. Competition agency empowered to investigate non-competitive behavior	• Requires a competition agency with the capacity to investigate and enforce non-competitive behavior. This is not a unique issue to mobile financial services. • Actions to restrict exclusivity agreements that harm consumers will discourage their use in mobile financial services too.
4. No regulatory action	• Exclusivity agreements are possible; however, experience with networked technologies (cell phones/ATMs) suggests that the market will move toward interoperability without regulatory action.

Policy Narrative:

Anti-trust legislation typically focuses on avoidance of monopolies and mergers and acquisitions (M&A) in an effort to prohibit companies within any one industry sector or sectors from dominating and being able to set or fix market prices. Cartels, groups of independent companies associated for the purpose of fixing high prices by agreement, are similarly discouraged. If account providers are signing merchants up exclusively, so that it restricts customer choice or unfairly restricts entry, it should be evaluated by the national competition agency.

Market Examples:

- ***Please Note:*** *A market example of a policy action associated with this risk was not identified during the literature review or the in-country consultations included in this project's scope. We welcome your suggestions of relevant examples for inclusion in subsequent versions.*

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
						x	x	x

Risk-based Policy Matrix – Appendix

3.1. Risk (Agents):

"Agent is unable to easily liquidate e-money inventory when the agency relationship is terminated."

Description:
Agents that voluntarily or involuntarily lose their agent status must be able to convert their e-money inventory to cash or deposit in a bank account.

Objective:

- Cash out procedures are covered in the agency agreement.
- Contractual disputes between account provider and agents subject to court resolution.

Policy Table:

Options	Implications
1. Regulatory authority requires providers to facilitate agent cash-out upon termination.	• Requirement mitigates agent liquidity risk in case of termination. • Requirement removes a potential barrier for entry of new agents, if they are uncertain of the market or the account provider. • Enforcement may be limited to review of agent agreement templates.
2. Provider sets contractual agent termination provisions with guidance from the regulatory authority.	• Provisions set expectation for agents upon contract initiation. (Provisions should enable liquidation within a timely manner.) • If provisions do not ensure a timely liquidation, this may constitute a barrier to entry for new agents.
3. No regulatory guidance	• Account provider has a commercial interest in enabling existing agents to exit: to reduce barriers to new agents. • Account provider sets own contractual obligations to liquidate agent's e-money inventory in a timely manner. • Agent may liquidate balances via other agents. • Lack of clear exit strategy at termination may constitute a barrier to entry for new agents.

Policy Narrative:
Upon termination of the agent relationship, the agent will likely want to cash-out part, or all, of their e-money inventory. As agents will carry larger inventories than the average consumer, other agents may be unwilling, or unable, to service their cash-out request. To avoid this situation, the agent agreement should provide a process for agent cash-out. If viewed as a significant issue, regulators could require such a procedure.

Market Examples:

- ***Please Note:*** *A market example of a policy action associated with this risk was not identified during the literature review or the in-country consultations included in this project's scope. We welcome your suggestions of relevant examples for inclusion in subsequent versions.*

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
x	x	x	x	x	x	x	x	x

Risk-based Policy Matrix – Appendix

3.2 Risk (Agents):

"Agent receives cash from client but fails to provide/transfer the e-money."

Description:

Agent receives funds from a service user but misdirects funds to the agent's own benefit. This situation could arise in one of two ways:

The consumer could be an existing customer without their phone with them, so they would not receive the transaction confirmation while with the agent.

The consumer may not be a customer but requests that the agent sends money to an existing customer, so does not receive independent phone confirmation of the transaction.

Objective:

- Effectively constrain diversion of funds.

Policy Table:

Options	Implications
1. Require that service users receive, and know they have a right to receive, clear confirmation that funds have been received and where they have been directed. This may include a paper receipt, if the customer does not have a phone, or if the individual is not a customer.	• Public confidence issue - in the account provider's interest to ensure that clients are not defrauded. • Police may need training on dealing with complaints of abuse. • Agents require protection from spurious claims of non-receipt.
2. Require that service users receive, and know they have a right to receive, clear confirmation that funds have been received and where they have been directed. This may include a paper receipt, if the customer does not have a phone, but would not apply to non-customers requesting 'informal remittance' service from an agent, (i.e. when the service is not formally offered by the provider).	• Public confidence issue - in the account provider's interest to ensure that clients are not defrauded. • Police may need training on dealing with complaints of abuse. • Agents require protection from spurious claims of non-receipt. • Non-customers receive no more protection in this situation, than if they asked any user on the network to provide the same service.
3.. Raise public awareness that users should have their cell phone available to ensure receipt of transaction confirmations.	• Reduces the need for potentially costly and unenforceable rules to ensure agents are crediting the proper accounts.
4. No confirmation requirement	• Customers requesting cash-in or remittance service

Options	Implications
	without their phone present are at risk of losing cash if the agent decides to misdirect the money, or not process the transaction.

Policy Narrative:

Consumer protection and public awareness campaigns, whether considered a reputational cost of doing business by first market entrants or regulated, may be the only risk inhibiting factor against this type of fraud.

Market Examples:

- **Afghanistan:** Discussing the critical importance of high-quality, expansive agent networks, a recent USAID study noted the sparse agent coverage of even the most popular systems as a continuing concern. Identification and public awareness campaigns for companies like M-Paisa have been extensive, but still may not mitigate the risks of those falsely posing as agents in sparsely populated or uncontrolled areas. In Afghanistan, there are more than 3,500 Roshan agents across the country, though only about 700 are trained on M-Paisa. Additionally, of those trained, only about 300 are active M-Paisa agents. Further impeding M-Paisa's growth is the fact that agents are not available to complete transactions nor, if available, agent liquidity is an issue.[60]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
			x		x	x	x	x

Risk-based Policy Matrix – Appendix

3.3. Risk (Agents):
"Agent is robbed."

Description:

Agents that hold both cash and e-money face a risk of robbery. The risk may be heightened if the volume of cash/e-money required follows a predictable remittance cycle, requiring a higher than normal cash on hand position. Agent may be forced to transfer all or part of its e-money inventory to the robber or other party. However, agents that are also merchants may find that accepting e-money as payment for goods and services sold reduces the need of cash on hand, and the risk of robbery.

Objective:

Agent responsibility for cash security should be clearly outlined in the contract with the account provider.

- If the payment system is e-money, cash is owned by its bearer so cash security is the responsibility of the bearer agent.
- If the agent is *deposit*-collecting, the cash in the till may be the customers', in which case greater security measures may be necessary.

Policy Table:

Options	Implications
1. Regulatory authority requires agents to be insured (whether by provider or self-provided)	• Insurance provides protection in case of theft. • Insurance requirement may constitute a barrier to entry for providers and /or agents.
2. Provider informally agrees to make the agent whole based on sufficient evidence of robbery.	• Agents will not view theft as a barrier to entry, as they will bear the theft losses. • Creates moral hazard that may encourage thefts.
3. No account provider or regulatory action - local police matter	• Agents bear liability for theft losses. • Agent liability may create a barrier to entry.

Policy Narrative:

Insurance policies typically may be designed for cash-intensive businesses that cover burglary and robbery, including options for coverage of guards, robbery insider and/or outside of the premises, safe burglary, property damage resulting from the acts of burglary or robbery, burglary of merchandise, theft from the courier transporting funds to and from financial institutions. In any case, the concern, particularly for a start up business, would be the potential barriers to entry of required insurance or, should insurance not be mandated but be unaffordable, losses resulting from a lack of an affordable policy.

Market Examples:

- ***Please Note:*** *A market example of a policy action associated with this risk was not identified during the literature review or the in-country consultations included in this project's scope. We welcome your suggestions of relevant examples for inclusion in subsequent versions.*

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		x			x	x	x	x

Risk-based Policy Matrix – Appendix

3.4. Risk (Agents):

"Agent threatened with individual customer demands or potentially larger group protests due to inability to perform cash-out transactions."

Description:

Agent unable to perform cash out transactions due to KYC/CDD policies, insufficient cash on hand to meet occasional heightened demand, and/or system/network outages.

For example, the account provider's system may be down, preventing KYC/CDD and transaction verification.

Customer may have lost ID, pin code or phone; an updated account provider policy may prevent agent from resetting pin without sufficient credentials, thus excluding the cash-out transaction.

Objective:

- Market access issue between account provider and its customers, impacting the account provider's market reputation.
- Only becomes a regulatory issue if customers cannot reasonably retrieve their funds through other agents. Otherwise, police/public orders issue.

Policy Table:

Options	Implications
1. Account agreement or regulatory requirement stipulates access requirements and service levels. (see 1.2, 1.7, 1.8 and 1.9)	• Account agreement or regulatory requirement mitigates unreasonable expectations. • If inability to meet service levels becomes a problem, customers can take legal action. More likely, customers would simply switch providers.
2. No regulatory action	• Local police relied upon to handle civil disorder issues.

Policy Narrative:

This risk refers to the amount of capital (both cash and e-money) held by agents, available for cash in/cash out transactions. In many mobile financial services systems, agents are the primary human interface with the consumer. Initial consumer confidence in a MFS system is, to a large degree, contingent on their ability to conduct cash-in/cash-out transactions. Consequently, maintaining a viable agent infrastructure is an important element of a strong MFS system.

To date, MFS providers have used commercial practices (e.g., commission structures, agent vetting processes, prepaid e-money reserves) to drive the proliferation of cash in/cash out agents. Market forces have determined which agents remain viable. MFS providers generally have not developed service level agreements (SLAs) with agents requiring them to maintain cash balances.

Recent MFS conferences (e.g., M-Banking 2009, Kenya School of Monetary Studies, May 2009) have raised the issue of an unregulated, ad hoc, cash in/cash out infrastructure and the impact this has had on consumer confidence. While the issue is viewed as significant, most experts agree that a regulatory solution would be difficult to craft and implement. The current view is that consumer demand and market forces will dictate the number of agents and the operating principles that govern agent conduct (e.g., availability of cash, hours of operation, etc.)

Market Examples:

- **El Salvador:** Under Article 1 of the Banking Law, deposit-taking, financial intermediation, and "other activities carried out by banks", permits the Central Reserve Bank (BCR) to authorize other operations and services. Banks are subject to regulation ranging from prudential to management and ownership rules, with licensing by the Superintendence of the Financial System (SupFin). However, a different framework governs member-based financial institutions, most of which were not subject to supervision by SupFin. This financial sector, comprised of savings and loan societies and cooperative associations, recently pushed for a new law allowing deposit-taking from the general public. While there is no specific regulation on the issuance of e-money by non-banks, the activity by this sector is defined as taking deposits and intermediating those deposits. According to a recent CGAP Branchless Banking Assessment, it is widely assumed that Salvadoran regulators would strictly apply this definition to e-money schemes and deem such activity to be banking activity, particularly if funds are to be intermediated. [61]
- **India:** Acknowledging the development of the mobile channel, The Reserve Bank of India (RBI) issued the Operative Guidelines for Mobile Banking Transactions (2008) pursuant to the Payment and Settlement Systems Act (2007). Only banks licensed, supervised and with a physical presence in India may offer mobile banking to their existing customers. These institutions must obtain prior approval of RBI before launching their service offering. MNOs and nonbank financial institutions may not offer mobile banking services. Cross-border and foreign remittances are not permitted. Daily transaction limits are set at Rs 5,000 for transfers and Rs 10,000 for goods and services purchases. Two factor authentication, including a PIN is required on all transactions, with a limit of Rs 50,000.[62]
- **Kenya:** A recent study on the community level effects of M-PESA on local economic activity indicated that money circulation was the most highly ranked of all effects. It was consistently identified by respondents (being ranked most important by men and no. 3 by women) as infusing cash into the community via remittances where they appeared to be needed most. The higher and faster circulation, in turn, contributed to expansion of businesses, food security, human capital accumulation, and rescue money (emergency funds), as well as increased employment opportunities.[63]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		x	x	x	x	x	x	x

Risk-based Policy Matrix – Appendix

3.5. Risk (Agents):
"Agent takes in cash that proves to be counterfeit."

Description:
Counterfeiter manufactures false notes to pass through agent and to integrate into the money supply.

Objective:

- Responsibility for accepting counterfeit currency for transfers the same as for sale of goods - with the agent.
- Agent training on counterfeits, and other illicit financial instruments, to be modeled on bank teller training and provided commensurate to the perceived risk.
- Account provider training program for agents subject to regulatory assistance/verification.

Policy Table:

Options	Implications
1. Regulatory authority provides mechanism for reporting, retrieval, and criminal investigation of suspect counterfeit notes. Regulatory authority sets parameters for training material for use by account providers with their agents.	• May incentivize agent to report counterfeit activity. • Reporting facilitates identification of issues, investigation, and apprehension of counterfeiters. • Regulatory authority requires capacity/budget to support anti-counterfeiting training and enforcement.
2. Account providers required, as part of AML/CFT/Fraud training programs, to institute and monitor agent compliance commensurate with perceived risk.	• Training facilitates identification of issues, investigation, and apprehension of counterfeiters. • Active program will deter use of agents to pass counterfeit notes.
3. No regulatory response to counterfeit currency in circulation.	• Increasing circulation of counterfeit currency. • However, agents have a vested interest in identifying and rejecting counterfeit notes since these would be rejected if deposited in the agent's bank account.

Policy Narrative:
As international authorities dealing with this issue reiterate, the crime of counterfeiting national currency is as old as the creation of money itself. With the advent advanced personal computer graphics programs and low-cost, high quality photographic and printing technologies and equipment available to the lay person, the ability to reproduce complex images on paper stock has never been easier. The resultant effect of this bogus currency introduced into circulation poses problems not only for national economies, but also for financial institutions, consumers, and economies worldwide. The intersection of mobile financial services and the use of national currencies, in this regard, pose similar need for international cooperation and private/public partnerships. These may be encouraged through such law enforcement organizations as INTERPOL, which maintains expertise through their Counterfeit and Security Documents Branch (CSDB), providing forensic support, operational assistance, and technical databases to assist the 188 member countries of INTERPOL regarding counterfeit national currencies[64]

Market Examples:

- **Kenya:** "Sec. 373 Any person who – (a) utters any counterfeit coin knowing it to be counterfeit, and at the time of such uttering has in his possession any other counterfeit coin; or (b) utters any counterfeit coin knowing it to be counterfeit, and either on the same day or on any of the ten day next ensuing utters any other counterfeit coin knowing it to be counterfeit; or (c) receives, obtains or has in his possession any counterfeit coin knowing it to be counterfeit, with intent to utter it, is guilty of a felony and is liable to imprisonment of three years."[65]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		x	x		x	x	x	x

Risk-based Policy Matrix – Appendix

3.6. Risk (Agents):
"Agent pays out cash that proves to be counterfeit.

Description:

Agent may pay out counterfeit currency received from customers without realizing it is counterfeit. Agent may use cash-out payments to distribute counterfeit currency. Agents may "get rid of" counterfeit currency they realize they have taken in by passing it on.

Objective:

- Passing counterfeit currency, whether as cash outs to e-payments or as change on trade purchases, is a criminal issue for the police, not a regulatory issue.
- However, account providers should provide agent training on counterfeits, as for 3.4.

Policy Table:

Options	Implications
1. Regulatory authorities should provide mechanism for reporting, retrieval, and criminal investigation of suspect counterfeit notes.	• Reporting facilitates identification of issues, investigation, and apprehension of counterfeiters. • Regulatory authority requires capacity/budget to support anti-counterfeiting training and enforcement.
2. Regulatory authorities to provide an incentive, or reward, system for reporting and retrieving counterfeit currency, possibly including cash payments.	• Financial incentives can increase cooperation of agent network in identifying and pursuing counterfeiters. • Regulatory authority requires budget to support incentive program. • Financial rewards may encourage agents to collaborate with counterfeiters; however, authorities will monitor agents more closely that consistently turn in counterfeits for reward.
3. Account providers required, as part of AML/CFT/Fraud training programs, to institute and monitor agent compliance commensurate with perceived risk	• Training facilitates identification of counterfeit currency and deters acceptance/distribution. • Agents may recirculate counterfeit currency if not incentivized or required to report it.
4. Regulatory authority or account provider could reward agents for identifying counterfeit currency or providing information on counterfeiters.	• Reward could provide the incentive for identification and the disincentive for passing the currency along. • Agents with frequent identification would need monitoring to ensure they were not involved in a counterfeit scheme. • Cost/capacity to implement such a scheme would need to be evaluated.
5. No regulatory oversight or training by account provider of agent	• Increased circulation of counterfeit currency.

Policy Narrative:

As international authorities dealing with this issue reiterate, the crime of counterfeiting national currency is as old as the creation of money itself. With the advent advanced personal computer graphics programs and low-cost, high quality photographic and printing technologies and equipment available to the lay person, the ability to reproduce complex images on paper stock has never been easier. The resultant effect of this bogus currency introduced into circulation poses problems not only for national economies, but also for financial institutions, consumers, and economies worldwide. The intersection of mobile financial services and the use of national currencies, in this regard, pose similar need for international cooperation and private/public partnerships. These may be encouraged through such law enforcement organizations as INTERPOL, which maintains expertise through their Counterfeit and Security Documents Branch (CSDB), providing forensic support, operational assistance, and technical databases to assist the 188 member countries of INTERPOL regarding counterfeit national currencies[66]

Market Examples:

- **Kenya:** "Sec. 373 Any person who – (a) utters any counterfeit coin knowing it to be counterfeit, and at the time of such uttering has in his possession any other counterfeit coin; or (b) utters any counterfeit coin knowing it to be counterfeit, and either on the same day or on any of the ten day next ensuing utters any other counterfeit coin knowing it to be counterfeit; or (c) receives, obtains or has in his possession any counterfeit coin knowing it to be counterfeit, with intent to utter it, is guilty of a felony and is liable to imprisonment of three years."[67]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		x	x	x	x	x	x	x

Risk-based Policy Matrix – Appendix

3.7. Risk (Agents):

"Provision of credit to agents by non-bank actors

Description:
Network models allow super agents/master agents to extend liquidity in the form of e-money directly to agents with no controls or oversight.

Objective:

- Liquidity needs of account providers should be balanced with consumer protection for agents so that extension of credit does not become a vicious cycle.

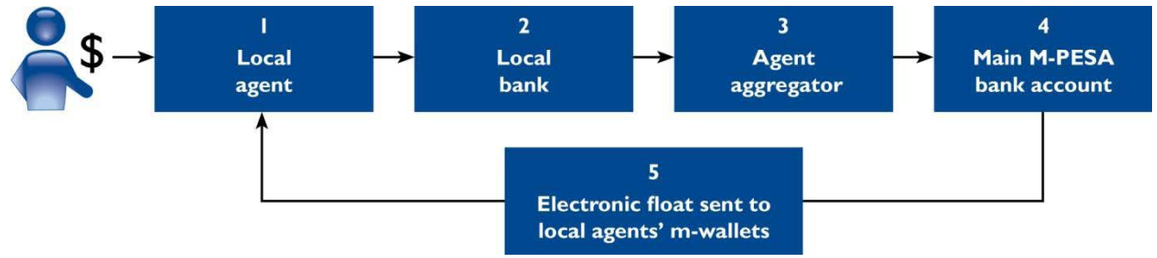
Policy Table:

Options	Implications
1. No regulatory action	• Agents and super-agents will manage their own credit needs and indebtedness, as any small business.

Policy Narrative:
Most agents are responsible for maintaining a balance of cash to service their customer base's needs. As such, some may seek credit from moneylenders, or other credit providers, risking potential over-indebtedness. However, the market, overtime, will sort out the competent agents from those that cannot manage their responsibilities. Agent liquidity requirements or service levels may lead providers to play a more proactive role in liquidity management, which could result in their providing credit to super-agents, employing super-agents and providing them with budget for liquidity management—see 1.9 for more on agent liquidity issues.

Market Examples:

- **Tanzania:** Vodacom received GSMA's MMU grant to support M-PESA aggregator agents to overcome liquidity issues experienced by lower-tier agents. It may be several days before agents receive e-money transfers to phones, because the electronic money moves from the local bank, through the agent aggregators, to the M-PESA bank account before it appears in the agent's m-wallet. To overcome the delay in step 5 (see diagram below), Vodacom provides credit to its aggregators, who are responsible not only for the selection, supervision and training of the local agents, but also with supplying them with electronic money without requiring advance payment prior to providing the electronic float. This is supposed to increase the agent's float, while simultaneously covering the cost of credit to the agents and client satisfaction/increasing transaction volume. [68] A USAID interview with a local super agent confirmed the need for this practice.[69]



Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		x		x		x		x

Risk-based Policy Matrix – Appendix

4.1. Risk (Account Providers):

"Provider employee manipulates agent credit allowances, agent e-money balances, or customer e-money balances for financial gain.

Description:
An insider with access to financial systems manipulates balances for his/her own financial gain.

Objective:

- Account providers responsible for their own internal security as a cost of doing business. Not a regulatory issue unless a) defalcations threaten the financial viability of the service, possibly providing a systemic impact, or b) service providers' customers are impacted, in which case the regulator has a consumer protection interest.

Policy Table:

Options	Implications
1. Regulatory authority requires providers to • obtain fraud insurance to protect against insider threats and • maintain 1:1 e-money reserve requirement in trust account. Depending on the liability loss, enlist law enforcement.	• Insurance will mitigate the risk of providers and the financial system against significant fraud risks. • Legal system must have the authority to arrest and prosecute those who committed the fraud. • Fraud insurance may not be available or may price providers out of entrance into the market
2. Providers implement institution specific fraud detection systems	• Fraud detection allows for issue identification, investigation and prosecution. • Variance across institutions may let criminals target weak systems; however, competition will allow for innovation.
3. No required regulatory response to insider employee provider fraud.	• Small-scale insider manipulation is unlikely to have much impact • Systemic fraud by insiders could damage the stability of the financial system and will significantly damage the reputation of the mobile system.

Policy Narrative:
Fundamental to most business models is the integrity of the employees. However, without proper safeguards, employees may be tempted to steal from their employer. If an employee of a service provider set up new mobile money accounts with mobile money balances which were not backed by currency, they could use that mobile money, whether through a cash-out, merchant purchase, or person-to-person transaction, and create a liability for the service provider. In effect, they are stealing from their employer. Without proper safeguards (i.e. daily settlement and fraud protection, which would identify unbacked balance increases or account set-ups), such liabilities could go unnoticed, as the trust fund would not routinely be fully drawn down. Employees should be subject, whether by regulatory requirement or firm policy, to due diligence screening which would identify those with a criminal history. Further, fraud insurance could be purchased to hedge against such behavior. Again, either by regulatory requirement or firm policy, internal controls should be in place that would quickly identify cash-in transactions that were not backed by physical currency. Daily settlement across the agent network should highlight any anomalies and allow for investigation. With the legal and reputation risk that exists, service providers have no incentive to manipulate mobile money balances; however, employees may attempt to do so at their employer's expense. As such, regulators and providers must be diligent in establishing the proper controls that can mitigate the potential for any systemic impact.

Market Examples:

- **Philippines:** In writing how to protect against fraud and system abuse, a recent GSMA study recently cited the fact that "well-trained agents are the first line of defense." A Central Bank requirement is for agents to receive a full day of training and the bank, in conjunction with SMART Money, provides such new agent training. Back-end transaction monitoring was instituted and can assist to identify other forms of fraud. GCASH implemented a sophisticated fraud monitoring technology solution which screens billions of transactions, identifying suspicious transaction patterns and flagging them for further investigation.[70]
- **Pakistan:** The State Bank of Pakistan (SBP) has regulatory authority over the payment systems that process payment instruments and e-money under the Payment Systems and Electronic Fund Transfer Act (2007), Section 3. This Act defines electronic money : "e-money is transferred through an electronic terminal, ATM, telephone instrument, computer, magnetic medium or any other electronic device…" The ACT also provides a range of institutions, not only banks, which may apply to issue electronic money, thereby becoming, "electronic money institutions." The Branchless Banking Regulations dated March 31, 2008, however, provide that those regulations do not apply to e-money, though there are provisions that do address risks posed by wireless networks. [71]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
x	x	x	x	x	x	x	x	x

Risk-based Policy Matrix – Appendix

4.2. Risk (Account Providers):
"Provider fails to adequately select, train and supervise agents and super agents."

Description:
Agents acting on behalf of a account provider can damage the account provider's business reputation, both with the public and with the regulator if they act improperly.

Objective:

- Account provider agent selection, training and supervision policies and procedures are acceptable to the regulator, subject to verification of compliance.
- However, this is primarily a business management issue rather than a regulatory issue unless agent performance problems become flagrant. Regulator may mandate KYC/CDD as a component of sound AML/CFT programs.

Policy Table:

Options	Implications
1. Regulatory authority trains and licenses agents to ensure capacity.	• Training and licensing can help to ensure a base capacity among agents. • Regulatory ownership or training licensing is high cost and requires capacity that the regulator is unlikely to have.
2. Regulatory authority requires provider to institute an AML/CFT/anti-Fraud training program which incorporates KYC/CDD guidelines. Training, compliance monitoring, and registration of agents is required by account provider.	• Training helps to ensure greater competence among the agent network, and thus a stronger, more stable mobile payment system. • The agent may not have sufficient training, resources or motivation to follow prescribed guidelines without threat of penalty or termination of agent relationship for non-compliance. • Regularity verification of training program is low cost and requires low capacity.
3. Provider institutes training program that certifies an agent according to policies and procedures of the company for KYC/CDD; may encourage agents to adopt sound business practices and follow government guidelines for KYC/CDD.	• Training helps to ensure greater competence among the agent network, and thus a stronger, more stable mobile payment system. • The agent may not have sufficient training, resources or motivation to follow prescribed guidelines without threat of penalty or termination of agent relationship for non-compliance. • No regulatory oversight of training program may allow sub-optimal programs.
4. No required training or licensing process for agents	• Agent selection entirely up to the account provider. • Lax screening and/or inadequate training could result in service quality problems.

Policy Narrative:
Training programs not only assist in protecting the financial account provider's reputation and the integrity of financial systems, they also reduce the likelihood of these institutions becoming a vehicle for or a victim of financial crime and suffering consequential reputational damage through the uninformed actions of their employees or designated third party account providers and agents. Additionally, such programs comprise an essential part of sound risk management (e.g. by providing the basis for identifying, limiting and controlling risk exposures in assets and liabilities, including assets under management). Providers, or their designees, should not only establish the identity of their customers, but should also monitor account activity to determine those transactions that do not conform with the normal or expected transactions for the financial footprint of that customer. Not only should KYC be a core feature of the provider's risk management procedures, it should be facilitated by the education of staff and complemented by regular compliance reviews and internal audit. A tiered approached to KYC/CDD is prudential based on the perceived degree of risk.[72]

Market Examples:

- **Indonesia:** The Money Transfer Regulation of 2006, requires a nonbank e-money provider to obtain a remittance license to offer P2P transfers, both domestic and international. Administrator is a person or entity that acts as a remitter agent or beneficiary agent of a money transfer, while an Operator merely provides the facility or system used for the transfer and/or performs the act of receiving or forwarding data and or information from one Administrator to another. This regulation does not permit Administrators to undertake money transfer activities through their owned networks or those provided by an Operator, or through a network of agents. Thus, the use of agents by non-banks is prohibited. Neither does the Regulation permit money remitters to conduct transactions through their agents. According to CGAP, "Current regulations would require every airtime dealer to apply individually for a remittance license, unless the airtime dealer is a 'branch office' of a money remittance license holder."[73]
- **Kenya:** The Registration of Persons Act requires all Kenyan citizens reaching the maturity of 18 years to be issued a national ID card after registering with the National Registration Bureau. This provides a unique identifier in Kenya.[74] For KYC purposes, the M-PESA agent collects the name, identification number (national ID or passport number), ID type, and date of birth of each user at the time of registration and enters this information into an electronic database. Safaricom retains this data for 10 years. Unless a fraud complaint or a high transaction occurs, the national ID is not cross referenced against the National Registration Bureau Database. In terms of the transactions on M-PESA, the data captured includes whether an agent was used and whether or not it was with a registered or unregistered M-PESA user. MNOs track every transaction detail on their network,

Risk-based Policy Matrix – Appendix

whether call or text, forming the call detail records. This includes the date and time the call started and ended, the number dialed, if it was caller initiated or roaming, etc.[75]

- **Palestine:** According to the Palestinian National Authority, The President, Anti-Money Laundering Decree Law of 2007, financial institutions and nonfinancial businesses and professions should institute and implement programs to prevent money laundering, which include, among other activities, the "ongoing training of officials and employees to help them identify transaction and actions linked to money laundering and to know the procedures which they must follow in such cases."[76]
- **South Africa:** Questions regarding outsourcing arrangements were addressed in guidance provided by a 2004 South African Reserve Bank (SARB) circular. While the circular does not specify which bank functions may be outsourced, it does clarify that the internal audit function may be outsourced on a case-by-case basis only and the compliance function may not be outsourced at all for a bank. Banks are left with discretion over outsourcing arrangements provided that the agreements are legally scrutinized and services are adequately performed in accordance with the institution's internal policies and procedures. This may include access to the outsourced entity by both the bank's internal and external auditors, as well as external agencies and SARB on outsourced functions and activities.[77]
- **Zambia:** One provider indicated a multi-tiered approach to agent selection and training, which included reviewing initial selection of the location, reputation ID, verification of the physical address, bank account, business license, as well as training on KYC documentation, account opening and maintenance, and assignment of a Customer Care Representative for ongoing support. The agents are also tiered as to service offerings: the top tier agency is a standalone location capable of supporting itself through cash in/cash out transactions and may obtain start up loans; the second tier is placed in strategic locations, such as service stations, where other cash-related business may support the agency; the third tier is reserved for those areas where the cash flow may be constrained, with low-end transactions of $100 or less.[78]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x		x			x	x	x

Risk-based Policy Matrix – Appendix

4.3. Risk (Account Providers):

"Account provider or provider's agent does not meet required regulatory responsibilities for AML."

Description:

Depending on the division of responsibilities, some AML procedures could be carried out by agents. Agents are generally not employees of the account provider and thus are related only through contractual arrangements. If roles are not clearly stipulated and enforced, compliance can be difficult.

Objective:

- Account providers complying with such regulatory oversight as provided in law and regulation, including effective suspicious transaction reporting.
- Predictable and enforceable penalties for non-compliance sufficient to motivate routine compliance.

Policy Table:

Options	Implications
1. Regulatory non-compliance results in corrective action and fine. Repeated non-compliance or significant instances of non-compliance will lead to a cease and desist order to the account provider.	• Penalties will create disincentive for non-compliance. • Implies that the regulatory authority has sufficient staffing and financial resources available to demonstrate effective enforcement.
2. Provider's agent agreement allows for termination for non-compliance.	• Termination threat will create a disincentive for agent non-compliance. • Despite contractual obligations of the agents, ML/TF risks will remain if not appropriately monitored by account provider and enforced by regulatory authorities.
3. No civil or criminal penalties for provider or provider's agent for non- compliance	• Enforcement of AML problematic, increasing risk of FATF censure.

Policy Narrative:

One risk-based approach is known as point-based KYC. This approach may be less restrictive for both agents and consumers, as it presumes the more KYC evidence a customer can provide (ranging from a national ID, passport, physical presence, utility bills, introduction by other clients, driver's license, etc.), then the more proportional the risk is to the institution. Services are then offered on a basis proportional to the perceived risk.

Chatain et al identified several innovative risk mitigating factors in mobile banking and securities accounts, or those similar to other electronic channels such are utilized in electronic banking channels for Internet banking and ATMs. National authorities may standardize national public identification to facilitate documentable measures to verify the customer and/or beneficial owner's identity when conducting transactional activity or establishing customer relationships. In the absence of a national customer ID, national authorities may provide for alternative ID instruments to comply with these requirements. All ID requirements should pay special attention to money laundering and terrorist financing threats that may arise from the anonymity of new or developing technologies.

Simplified or reduced CDD measures could apply to the beneficial owners of pooled accounts held by designated non financial businesses or professions, in the event such individuals are subject to AML/CFT requirements and related monitoring. The Basel CDD paper may provide guidance to financial institutions holding such accounts as well (see Section 2.2.4).[79] In the absence of a national customer ID, Banks, MNOs and agents should have policies and procedures in place to address specific risks associated with new or developing technologies that permit remote and non-face-to-face business relationships and transactions, in addition to any risks associated with the nested agent relationships that might obscure customer identities in the payment chain.

Market Examples:

- **Cambodia:** WING is a payment platform wholly owned by ANZ Banking Group, which partners with ANZ Royal to hold client deposits. It launched an m-banking, USSD solution with SMS receipting in January 2009 that is capable of working with any MNO. WING currently offers airtime top-ups, bill payments, and money transfers, and has partnered with five telcos in Cambodia. WING continues to engage the National Bank of Cambodia (NBC) since electronic money legislation is still being developed and keeps in close contact with the bank regarding this. In the meantime, it WING operates under a letter of no objection issued by NBC.[80]
- **India:** Under the Prevention of Money Laundering Act of 2002, the law issued AML guidelines, including KYC standards. Banks were advised to tier customer risk according to low, medium, and high, adjusting account ID requirements. Reserve Bank of India's 2005 Circular relaxed the proof of residence requirements of small value accounts, permitting identity and address verification via introduction by another account holder who passed full KYC in at least the preceding 6 months.[81]
- **Kenya**: Under Kenya's Registration of Persons Act, citizens 18 or over must register with the National Registration Bureau and obtain a national ID. Failure to do so is a crime. Individuals obtaining citizenship by birth only need to demonstrate that one parent is a Kenyan citizen, usually by presenting a parent's national ID. However, for Nubians, Kenyan Somalis, and coastal Arabs, the standard is stricter. Registration officials have broad discretion under Section 8 of the Registration Act, which permits officers to require an applicant to produce additional evidence. The Principle Registrar may demand proof of "other particulars as may be prescribed (Section 5)." Moreover, under Kenyan citizenship law, women cannot pass nationality to their children. Children of "unknown origin" or who might otherwise be stateless, including some orphans and street children, are not automatically granted Kenyan nationality.[82] Refugees cannot naturalize, increasing the risk of statelessness over time. In terms of flexible ID requirements for users, account provider M-Pesa accepts a national ID, a passport (Kenyan or foreign), Alien certification, and military or diplomatic IDs. It is also is considering lowering the minimum age of its users from 18 to 16 with parental consent.[83]

Risk-based Policy Matrix – Appendix

- **Korea:** According to one study, TelCos in many jurisdictions where m-FS predominates did not sufficiently perform CDD on non-residents; it is recommended that enhanced KYC and CDD be performed for such customers similar to the manner in which banks perform such measures. In Korea, there are comprehensive procedures in place for mitigating the risks of anonymity with cooperation between the banks and the TelCos. To conduct m-FS, a customer must hold a bank account, travel in person to the bank branch and provide ID (a valid passport for foreign citizens), and complete a funds transfer form in order to receive access to e-banking. Upon completion of these steps, an ID and password are issued to the customer, as well as a letter permitting the customer to obtain a SIM card from the TelCo. Service for m-FS is available only to post-paid individual subscribers, rather than corporate entities.[84]
- **Zambia:** Engaging regulators by sharing information on technologies and proposed AML, KYC/CDD procedures at each stage of product initiation has provided nonrestrictive environment for mobile financial services to develop. For instance, under the auspices of the AML directives of 2004, the KYC procedures allow for the use of alternative verification methods when identifying a potential bank customer. Opening an account, the law requires a national registration card, driver's license, or passport, and proof of name and address. Flexibility is permitted in that once a customer receives his/her identity document, another bank customer, the potential customer's employer, or a village chief can verify his/her identity.[85]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
x	x	x	x		x	x	x	x

Risk-based Policy Matrix – Appendix

4.4. Risk (Account Providers):

"Trust fund is inadequately funded."

Description:

The account provider fails to adequately fund the trust account, thereby making the trustee inoperative.

A trustee's fund investment strategy fails to conserve the fund's value.

Objective:

- Trust funds are regulated and supervised similar to insurance reserve accounts to ensure adequate coverage of trust liabilities.

Policy Table:

Options	Implications
1. Regulatory authority requires minimum1:1 reserve requirement which is monitored through daily/weekly reporting with tiered enforcement options, including fines for non-compliance.	• Reporting requirements allow banks/providers to demonstrate to regulators and consumers their stability and soundness by meeting their requirement. The frequency of the reporting creates greater assurance, and thus lower risk. • Reporting requirements will impose a cost on banks/Account Providers. • Frequent reporting requirements could create a capacity issue for regulators that do not have the staff to review reports and monitor compliance.
2. Regulator requires trustee to be bonded to cover the performance risk.	• Bonding will diversify the exposure of stakeholders; however, the cost could create a barrier to entry. If the cost is passed on to customers, the adoption/usage rate might slow. • Bonding costs could be covered by the interest that the trust accounts generate. • Monitoring and enforcement will focus on the acceptability of the bonding (insurance) company and the coverage provided.
3. Regulatory agency creates a new type of deposit insurance at the payment account holder level.	• Not needed for bank Account Providers Account Providers, since funds already on deposit in covered bank accounts. • For cell-phone based Account Providers Account Providers with pooled trust funds, this would substantially expand deposit insurance beyond current global practices and dilute the incentive for service users to open a formal bank account.
4. No regulatory action.	• Customers may lose mobile money balances if account provider is not managing trust accounts appropriately.

Policy Narrative:

The non-bank account provider is responsible for ensuring that funding of the trust account covering the value of payments in transit is adequate to cover the sum of the value of those payments. The trustee's primary responsibility is to protect the value of those funds in the trust account to ensure that no losses are incurred that would impair that coverage. It is incumbent on the account provider to chose a qualified trustee, and on the trustee to develop and comply with a sound investment strategy that will ensure that the value of the trust account is preserved and that the trust account provides adequate liquidity to ensure that all payment obligations can be honored. In its *Examiner's Guide to Problem Bank: Identification, Rehabilitation, and Resolution* document, the U.S. Comptroller of the Currency noted prior to the recent financial crisis that the increase in national bank securitization activity and the proliferation of capital markets products had shifted increasing levels of credit risk to off-balance-sheet transactions. The credit risks inherent in capital market products, such as asset securitizations and derivatives, is difficult to quantify due to the need to assign a credit risk equivalent to these types of instruments. A bank that engages in securitizations needs to be fully aware of relevant risk-based capital rules applying to these transactions. As part of its overall internal controls and risk management policies, senior management and its supervising board of directors should include an assessment of off-balance-sheet and any other indirect exposures when determining the overall quantity of risk assumed by the financial institution that is custodian of a trust account. Moreover, both parties should ensure that all valuation methods and key assumptions used to value the residuals and servicing assets and liabilities associated with trust management are reasonable, fully documented, and well supported.[86]

Market Examples:

- ***Please Note:*** *A market example of a policy action associated with this risk was not identified during the literature review or the in-country consultations included in this project's scope. We welcome your suggestions of relevant examples for inclusion in subsequent versions.*

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
x	x	x		x		x	x	x

Risk-based Policy Matrix – Appendix

4.5. Risk (Account Providers):

"Agent fraud untraceable due to poor records."

Description:
Lax or non-existent record keeping of transactions by agents creates challenges for providers trying to research fraud issues. Transactions may be commingled among merchant receipts, possibly leading to fraud and agent employee theft.

Objective:

- Agents able to document their mobile financial transactions.
- Account Providers able to support police investigation of complaints of fraud.
- Regulatory involvement only in cases of systematic failure of account provider to ensure its agent network operates within reasonable bounds.

Policy Table:

Options	Implications
1. Regulatory authority requires agents to maintain paper records for a time period (consistent with other financial records) to support account provider's electronic records for investigation purposes.	• Audit trail requirements will discourage fraud, but may increase operating expenses and may not be complied with, particularly if fraud is involved. • Account provider's electronic records may be sufficient and more reliable.
Account provider operating and record keeping procedures developed, in concert with regulators, to support investigation in case of agent fraud.	• Generally in account provider's own interests to ensure transaction audit trails. • Providers will determine the degree of fraud protection on an institution by institution basis.

Policy Narrative:

In some cases, particularly when the service links "traditional" bank channel accounts to TelCo partners, AML/CFT obligations likely reside with the bank, as the primary financial institution responsible for providing m-FS. However, when the TelCo can be a channel through which other services are provided and the merchant can also receive payments and conduct non-bank account transfers, the line between financial and telecommunication providers blurs.

Chatain et. al posit that TelCos and some other non-bank entities providing m-FS should be included within the regulatory definition of "financial institutions" when according to FATF these TelCos function as: "any person or entity who provides its customer with transfer of money or values services, or issues and managers means of payment, inter alia, electronic money." This broad definition would permit the TelCo's AML/CFT to comport with the actual role it performs within the financial or non-financial sector.[87]

There is no consensus on how to implement standards internationally, though the majority of TelCos perform some KYC and CDD measures as best business practices.[88]

Market Examples:

- **Kenya:** In a recent presentation entitled "10 YEARS ON FROM THE US EMBASSY BOMB BLAST" in Nairobi, Kenya,"[89] Director Samuel Mutungi provided a case study on lessons learned for terrorist attacks regarding disaster recovery and business continuity planning for financial services. One of the main mitigating strategies aiding in recovery for Co-Operative Bank, despite the fact that the ICT equipment was damaged and networks/systems were destabilized, was that the Bank's systems back-up e.g , redundancies, had recently been moved off site.
- **South Africa:** The South African Financial Intelligence Center Act (FICA) permits electronic record keeping and outsourcing to third party intermediaries. For MTN group, the South African telecommunications company, client identification records are collected by agents, but forwarded to the main office for verification and retention.[90] Value in mobile financial transactions, at some point in the transfer, is typically stored on the computer servers of account providers or financial institutions. These servers, however do not have to reside in the country of originating activity. This may or may not create concerns for national regulators in terms of evidence collection, search, seizure, asset forfeiture/sharing, and information sharing.[91]
- **Philippines:** The use of new and developing technologies, such as the intersection of information and communications technologies and financial services, raises new areas of consideration in terms of records retention and retrieval. In the "Effects of Cell phone on Anti-Money Laundering/Combating Terrorism (AML/CFT) Wire Remittance Operations"[92] which examined mobile financial services practices in the Philippines, the author cites several emergent safety and soundness factors:
  i. Tests of electronic systems security, hardware, and software,
  ii. Tests of customer ID and point-of-sale samples,
  iii. Anti-virus protection,
  iv. Internal security policies and procedures for electronic systems,
  v. Cross industry and regulatory collaboration in records involving text and SIM cards, and
  vi. Critical infrastructure protection for the telecommunications and the financial sectors.

  Customer Detail Records: Mobile financial account providers maintain customer activity records (Customer Detail Records) similar to financial institutions and payment system providers. These detailed customer records relate to the mobile operator's system usage and include information relevant to AML and CFT, such as each mobile calls originating and receiving phone and the call's duration.
- **Malaysia:** In Malaysia, Maxis maintains ongoing transaction records for active customers and for terminated customer retains them for an additional seven years.

Risk-based Policy Matrix – Appendix

- **Hong Kong:** In Hong Kong SAR of China, AML regulations for mobile account providers require that records be maintained on all transactions over HK $8,000, however transactions below this figure are recorded in the mobile service provider systems, too.[93]
  Safeguarding electronic customer and business data: avoiding data leaks, and maintaining high – quality IT systems is a critical business enabler in records retention efforts for AML and CFT. In light of recent data leaks, e-finance regulations are emerging.
- **Macao SAR:** For instance, Banks in Macao SAR of China do not permit m-FS transfers outside of the same bank or internationally.
- **Philippines:** The Philippines caps m-FS transactions per day and per month in order to mitigate ML risks.[94]
- **Indonesia:** The Bank of Indonesia's Circular Letter 10/49/DASP outlines requirements for money transfer services conducted by nonbanks, requiring that individuals and entities apply for a money transfer license to provide not only their risk management procedures, including KYC. KYC must include verification of both sender and recipient at the time of the funds transfer (via government issued ID, driver's license, or passport). Additionally, the sender and recipient must be re-verified in the event the transfer exceeds IDR 100,000,000 (approximately USD 8,600), any suspicious transactions are detected, and there is concern as to the veracity of sender/receiver provided information. Additionally, nonbank providers must ask for information about the source of funds, as well as the purpose of the funds transfer; and have appropriate information systems in place for monitoring, analyzing and reporting transactions in which they engage and reporting suspicious transactions to the Financial Intelligence Unite and Financial Transactions and Reports and Analysis Center (PPATK)[95]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x	x	x		x	x	x	x

Risk-based Policy Matrix – Appendix

4.6. Risk (Account Providers):

"System availability cannot be maintained by account provider."

Description:

Customers will seek other providers, and potentially regulators will take action, if providers are unable to effectively maintain their system availability.

Objective:

- Account provider's services reasonably consistently available during normal business hours.
- Continuation of operating license contingent on maintaining reasonable service.

Policy Table:

Options	Implications
1. Regulatory authority mandates system redundancy requirements and disaster recovery to ensure continued financial system access, particularly for significant Account Providers.	• Redundancy and continuity will mitigate the risk of system availability and limit the duration when a failure occurs. • Documented alternative access procedures in the event of system failures for providers. • Regulations that focus on achieving the objective rather than prescribing specific procedures will enable account providers to innovate to provide the least cost solution. • Implies the regulator has, or can procure, the technical expertise to validate account providers' contingency plans.
2. Regulatory authorities permit off-shore data hosting and/or backup.	• In some jurisdictions where the infrastructure is weak, hosting data records in a more developed jurisdiction may be necessary to ensure adequate data security and integrity. • Can reduce operating expenses (and service fees) by facilitating economies of scale. • May require availability of fiber optic connections to ensure adequate band width. • May require agreement with hosting country regulator to verify compliance with data safety and security requirements.
3. Providers establish their own redundancy requirements and disaster recovery to ensure continued financial system access.	• Redundancy and continuity planning will mitigate the risk of failure in system availability and limit the duration when a failure occurs. • Should be supported by documented alternative access procedures in the event of system failures for providers. • Lack of regulatory requirement will allow each institution to define the extent of their contingency planning, which may leave some less protected than may be appropriate for a payment system. However, it will also allow individual institutions to innovate.

Policy Narrative:

The core components of any payment system must ensure availability, capacity, operational continuity, and security to the public that is being served. This may necessitate both integrating existing technologies in new ways, as well as providing interoperability among new actors with innovative technologies. The National Fire Prevention Association NFPA 1600 defines Business Continuity Program (BCP) in its general definitions as follows: An ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and recovery plans, and ensure continuity of services through personnel training, plan testing, and maintenance. An enhancement to NFPA includes recovery actions, which often extend long after the incident itself and the related programs, should be designed to include mitigation components for avoiding damage from future incidents.[96] Contingency plans for e-government can mitigate the risks of external events, specifically if the BCP encompasses resilience in communications and financial services via mobile banking and payments.

Market Examples:

- **Brazil:** All clearing and settlement account providers are either banks or entities controlled by banks, with the largest ATM and POS networks controlled by the largest banking conglomerates. Access to these systems is self-regulated, with oversight by the Central Bank of Brazil (CBB). The interoperability among the 25 ATM and 4 POS networks, as well as the dominance of the large banks, is driving small and medium sized institutions to create an independent automated clearing house (ACH) for low value payments, including mobile banking. While in the nascent stages, it is nonetheless encouraged by CBB.[97]
- **El Salvador:** The Central Reserve Bank (BCR) has broad regulatory authority over check clearinghouses and other payment systems used and operated by financial institutions; however there is no national payments law in El Salvador. El Salvador is a signatory to the Central American Treaty on Payments, under which BCR maintains oversight of what it considers to be systemically important payment and settlement systems. BCR also defines the parameters of high and low value payments under the Treaty terms and conditions, though the Treaty does not specifically cover retail payments. The issuance of stored value instruments, such as prepaid cards and mobile banking, have not been clarified within the context of the regulatory framework for payment services.[98]

Risk-based Policy Matrix – Appendix

- **South Africa:** Under the auspices of The South African Reserve Bank Act, the South African Reserve Bank (SARB) is authorized to "perform the functions, implement the rules and procedures, and in general, take the steps necessary to establish, conduct, monitor, regulate, and supervise payment, clearing, and settlement systems. Access to the national payment and settlement systems is restricted to banks only, with non-bank actors able to access the system via joint ventures with banks that are existing members. Under the National Payment System Act of 1998, SARB can delegate its responsibilities to a self-regulatory industry body, while retaining oversight control, and has done so with respect to the Payments Association of South Africa (PASA); PASA has appointed Bankserv as the payment clearinghouse for the South African banking industry and Bankserv provides interbank electronic transaction switching services to the banking sector. The switching services are majority owned by the countries four largest banks, ABSA Bank, First National Bank of South Africa (FNB), Nedbank, and Standard Bank, with 90% of the market. [99]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x	x	x			x	x	x

Risk-based Policy Matrix – Appendix

4.7. Risk (Account Providers):
"Agents are consistently out of cash."

Description:
Without effective cash forecasting mechanisms, agents may have difficulty managing their cash needs. Not only will this reduce the benefit of the service for customers, it will also damage the reputation of the service/provider.

Objective:

- Agents have sufficient cash on hand to support most cash-out requests.
- Account providers support agents with cash management and forecasting.

Policy Table:

Options	Implications
1. Regulator mandates liquidity requirements for providers. (by agent or by geographic region) The provider could be required to appoint an "agent of last resort" to ensure customer access.	• Requirement may enhance access to cash within a reasonable amount of time. • Consistent shortages decrease confidence in a provider's system. • Requirement could raise a cost barrier to entry as small players may not have cash forecasting/cash management capabilities. • Providers may decide to hire some agents as employees, as independent agents in high-volume areas may not be able to maintain balances or deal with security issues. • Forecasting and management capabilities are similar for ATM and Branch cash forecasting/ management. • Regulation implies monitoring and enforcement capacity.
2. Providers forecast and manage liquidity of agent network to optimize service for consumers.	• Enhances customer access to cash within a reasonable amount of time, improving public perception of service. • Providers may decide to hire some agents as employees, as independent agents in high-volume areas may not be able to maintain balances or deal with security issues. • Forecasting and management capabilities are similar for ATM and Branch cash forecasting/ management.
3. No oversight for agent liquidity	• Customers may be unable to withdraw cash from mobile money accounts from time to time, when agents run out of cash. • Market forces will improve liquidity management over time, as account providers keep reliable agents, take on some agent responsibilities, or partner with other institutions as agents of last resort.

Policy Narrative:
This risk refers to the amount of capital (both cash and e-money) held by agents, available for cash in/cash out transactions. In many mobile financial services systems, agents are the primary human interface with the consumer. Initial consumer confidence in a MFS system is, to a large degree, contingent on their ability to conduct cash-in/cash-out transactions. Consequently, maintaining a viable agent infrastructure is an important element of a strong MFS system.

To date, MFS providers have used commercial practices (e.g., commission structures, agent vetting processes, prepaid e-money reserves) to drive the proliferation of cash in/cash out agents. Market forces have determined which agents remain viable. MFS providers generally have not developed service level agreements (SLAs) with agents requiring them to maintain cash balances.

Recent MFS conferences (e.g., M-Banking 2009, Kenya School of Monetary Studies, May 2009) have raised the issue of an unregulated, ad hoc, cash in/cash out infrastructure and the impact this has had on consumer confidence. While the issue is viewed as significant, most experts agree that a regulatory solution would be difficult to craft and implement. The current view is that consumer demand and market forces will dictate the number of agents and the operating principles that govern agent conduct (e.g., availability of cash, hours of operation, etc.) Further, similar to branch and ATM channels, the market will provide cash forecasting solutions to minimize liquidity issues.

Market Examples:

- **El Salvador:** Under Article 1 of the Banking Law, deposit-taking, financial intermediation, and "other activities carried out by banks", permits the Central Reserve Bank (BCR) to authorize other operations and services. Banks are subject to regulation ranging from prudential to management and ownership rules, with licensing by the Superintendence of the Financial System (SupFin). However, a different framework governs member-based financial institutions, most of which were not subject to supervision by SupFin. This financial sector, comprised of savings and loan societies and cooperative associations, recently pushed for a new law allowing deposit-taking from the general public. While there is no specific regulation on the issuance of e-money by non-banks, the activity by this sector is

Risk-based Policy Matrix – Appendix

defined as taking deposits and intermediating those deposits. According to a recent CGAP Branchless Banking Assessment, it is widely assumed that Salvadoran regulators would strictly apply this definition to e-money schemes and deem such activity to be banking activity, particularly if funds are to be intermediated. [100]

- **India:** Acknowledging the development of the mobile channel, The Reserve Bank of India (RBI) issued the Operative Guidelines for Mobile Banking Transactions (2008) pursuant to the Payment and Settlement Systems Act (2007). Only banks licensed, supervised and with a physical presence in India may offer mobile banking to their existing customers. These institutions must obtain prior approval of RBI before launching their service offering. MNOs and nonbank financial institutions may not offer mobile banking services. Cross-border and foreign remittances are not permitted. Daily transaction limits are set at Rs 5,000 for transfers and Rs 10,000 for goods and services purchases. Two factor authentication, including a PIN is required on all transactions, with a limit of Rs 50,000.[101]
- **Kenya:** A recent study on the community level effects of M-PESA on local economic activity indicated that money circulation was the most highly ranked of all effects. It was consistently identified by respondents (being ranked most important by men and no. 3 by women) as infusing cash into the community via remittances where they appeared to be needed most. The higher and faster circulation, in turn, contributed to expansion of businesses, food security, human capital accumulation, and rescue money (emergency funds), as well as increased employment opportunities.[102]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x	x	x	x	x	x	x	x

Risk-based Policy Matrix – Appendix

4.8. Risk (Account Providers):

"Agent contracted to multiple account providers (i.e. a cell phone provider and a bank) with different regulatory requirements (e.g. KYC) does not meet its responsibilities for one or more."

Description:
When an agent contracts with more than one provider (i.e. a account provider and a bank), and the regulatory requirements differ between the institutions, the agent may confuse their responsibilities, meet the lower regulatory burden between the two, or not meet the regulatory requirements for either.

Objective:

- Account providers to hold agents responsible for their individual contractual agreements, whether exclusive or not.

Policy Table:

Options	Implications
1. Regulatory authority prohibits agents from representing multiple account providers.	• Restricting multiple agent relations may limit competition, particularly if the first mover has locked in the most suitable agents. • Agents may not achieve adequate volumes to justify being a paying agent is not able to link to multiple account providers. • Difficult and expensive to monitor.
2. Providers do not permit agents to enter into contractual obligations with other account providers without prior consent.	• Helps first mover justify market entry. • Limits subsequent competition by locking in the most suitable agents. • May limit agent profitability below breakeven point, limiting service expansion.
3. No action is taken by regulatory authorities or account providers restrict agents to a single account provider.	• Agents may link to multiple account providers. • Ensures competition based on service quality. • May reduce incentive for first mover.

Policy Narrative:
Competition can be seen to raise productivity because it allows the most productive companies to gain market share, thereby creating more jobs and obliging the less productive ventures to improve or concede and close operations. Permitting agents to manage their relations on a contractual basis may encourage competition based on service quality.

Market Examples:

- **Kenya:** "GUIDELINE ON AGENT BANKING, PART VI AGENT OPERATIONS6.1 Non-exclusivity
  6.1.1. No contract between an institution and an agent shall be exclusive.
  6.1.2. An agent may provide services for agent banking to multiple institutions provided that the agent has separate contracts for the provision of such services with each institution and provided further that the agent has the capacity to manage the transactions for the different institutions.
  6.1.3. An institution seeking to contract an entity which has already been contracted by another institution to carry out agent banking shall assess the capacity of the agent to manage transactions for different institutions. Due regard shall be taken to the space, technological capacity and adequacy of funds or float of the agent."

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
x		x	x		x	x	x	x

Risk-based Policy Matrix – Appendix

4.9. Risk (Account Providers):

"Individual poses as agent to collect deposits or payments from unsuspecting customers."

Description:

If an individual poses as an agent for a account provider, they could accept deposits or payments from customers and pocket the funds. The risk is likely higher in remote areas where oversight is limited, and where financial literacy is lower.

Objective:

- Consumers able to avoid fraud through spurious agents.

Policy Table:

Options	Implications
1. Regulatory authority requires all account provider agents to be registered. This list of registered agents published, and all registered agents post evidence of registration.	• Increased public information of registered agents allows consumers to protect themselves by only frequenting registered agents. • Implies regulatory capacity for agent registration and the public information campaign. • Requires that account providers require each agent to post registration at its place of business. • Most susceptible consumers, those who are financially illiterate, will be the most difficult to reach with an information campaign.
2. Regulatory authority requires providers to publish a list of official agents on a periodic basis to limit the potential for fraud.	• Account provider assumes responsibility for distributing and advertising list of its agents. • Increased public information of official agents allows consumers to protect themselves by only frequenting official agents. • Most susceptible consumers, those who are financially illiterate, will be the most difficult to reach with an information campaign.
3. Rely on the significant consumer protection built into the system through electronic receipts and account limits to mitigate fraud.	• During cash in, the agent will have to have enough e-money available to initiate the transaction and resulting confirmation to the service user. • Transaction limits inhibit service users from acting as informal agents. • Monitoring systems flag suspicious behaviour, enabling the account provider to shut down informal agents.
4. No regulatory action	• Public may not understand that account providers are not accountable for actions of these bad actors. • Instances of fraud subject to normal police investigation.

Policy Narrative:

In conformity with FATF Recommendation 23 and Special Recommendation VI[103], countries, at the national and sub-national level may AML/CFT requirements that include agent registration and licensing requirements, as well as the submission of updated registration lists to competent authorities. Registration of sub-agents may be included. Agent registration and licensing fees vary from flat rates to a percentage of business services offered. Non-prohibitive agent registration and licensing fees should be employed to encourage compliance.

Licensing for financial account providers may be an effective way to ensure that account providers adhere to AML and CFT procedures, prevent potentially hazardous business models from reaching the market, and obtain revenue minimal operating revenues for licensing fees. In addition, such practices may assist in mitigating risks in a rapidly changing market environment by helping regulators keep abreast of new entrants in the service arena.

FATF 23 mentions that "other financial institutions should be licensed or registered and appropriately regulated, and subject to supervision or oversight for anti-money laundering purposes, having regard to the risk of money laundering or terrorist financing in that sector." Though it does not specify m-FS, businesses which provide a service of "money or value transfer, or currency changing" are noted.[104]

Special Recommendation VI on Alternative Remittances includes licensing and registration provisions for persons or legal entities providing services for the transmission of money or value through informal transfer systems or networks.[105] This provision has likewise been interpreted by some as applying to m-FS.

Chatain et. al posit that TelCos and some other non-bank entities providing m-FS should be included within the regulatory definition of "financial institutions" when according to FATF these TelCos function as: "any person or entity who provides its customer with transfer of money or values services, or issues and managers means of payment, inter alia, electronic money." This broad definition would permit the TelCo's AML/CFT to comport with the actual role it performs within the financial or non-financial sector.[106]

Market Examples:

- **Kenya:** The Banking Act in Kenya defines banking business as having two key components. The first defines how funds are accepted and utilized by the institution and the second defines where the physical location of the institution may be organized to transact business. A bank may transact business only at its head office, branch, or place of business, all of which can only be operated with

Risk-based Policy Matrix – Appendix

the approval of the Central Bank of Kenya. CGAP notes in its examination of Kenyan banking that it would be difficult to determine if agents would be included in the definition of a bank under the Banking Act. Outsourcing of banking activities is not addressed in the regulations, but is approved on a case-by-case basis by CBK. Non-bank institutions are not under the same regulatory scrutiny.[107]

- **Brazil:** In Brazil, authorities enable compliance and mitigate risk by making banks fully liable for the acts of their agents. For instance, bank authorities have supervisory oversight as to the transaction details and records of their agents.[108] As the authors in "Integrity in Mobile Financial Services" conclude, "Licensing/registration and ongoing monitoring of m-FS providers should be implemented. As observed during fieldwork and recommended by FATF, licensing for financial Account Providers is an effective way to make certain m-FS providers adhere to AML and CFT procedures and prevent potentially hazardous business models from reaching the market." Of particular note, the authors cite this practice may prevent the creation of shell corporations, or front companies, which might be used to conceal and divert funds for criminal purposes via an m-FS platform.[109]

  In Brazil, for instance, agent networks are either managed directly by a bank or outsourced to a third party, which is considered an agent by the Central Bank of Brazil (CBB). Network managers provide services that range from AML/CFT training to agent selection, as well as point of sale maintenance and cash handling. The expansive reach of agent networks enables financial services to those individual who might not otherwise have access in Brazil and CBB oversight actually identified agent breaches in consumer protection rules; agents were noted as not disclosing fees and charging extra fees; selling client information to third parties; and committing loan fraud (not making bill payments for which they had received funds), among other transgressions. Such weeding out of dishonest actors in the system may be a facilitator of faith and trust in the public perceptions of the agent community.[110]

- **India:** In November 2006, India took limited steps toward the outsourcing of small value remittances and other payment instruments through business correspondents; restrictions included limiting eligible institutions to operate as correspondents to non-profit institutions, post-offices and cooperatives, as well as denying the ability of the correspondent to charge the customer for services rendered on behalf of the bank. Guidelines require that the Reserve Bank of India remain responsible for the actions of the agent as a risk mitigator, allowing RBI the authority to inspect the agent, as well as review agent records relevant to outsourced activities.[111]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		x	x		x	x	x	x

Risk-based Policy Matrix – Appendix

5.1. Risk (Trust Account Holding Financial Institutions):

"Liability concentration risk caused by an expanding trust account that may have a material impact on the trustee institution's balance sheet, particularly for those trust funds on deposit with the trustee bank."

Description:
Trust funds of a successful account provider could become significant to the point of representing a funding concentration risk for the trustee bank - liquidity risk - should there be a sudden reduction in the volume of items in transit through the account provider's system. This could be due to new competition, changes in regulation, account provider decision to diversify its own risks, or civil disturbances that cause a flight to cash.

Objective:

- Trustee banks limit the size of trust accounts they manage to what is reasonably manageable for that institution.

Policy Table:

Options	Implications
1. Bank regulators limit risk concentrations as a normal part of their supervisory activities - this process should include funds held in trust, so off-balance sheet unless held in deposit accounts.	• Concerns with managing risk concentrations may restrict bank interest in providing trust services. • Trust funds need investment opportunities that provide adequate liquidity in case of rapid disintermediation.

Policy Narrative:
The issue of liability concentration risk caused by an expanding trust account should be addressed within the overall framework of the trust account holding financial institution's asset-liability management, and its policies on funding concentration and liquidity management. However, since these are moneys held in trust, the overall management of the funds might warrant a separate, and perhaps more conservative, set of policies relative to those pertaining to on-balance sheet liabilities. Ultimately, it is the responsibility of both bank senior management and the institution's Board of Directors to ensure that a sound internal control system is in place, and in effect, to safeguard a trust account from any material risks that could adversely affect the achievement of the bank's goals through recognition of risks and continuous assessment.

At the level of the national regulator, banking supervisors should uphold Basel Core Principle #14 which asserts that "banking supervisors must determine that banks have in place internal controls that are adequate for the nature and scale of their business," including trust account management, if applicable. In line with Basel Core Principle 13, supervisors should require that all banks—regardless of size—have an effective system of internal controls that (a) is consistent with the nature, complexity and risk inherent in their on- and off-balance-sheet activities (including trust account management); (b) responds to changes in the bank's environment and conditions; and c) in cases where Supervisor's determine an action or activity is not adequate or effective for that bank's specific risk profile, take appropriate and necessary action. This would include addressing issues of liability concentration caused by an expanding trust account.

Market Examples:

- ***Please Note:*** *A market example of a policy action associated with this risk was not identified during the literature review or the in-country consultations included in this project's scope. We welcome your suggestions of relevant examples for inclusion in subsequent versions.*

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x					x		

Risk-based Policy Matrix – Appendix

5.2. Risk (Trust Account Holding Financial Institutions):

"The reputation of the financial institution which holds the trust account for the mobile financial account provider is damaged due to its mismanagement of the trust account."

Description:
The financial institution which holds the trust fund for the account provider takes on reputational risk. If the trust funds are invested in instruments that do not conserve their value, the liability coverage provided by the trust assets may become inadequate, potentially leading to a crisis in confidence in the service.

Objective:

- Preserve the value of the trust funds through prudent investment management, subject to regulatory oversight (as for insurance company reserves)
- The affiliation risk will be managed by the market. Banks should not enter into agreements with mobile financial account providers with which they have concerns.

Policy Table:

Options	Implications
1. Regulatory requirements govern the investment instruments in which trust account holding financial institutions may invest funds.	• Conservative investment strategies for the trust funds will preserve asset values but limit investment income which might otherwise be applied to offset account provider costs and keep transaction fees low.
2. Regulators evaluate reputational risk of major trust relationships.	• Adverse selection may come into play - those banks most qualified to act as trustees may be the most reluctant to take on the risks of doing so.

Policy Narrative:
In its *Examiner's Guide to Problem Bank: Identification, Rehabilitation, and Resolution* document, the U.S. Comptroller of the Currency noted prior to the recent financial crisis that the increase in national bank securitization activity and the proliferation of capital markets products had shifted increasing levels of credit risk to off-balance-sheet transactions. The credit risks inherent in capital market products, such as asset securitizations and derivatives, is difficult to quantify due to the need to assign a credit risk equivalent to these types of instruments. A bank that engages in securitizations needs to be fully aware of relevant risk-based capital rules applying to these transactions. As part of its overall internal controls and risk management policies, senior management and its supervising board of directors should include an assessment of off-balance-sheet and any other indirect exposures when determining the overall quantity of risk assumed by the financial institution that is custodian of a trust account. Moreover, both parties should ensure that all valuation methods and key assumptions used to value the residuals and servicing assets and liabilities associated with trust management are reasonable, fully documented, and well supported.[112]

Market Examples:

- ***Please Note:*** *A market example of a policy action associated with this risk was not identified during the literature review or the in-country consultations included in this project's scope. We welcome your suggestions of relevant examples for inclusion in subsequent versions.*

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
			x			x	x	x

Risk-based Policy Matrix – Appendix

5.3. Risk (Trust Account Holding Financial Institutions):

"The reputation of the financial institution which holds the trust account for the mobile financial account provider is damaged due to its association with an account provider whose payment system is poorly run."

Description:
The financial institution which holds the trust fund for the account provider takes on reputational risk. If the account provider is poorly managed, the trustee's affiliation with an institution that loses the public trust could damage its own reputation.

Objective:

- Preserve the value of the trust funds through prudent investment management, subject to regulatory oversight (as for insurance company reserves)
- The affiliation risk will be managed by the market. Banks should not enter into agreements with mobile financial account providers with which they have concerns.

Policy Table:

Options	Implications
1. Regulatory requirements govern the investment instruments in which trust account holding financial institutions may invest funds.	• Conservative investment strategies for the trust funds will preserve asset values but limit investment income which might otherwise be applied to offset account provider costs and keep transaction fees low.
2. Regulators evaluate reputational risk of major trust relationships.	• Adverse selection may come into play - those banks most qualified to act as trustees may be the most reluctant to take on the risks of doing so.

Policy Narrative:
The risk identified above relates to the reputation risk brought on to the financial institution holding the trust account on behalf of a mobile network operator (account provider) by the account provider's poorly run payment system. The contagion risk of the account provider is born by the bank holding the trust account. As part of its overall risk management policy, a bank should not enter into agreements with mobile financial account providers with which they have concerns, and they should undertake appropriate due diligence on any prospective mobile network operator partner prior to engaging in any legally binding partnership. As is the case with any trust and foundation establishment, when opening an account for a trust, the bank should take reasonable steps to verify the trustee(s), the settler(s) of the trust (including any persons settling assets into the trust), any protector(s), beneficiary (ies), and signatories. Beneficiaries should be identified when they are defined.[113]

Market Examples:

- **Kenya:** Several articles have been written of late that aim to distill the salient features of M-PESA's sudden and sustained success in Kenya.[114] Others maintain that much of M-PESA's rapid success is directly correlated with the high level of trust which the Kenyan public places on its account provider, Safaricom, and its management. If this is true and there should be a sudden deterioration in Safaricom's good fortune due even to exogenous shocks beyond its management or control, this level of trust could correspondingly diminish and pose a strong contagion risk on the fortunes and reputation of the financial institution holding the trust account/s that form a key link in Kenya's mobile phone banking ecosystem.

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
			x			x		

Risk-based Policy Matrix – Appendix

6.1. Risk (Payment Systems):

"Government mandated usage of government owned payment utility to process and clear all payment transactions regardless of type."

Description:
Government may have invested in a national payment system designed not just for inter-bank settlements but to reach down to the retail level, and may seek to protect its investment by blocking development or use of other payment systems. This risks blocking innovation to improve efficiency and lower payment costs.

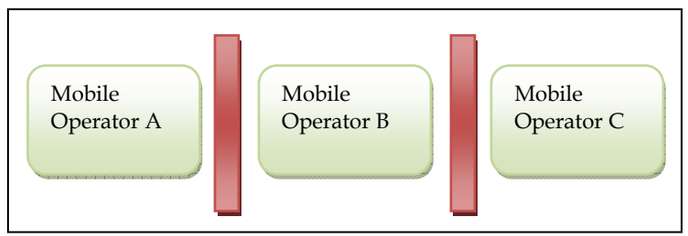
Objective:
Limit government involvement in payment systems to a) interbank settlements, and b) establishing an enabling environment for retail payments that encourages competition and innovation within accepted security standards.

Policy Table:

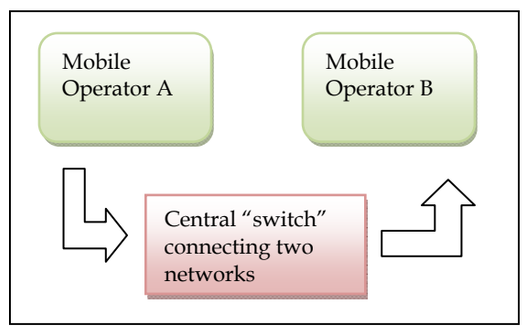
Options	Implications
1. Government ownership of the payment switch effectively requiring any existing and new account provider to connect to and use the system for its payment services.	• Interoperability creates benefits to consumers, as they can transfer to any other consumer regardless of network. • If government perceives a profit opportunity, rather than a public good, monopolistic pricing of the transaction could ensue. • There is no incentive for a new technology innovations since the government requires all transactions to be processed through the system
2. Mobile financial account providers allowed to use whatever payment system best serves the needs of their clients.	• Market pricing • Incentive to innovate processing systems and reduce transaction costs • Interoperability will be market driven.

Policy Narrative:
When there is a lack of interoperability requirements or a strong competition agency present, it is not uncommon for a single mobile operator to dominate the market. According to CGAP, "The mobile industry is an oligopoly, especially in developing countries, where the smaller market size may justify only two or three competitors. Having these players dominate the branchless banking market may not be a palatable option for banking regulators and competition authorities alike."[1] Market domination by a single entity is commonly seen in countries which have a "closed loop" system of mobile banking (see diagram below). Customers of mobile operator A can only send and receive payments from others on mobile operator A's network, but not those on B or C's network. Therefore, in a "closed loop" system, customers would be weary of using the services of a new player, as they would not be able to transfer/receive payments to or from individuals who are not on their network. This phenomenon, known as "network effect," occurs when the value of the service to each individual user increases with the overall number of the users of the service. Network effects foster the "first player advantage" where a mobile operator who enters the market early is able to "lock in" customers who seek to maximize the number of people they can connect to (assuming quality of service is high).[2] This system poses challenges to regulators not only because it limits the public's freedom to choose between providers, but it can also stifle innovation and potentially lead to anti-competitive pricing. On the other hand, in an "open loop" system, payments are able to be made across different networks through a central "switch." Therefore, customers of mobile operator A (see diagram below) are not limited to only sending/receiving payments to others on their network, but can also connect to customers of mobile operator B. This system of interoperability expands customers' choice in selecting providers and fosters competition.

Closed Loop System



Open Loop System



[1] Ivatury, Gautam and Ignacio Mas (2008) "The Early Experience with Branchless Banking." CGAP, Washington DC. [Online] http://www.cgap.org/gm/document-1.9.2640/FocusNote_46.pdf

[2] Porteous, David. (2006)

Risk-based Policy Matrix – Appendix

Market Examples:

- **Nigeria:** "As switches connect consumers to their bank accounts to authorize transactions, only banks or a consortium of banks or agents for banks or banking consortium or any other company as approved by the CBN, can act as a switching company. This provision is to minimize fraud and mitigate risk to the banking system. Third party providers are to submit themselves to the scrutiny of the Central Bank only after having signed a switching agreement with a bank or consortium of banks. The switching companies must meet the standards defined in the 3rd party service provider agreement. Third parties or account providers must meet the guidelines as described under 'Guidelines for Vendors and Outsourcing.'" Additionally, the report advises that settlement of e-payment transactions that are delivered through the mobile channel should be done through the banking system only.[115]
- **Ghana:** The e-Zwich was designed as an electronic clearing and payment settlement system with a common platform to link all Ghanaian financial institutions. It anchors on biometric (fingerprint) ID technology, permitting smartcard holders to perform financial transactions and services for goods and services, at any e-Zwich point-of-sale (POS) or ATM. In addition to performing all transactions associated with a traditional bank account, such as money transfers, cash withdrawals, bill pays, the card holder can also receive pensions, salaries, and use mobile banking services.[116] Some press reports indicate that there have been user complaints regarding false negatives during biometric authentication, requiring them to establish their identity prior to using their cards. Merchants' complaints include inability to synchronize transactions with the e-Zwich mainframe at the end of the day; e-Zwich utilizes GPRS modems when Internet connections are unavailable, resulting in failed connectivity. Other concerns include the fact that the electronic switch is not managed by the Bank of Ghana and the biometric portion is not the province of the National Health Insurance Scheme (NHIS), Electoral Commission, DVLA (Drivers & Vehicles Licensing Authority), and Ghana Passport Office.[117]
- **Mexico**: The mobile phone industry is highly concentrated in a single MNO, Telcel, which has 85% of the market share. The Communications and Transport Secretariat (SCT), the country's telecommunications policy maker, has the authority to impose special price, quality, and disclosure requirements on dominant MNOs to promote competition. Despite complaints against Telcel's pricing practices and its dominant position, the SCT has taken no measures so far.[118]
- **South Africa**: [Example of open loop system] WIZZIT works across all networks in the country. To transfer money Wizzit uses the well developed South African inter-bank clearing house system. It accesses the clearing system as an autonomous division of the South African Bank of Athens Ltd. This 'any-to-any' feature is seen as a significant advantage in giving the Wizzit account the ability to transact with any mobile user regardless of the identity of their network operator or their bank.[119]
- **Kenya**: Safaricom, the dominant mobile network operator, holds 79% of the market share. This is despite extensive efforts by its competitor, Zain, which only holds 20% of the market. Safaricom's m-banking product, M-PESA, is only compatible with M-PESA account holders and certified agents. Therefore, M-PESA operates under a closed system, limiting interoperability.[120]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x	x	x				x	

Risk-based Policy Matrix – Appendix

7.1. Risk (National Regulators):

"Illicit financial activities enabled by weak KYC/CDD requirements/enforcement."

Description:
If the AML?CFT requirements do not apply to mobile financial services, illicit actors could leverage the mobile network for illicit means. If the party providing the financial service is held to these standards, but its ability to comply/enforce them is limited, the risk still remains. (The ability to enforce AML/CFT among a disparate agent population is a critical element.).

According to FATF, "the general rule is that customers should be subject to the full range of customer due diligence measures. However, there are circumstances in which it would be reasonable for a country to allow its financial institutions to apply the extent of the customer due diligence measures on a risk sensitive basis."[121] Additionally, the Basel Committee on Banking Supervision notes that KYC is directly associated with the fight against money laundering and, as such, should form a core feature of a bank's risk management and control procedures. Further, KYC should be complemented by regular compliance reviews and internal audit. "The intensity of KYC programmes beyond these essential elements should be tailored to the degree of risk."[122]

The financial institution should adopt procedures for limiting transactions prior to customer verification. This may include restrictions as to the type, number, and/or amount of transaction performed, in addition to monitoring transactions outside of the customer's projected financial footprint. This is particularly critical in non-face-to-face business relationships[123] (such as m-FS).

Objective:

- Risk-based supervision and enforcement of AML/CFT safeguards to enable authorities to focus on the highest priority risks.

Policy Table:

Options	Implications
1. Regulatory authority implements and enforces a point – based (stepped based on risk) AML/CFT system.	• Point-based AML/CFT system allows flexibility for consumers with various forms of identification; however, limits risk by embedding a standard due diligence requirement industry-wide. • Regulatory authority to implement/monitor/enforce can be costly, considering that agents are the implementers.
2. Account providers elect to have account opening conducted by employees rather than agents, so as to maintain stricter AML/CFT controls.	• Account providers can hedge risk by controlling account opening process. • Potential customers inconvenienced as account provider has limited footprint relative to agent network. • Cost of building a network to support would be costly.
3. account providers institute institution specific KYC/CDD policy for agents, which should comport with sound AML/CFT standards.	• Point-based AML/CFT system allows flexibility for consumers with various forms of identification; while limiting risk by embedding a standard due diligence requirement network-wide. • Lack of regulatory guidelines will lead to variance in system strength which can allow for exploitation. • Implies regulatory capacity to monitor individual account provider policies and procedures, but allows for innovation in achieving the objective.
4. No regulatory action for mobile on AML/CFT.	• Illicit actors leverage mobile networks for illegitimate financial purposes; illicit activity flourishes in economically disadvantaged regions/zones where provider enforcement mechanisms are weak

Policy Narrative:
One risk-based approach is known as point-based AML/CFT. This approach may be less restrictive for both agents and consumers, as it presumes the more KYC evidence a customer can provide (ranging from a national ID, passport, physical presence, utility bills, introduction by other clients, driver's license, etc.), then the more proportional the risk is to the institution. Services are then offered on a basis proportional to the perceived risk.

Chatain et al identified several innovative risk mitigating factors in mobile banking and securities accounts, or those similar to other electronic channels such are utilized in electronic banking channels for Internet banking and ATMs. National authorities may standardize national public identification to facilitate documentable measures to verify the customer and/or beneficial owner's identity when conducting transactional activity or establishing customer relationships. In the absence of a national customer ID, national authorities may provide for alternative ID instruments to comply with these requirements. All ID requirements should pay special attention to money laundering and terrorist financing threats that may arise from the anonymity of new or developing technologies.

Simplified or reduced CDD measures could apply to the beneficial owners of pooled accounts held by designated non financial businesses or professions, in the event such individuals are subject to AML/CFT requirements and related monitoring. The Basel CDD paper may provide guidance to financial institutions holding such accounts as well (see Section 2.2.4).[124] In the absence of a national customer ID, Banks, MNOs

Risk-based Policy Matrix – Appendix

and agents should have policies and procedures in place to address specific risks associated with new or developing technologies that permit remote and non-face-to-face business relationships and transactions, in addition to any risks associated with the nested agent relationships that might obscure customer identities in the payment chain.

Market Examples:

- **Kenya**: Under Kenya's Registration of Persons Act, citizens 18 or over must register with the National Registration Bureau and obtain a national ID. Failure to do so is a crime. Individuals obtaining citizenship by birth only need to demonstrate that one parent is a Kenyan citizen, usually by presenting a parent's national ID. However, for Nubians, Kenyan Somalis, and coastal Arabs, the standard is stricter. Registration officials have broad discretion under Section 8 of the Registration Act, which permits officers to require an applicant to produce additional evidence. The Principle Registrar may demand proof of "other particulars as may be prescribed (Section 5)." Moreover, under Kenyan citizenship law, women cannot pass nationality to their children. Children of "unknown origin" or who might otherwise be stateless, including some orphans and street children, are not automatically granted Kenyan nationality.[125] Refugees cannot naturalize, increasing the risk of statelessness over time. In terms of flexible ID requirements for users, account provider M-Pesa accepts a national ID, a passport (Kenyan or foreign), Alien certification, and military or diplomatic IDs. It is also is considering lowering the minimum age of its users from 18 to 16 with parental consent.[126]
- **South Africa:** Admitted to FATF in June 2003, South Africa conformed to the CDD/KYC standards. However, in practice this left nearly one third of its citizens unable to qualify for opening bank accounts. The "mass banking clients" compliance exemption (Number 17) in the Financial Intelligence Centre Act (FICA) of 2001, is an example of how South Africa addressed this issue for low income clients who had now tax number and were unable to produce address verification. The exemption limits the maximum account balance to US $4,000 and limits deposit and withdrawals, as well as the ability to conduct cross border funds transfers.[127] To mitigate the risk of anonymity, TelCo representatives for Wizzit travel to remote locations for customer verification procedures. MTN-Standard Bank allows remote registration via Internet, call center or mobile, however, customer information is then cross-verified by 3rd party database checks.[128]
- **Korea:** According to one study, TelCos in many jurisdictions where m-FS predominates did not sufficiently perform CDD on non-residents; it is recommended that enhanced KYC and CDD be performed for such customers similar to the manner in which banks perform such measures. In Korea, there are comprehensive procedures in place for mitigating the risks of anonymity with cooperation between the banks and the TelCos. To conduct m-FS, a customer must hold a bank account, travel in person to the bank branch and provide ID (a valid passport for foreign citizens), and complete a funds transfer form in order to receive access to e-banking. Upon completion of these steps, an ID and password are issued to the customer, as well as a letter permitting the customer to obtain a SIM card from the TelCo. Service for m-FS is available only to post-paid individual subscribers, rather than corporate entities.[129]
- **India:** Under the Prevention of Money Laundering Act of 2002, the law issued AML guidelines, including KYC standards. Banks were advised to tier customer risk according to low, medium, and high, adjusting account ID requirements. Reserve Bank of India's 2005 Circular relaxed the proof of residence requirements of small value accounts, permitting identity and address verification via introduction by another account holder who passed full KYC in at least the preceding 6 months.[130]
- **Brazil:** HSBC uses cross channel verification, such as confirming credit card transactions via mobile phone text messages.[131]
- **Mexico:** AML/CFT regulation is based on several laws that require a broad range of entities to have AML/CFT policy, specialized personnel, training, systems, and procedures. All financial institutions, money transferors, and the third parties providing services on their behalf are covered by the law. MNOs are not. To open an account, banks must produce a file on the client that includes name, address, birth date, nationality, profession, professional activity, and telephone, copies of the identification document, tax card, and proof of address (if different from the ID document). Foreigners must provide proof of legal residence, in addition to an address in their country of origin.[132]
- **Jordan:** In Jordan, banks must identify and verify customer identity according to the Central Bank of Jordan Instruction 42 under its Anti-Money Laundering Law issued in 2007 and 2008. Verification consists of customers presenting their Jordanian national ID and proof of address, which must be verified in a face-to-face setting by a "bank employee." Agents may fax ID to branches to comply with Instruction 42 requirements. Mobile network operators are not considered financial companies under the AML law and would not be covered by mobile banking, however, do require presentment of national ID for Jordanians or passports for non-Jordanians for KYC requirements.[133]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
x	x	x	x		x	x	x	x

Risk-based Policy Matrix – Appendix

7.2. Risk (National Regulators):

"Identification of illicit financial activities hampered by insufficient reporting requirements."

Description:

Reporting of large or suspicious transactions to appropriate authorities and/or the Financial Intelligence Units (FIUs) provides information on mobile financial transactions that exceed or are structured to avoid reporting requirements, as well as on trends and patterns of unusual mobile financial activity.

FATF recommendations specify creation of specialized government units, called Financial Intelligence Units (FIUs), to be a central node for monitoring and analyzing financial transactions, as well as collecting and disseminating related information to appropriate authorities. FIUs operate under different guidelines, but under special provisions may exchange information with foreign counterpart FIUs to detect, deter, and disrupt ML/TF and other illicit financial crimes.[134]

Objective:

- Risk-based supervision and enforcement of AML/CFT safeguards to enable authorities to focus on the highest priority risks

Policy Table:

Options	Implications
1. Financial regulatory authority includes mobile providers in AML/CFT reporting requirements to appropriate authorities and/or the FIUs. Account providers file Suspicious Transaction Reports (STR) for transactions meeting specified criteria.	• Standardized reporting, in line with financial institutions, mitigates potential for illicit activities and facilitates investigation. • Reporting requirements impose a cost on the account provider, which would be reflected in usage fees.
2. STRs for all reporting entities indicate the channel used, including mobile.	• Account provider may not have the technology to identify suspicious transactions, resulting in a dump of all transactions on the FIU. • FIU may not have the capacity or budget to analyze reports for mobile sector.
3. Account Providers are not included in STR reporting requirement.	• Mobile financial services could be used to channel large quantities of small payments in support of illicit activities.

Policy Narrative:

While the internal financial intelligence/fraud units of Account Providers require due diligence information from their customers for business purposes, there is no standardization by authorities as to the requirements for mobile financial Account Providers and related transactions in terms of STRs. Financial intelligence and law enforcement authorities should develop clear rules and guidelines for m-FS transaction providers. Once received, FIUs or investigative authorities should ensure they have the capacity to analyze STR information that is reported and effectively use the information in prosecutorial and/or enforcement actions.

According to FATF Recommendation 13, if a financial institution suspects that funds are the proceeds of criminal activity or TF, it should be reported promptly to the FIU. Consequently, AML/CFT reporting obligations are particularly germane to mobile financial services as most activities are identified ex-post. Further, FATF Special Recommendation IV stipulates that should financial institutions, other businesses or entities subject to anti-money laundering obligations, suspect or reasonably suspect funds may be linked or related to terrorism[135] , then such suspicions should be reported with due haste to competent authorities.[136]

Likewise, FATF Recommendation 25 provides that competent authorities should establish guidelines that will assist financial institutions and non-financial intermediaries in the detection and deterrence of ML/TF and other illicit financial crimes. As the national center for receiving and analyzing suspicious financial transaction reports, the FIU may provide guidelines on the limitations on size and velocity of mobile financial transactions and related reporting that exceeds or is structured to avoid limits, as well as trends and patterns of unusual mobile financial activity.[137]

According to the authors of "Integrity in Mobile Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing," there is general trepidation in law enforcement circles over the fact that m-FS providers are outside of the regulatory regime imposed upon other financial institutions. Based on the authors' fieldwork, not all m-FS providers fully followed the same AML and CFT practices as traditional banks, insurance, and securities firms. If TelCos did comply with such controls, partner entities, such as agents, merchants, and third party processors may not be in compliance. Additionally, all parties had varying degrees, if any training or awareness of the necessity for AML and CFT standards, which enabled them to differing degrees to protect not only their own businesses but all those in the financial transaction chain.[138]

Market Examples:

- **Africa:** several Account Providers in (Zambia, Kenya) noted that despite efforts at identifying suspicious activity and/or working with appropriate authorities, there was no centralized FIU to which to report these activities formally. Central authorities noted a need for AML and CFT capacity building and training.[139]
- **Philippines:** One of the most collaborative agent - FIU models to date in terms of working directly with the mobile financial services industry has been that of the Philippines. Over 10% of the 89 million Filipinos working abroad in 2007 sent an estimated $14.45 billion USD home through formal remittance channels. This equated to 10% of the Philippines GDP. [140] Both Globe and G-Cash are regulated by Bangko Sentral ng Pilipinas (BSP), the Central Bank, and the Anti-Money Laundering Council (AMLC), the Philippines FIU. Both are regulated as money service businesses, non-bank financial institutions.[141]
- **Korea:** Having conducted fieldwork in Brazil, Hong Kong, SAR of China, Malaysia, the Philippines, South Africa, and South Korea, the authors of "Integrity in Mobile Financial Services" noted that while

Risk-based Policy Matrix – Appendix

Telcos in these areas required information for business purposes, uniform guidance from the FIU had not been provided. A related challenge in some jurisdictions appeared to be the technical ability of the FIU to analyze financial data at the same sophistication level as the Telco or bank involved in the m-FS transactions. "To detect criminal or TF activity, it is imperative that such information be made available to and fully processed by intelligence and law enforcement authorities."[142]
KoFIU (The Korean Financial Intelligence Unit) receives and analyzes suspicious transaction reports (STRs) from financial transactions conducted through a variety of channels, including m-FS. Typologies[143] released by KoFIU to educate their FIU counterparts in illicit mobile usage, include:

i. Cyber Gaming Case: Proceeds from illegal online gaming and identity theft were placed in the Korean banking system via m-FS and other electronic methods.
ii. Cross-border Remittance Case: A person used false identities and several bank accounts, sending the funds cross border by m-FS and other electronic means to various unspecified sources.
iii. Swindling and investment fund Case: A person founded a fraudulent financial consulting firm and clients sent funds to him via m-FS and other electronic means.[144]

- **El Salvador:** Mobile banking is still in the embryonic stages and available only to those with a bank account. Financial institutions are required to maintain both systems and policies that provide access to both the identity and transaction profiles of their clientele. In order to open a bank account, a customer must provide their name, date and place of birth, nationality, address, profession, and marital status, in addition to presenting an identity card. The Banking Law, however, does not stipulate which identity documents are acceptable. Further, banks and insurance companies are required to inform the country's Financial Intelligence Unit (FIU) customers conducting single or aggregate transactions in a one month period exceeding USD 500,000 and are to confirm that the activity is in line with the client's financial footprint. Supporting documentation on the transactions is to be maintained for a minimum of 5 years.[145]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
x			x		x	x	x	x

Risk-based Policy Matrix – Appendix

7.3. Risk (National Regulators):

"Illicit financial activities facilitated by unlicensed/ unmonitored agent network."

Description:
As agents are a critical component of the mobile payment network, they have the ability to facilitate fraud or criminal activity (e.g. if they do not comply with KYC / CDD requirements, customers could conceivably set up accounts under false identities). In conformity with FATF Recommendation 23 and Special Recommendation VI[146], countries, at the national and sub-national level may AML/CFT requirements that include agent registration and licensing requirements, as well as the submission of updated registration lists to competent authorities. Registration of sub-agents may be included. Agent registration and licensing fees vary from flat rates to a percentage of business services offered. Non-prohibitive agent registration and licensing fees should be employed to encourage compliance.

Objective:

- Risk-based supervision and enforcement of AML/CFT safeguards to enable authorities to focus on the highest priority risks.

Policy Table:

Options	Implications
1. Regulatory authority trains and licenses agents to ensure capacity.	• Training and licensing can help to ensure a base capacity among agents. • Regulatory ownership or training licensing is high cost and requires capacity that the regulator is unlikely to have.
2. Regulatory authority requires account provider to institute an AML/CFT/anti-fraud training program which incorporates AML/CFT guidelines. Training, compliance monitoring of, and registration of agents is required by account provider.	• Training helps to ensure greater competence among the agent network, and thus a stronger, more stable mobile payment system. • Motivating agents o follow prescribed guidelines may be challenging. • Implies regulatory support for and verification of training program.
3. Provider institutes training program that certifies an agent according to policies and procedures of the company for AML/CFT; may encourage agents to adopt sound business practices and follow government guidelines for AML/CFT.	• Training helps to ensure greater competence among the agent network, and thus a stronger, more stable mobile payment system • Motivating agents to follow prescribed guidelines may be challenging. • No regulatory enforcement of training program may allow sub-optimal programs.
4. No required training or licensing process	• Least direct costs for account providers and regulators. • May result in indirect costs through use of mobile financial services to support illicit activities.

Policy Narrative:
Licensing for financial account providers may be an effective way to ensure that account providers adhere to AML and CFT procedures, prevent potentially hazardous business models from reaching the market, and obtain revenue minimal operating revenues for licensing fees. In addition, such practices may assist in mitigating risks in a rapidly changing market environment by helping regulators keep abreast of new entrants in the service arena.

FATF 23 mentions that "other financial institutions should be licensed or registered and appropriately regulated, and subject to supervision or oversight for anti-money laundering purposes, having regard to the risk of money laundering or terrorist financing in that sector." Though it does not specify m-FS, businesses which provide a service of "money or value transfer, or currency changing" are noted.[147]

Special Recommendation VI on Alternative Remittances includes licensing and registration provisions for persons or legal entities providing services for the transmission of money or value through informal transfer systems or networks.[148] This provision has likewise been interpreted by some as applying to m-FS.

Chatain et. al posit that TelCos and some other non-bank entities providing m-FS should be included within the regulatory definition of "financial institutions" when according to FATF these TelCos function as: "any person or entity who provides its customer with transfer of money or values services, or issues and managers means of payment, inter alia, electronic money." This broad definition would permit the TelCo's AML/CFT to comport with the actual role it performs within the financial or non-financial sector.[149]

Market Examples:

- **Kenya:** The Banking Act in Kenya defines banking business as having two key components. The first defines how funds are accepted and utilized by the institution and the second defines where the physical location of the institution may be organized to transact business. A bank may transact business only at its head office, branch, or place of business, all of which can only be operated with the approval of the Central Bank of Kenya. CGAP notes in its examination of Kenyan banking that it would be difficult to determine if agents would be included in the definition of a bank under the Banking Act. Outsourcing of banking activities is not addressed in the regulations, but is approved on a case-by-case basis by CBK. Non-bank institutions are not under the same regulatory scrutiny.[150]
- **Brazil:** In Brazil, authorities enable compliance and mitigate risk by making banks fully liable for the acts of their agents. For instance, bank authorities have supervisory oversight as to the transaction

Risk-based Policy Matrix – Appendix

details and records of their agents.[151] As the authors in "Integrity in Mobile Financial Services" conclude, "Licensing/registration and ongoing monitoring of m-FS providers should be implemented. As observed during fieldwork and recommended by FATF, licensing for financial account providers is an effective way to make certain m-FS providers adhere to AML and CFT procedures and prevent potentially hazardous business models from reaching the market." Of particular note, the authors cite this practice may prevent the creation of shell corporations, or front companies, which might be used to conceal and divert funds for criminal purposes via an m-FS platform.[152]

In Brazil, for instance, agent networks are either managed directly by a bank or outsourced to a third party, which is considered an agent by the Central Bank of Brazil (CBB). Network managers provide services that range from AML/CFT training to agent selection, as well as point of sale maintenance and cash handling. The expansive reach of agent networks enables financial services to those individual who might not otherwise have access in Brazil and CBB oversight actually identified agent breaches in consumer protection rules; agents were noted as not disclosing fees and charging extra fees; selling client information to third parties; and committing loan fraud (not making bill payments for which they had received funds), among other transgressions. Such weeding out of dishonest actors in the system may be a facilitator of faith and trust in the public perceptions of the agent community.[153]

- **India:** In November 2006, India took limited steps toward the outsourcing of small value remittances and other payment instruments through business correspondents; restrictions included limiting eligible institutions to operate as correspondents to non-profit institutions, post-offices and cooperatives, as well as denying the ability of the correspondent to charge the customer for services rendered on behalf of the bank. Guidelines require that the Reserve Bank of India remain responsible for the actions of the agent as a risk mitigator, allowing RBI the authority to inspect the agent, as well as review agent records relevant to outsourced activities.[154]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x	x	x	x	x	x		

Risk-based Policy Matrix – Appendix

7.4. Risk (National Regulators):

"Inadequate transaction records impair investigation of fraud or criminal activity."

Description:
Full transaction audit trails are essential to investigations to follow the money trail. Records retention should permit reconstruction of transaction details, including personally identifying data of the transaction parties.

FATF Special Recommendation VII notes that "countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain."

FATF Recommendation 10[155] notes that records retention to reconstruct transaction details, including personally identifying data of the transactor, aids evidence collection in administrative, civil, and criminal sanctions. Further, necessary records should be available to competent authorities for at least five years.[156]

Objective:

- Regulatory framework follows international standards for financial records retention to mitigate risks, which sets 5 years to enable information requests from competent authorities.

Policy Table:

Options	Implications
1. All service users required to maintain an individual bank account through which all transactions flow.	• Cell phone company role limited to messaging - actual transactions occur in the bank. • Ensures that full transaction records exist within the formal banking system. • Acceptable to users who already have bank accounts, but represent a high cost barrier to users who have no need for a full banking relationship. • Would substantially restrict expanding access to financial services to the unbanked.
2. Regulator requires transaction level reporting and implements internal suspicious transaction identification process.	• Internal systems facilitate investigation • Lowers account provider costs by enabling a raw data dump on the FIU, without the need for analysis. • Implies FIU capacity to absorb and analyze large volumes of transaction data, essentially all of which will be routine.
3. Regulatory authority requires the account provider to maintain all payment transaction records for 5 years following the completion of the transaction. (Should mimic financial requirements)	• Record retention requirements will facilitate investigation. • Records retention responsibilities may be tiered to transaction amounts and type of services provided (e-money issuer, remittance services, Telco) • Retention requirements will impose a cost on providers, which would be passed on to service users. • Differs from normal cell phone call records, which may be subject to shorter record retention.
4. Provider sets internal policies and procedures for maintaining all records obtained through the CDD process and transaction records (Customer Detail Records-CDRs) for a specified period following the completion of the transaction, failure of the account provider, and/or termination of customer relationship.	• Record retention requirements will facilitate investigation. • If the standards for retention are low, authorities may not be able to trace transactions within a payment chain from one provider to another or reconstruct sender/receiver identities in the prosecution of financial crimes.
5. No mandatory or implied records retention policies for mobile financial services	• Ability to reconstruct audit trail is dependent on business practices for records retention and retrieval capability of account providers and others in the account provider's network.

Policy Narrative:

In some cases, particularly when the service links "traditional" bank channel accounts to TelCo partners, AML/CFT obligations likely reside with the bank, as the primary financial institution responsible for providing m-FS. However, when the TelCo can be a channel through which other services are provided and the merchant can also receive payments and conduct non-bank account transfers, the line between financial and telecommunication providers blurs.

Chatain et. al posit that TelCos and some other non-bank entities providing m-FS should be included within the regulatory definition of "financial institutions" when according to FATF these TelCos function as: "any person or entity who provides its customer with transfer of money or values services, or issues and managers means of payment, inter alia, electronic money." This broad definition would permit the TelCo's AML/CFT to comport with the actual role it performs within the financial or non-financial sector.[157]

Risk-based Policy Matrix – Appendix

There is no consensus on how to implement standards internationally, though the majority of TelCos perform some KYC and CDD measures as best business practices.[158]

Market Examples:

- **Kenya:** In a recent presentation entitled "10 YEARS ON FROM THE US EMBASSY BOMB BLAST" in Nairobi, Kenya,"[159] Director Samuel Mutungi provided a case study on lessons learned for terrorist attacks regarding disaster recovery and business continuity planning for financial services. One of the main mitigating strategies aiding in recovery for Co-Operative Bank, despite the fact that the ICT equipment was damaged and networks/systems were destabilized, was that the Bank's systems back-up e.g , redundancies, had recently been moved off site.
- **South Africa:** The South African Financial Intelligence Center Act (FICA) permits electronic record keeping and outsourcing to third party intermediaries. For MTN group, the South African telecommunications company, client identification records are collected by agents, but forwarded to the main office for verification and retention.[160] Value in mobile financial transactions, at some point in the transfer, is typically stored on the computer servers of account providers or financial institutions. These servers, however do not have to reside in the country of originating activity. This may or may not create concerns for national regulators in terms of evidence collection, search, seizure, asset forfeiture/sharing, and information sharing.[161]
- **Philippines:** The use of new and developing technologies, such as the intersection of information and communications technologies and financial services, raises new areas of consideration in terms of records retention and retrieval. In the "Effects of Cell phone on Anti-Money Laundering/Combating Terrorism (AML/CFT) Wire Remittance Operations"[162] which examined mobile financial services practices in the Philippines, the author cites several emergent safety and soundness factors:
    vii. Tests of electronic systems security, hardware, and software,
    viii. Tests of customer ID and point-of-sale samples,
    ix. Anti-virus protection,
    x. Internal security policies and procedures for electronic systems,
    xi. Cross industry and regulatory collaboration in records involving text and SIM cards, and
    xii. Critical infrastructure protection for the telecommunications and the financial sectors.

    Customer Detail Records: Mobile financial account providers maintain customer activity records (Customer Detail Records) similar to financial institutions and payment system providers. These detailed customer records relate to the mobile operator's system usage and include information relevant to AML and CFT, such as each mobile calls originating and receiving phone and the call's duration.
- **Malaysia:** In Malaysia, Maxis maintains ongoing transaction records for active customers and for terminated customer retains them for an additional seven years.
- **Hong Kong:** In Hong Kong SAR of China, AML regulations for mobile account providers require that records be maintained on all transactions over HK $8,000, however transactions below this figure are recorded in the mobile account provider systems, too.[163]
  Safeguarding electronic customer and business data: avoiding data leaks, and maintaining high – quality IT systems is a critical business enabler in records retention efforts for AML and CFT. In light of recent data leaks, e-finance regulations are emerging.
- **Macao SAR:** For instance, Banks in Macao SAR of China do not permit m-FS transfers outside of the same bank or internationally.
- **Philippines:** The Philippines caps m-FS transactions per day and per month in order to mitigate ML risks.[164]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		x	x		x	x		

Risk-based Policy Matrix – Appendix

7.5. Risk (National Regulators):

"National regulators and/or law enforcement authorities unable to effectively investigate fraud or criminal activity due to lack of operational support systems and human capacity."

Description:
Investigative officials are unlikely to have the human capacity to effectively regulate the network of providers, agents, trust accounts and customers necessary to mitigate the known risks. If the regulatory framework entailed licensing/supervising agents, as well as providers and banks, the number of regulators required for this activity would likely be well beyond that on staff for the regulatory authorities.

Objective:

- Risk based regulatory framework that minimizes the role of the regulator while providing an enabling environment that mitigates against risks to the customer, account provider network and the financial system.
- Regulatory capacity sufficient to provide a deterrent to illicit use of mobile financial services through heightened risk of discovery and prosecution.

Policy Table:

Options	Implications
1. Establish an FIU with sufficient resources to credibly investigate suspicious transactions and initiate prosecution of illicit activity. Establish specialized investigative, prosecutorial and judicial expertise within the legal system.	• Would enable the country to comply with FATF guidelines and participation in the Egmont group. • Would extend activities already in principle required for banking and insurance to mobile financial services. • Has cost implications - may require a fee regime on account providers, which would be passed on to users, reducing the financial incentives to use mobile financial services.
2. FIU established but not adequately resourced, or no FIU established.	• No direct cost incurred, but • Not in compliance with FATF guidelines, potentially risking inclusion in the list of non-compliant countries, leading to restrictions of access to international financial markets.

Policy Narrative:
FATF Recommendations 29-31 address adequate powers, adequate resources and effective mechanisms regarding human capacity of both appropriate authorities to monitor and mitigate illicit financial activity. Compliance by financial institutions is addressed by Recommendation 29; Supervisors should be "authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose adequate administrative sanctions for failure to comply with such requirements." Countries, as well, should both provide their competent authorities involved in AML and CFT with sufficient "financial, human, and technical resources" (Rec. 30) and well as ensuring that "policy makers, the FIU, law enforcement and supervisors" can effectively and efficiently develop and implement AML and CFT policies (Rec 31).

Market Examples:
Of the countries reviewed for this study, only Nigeria currently has an FIU that is a member of the Egmont Group. Several countries are members of the FATF Regional-Style Bodies. Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), the purpose of which is to combat money laundering by implementing the FATF Forty Recommendations. ESAAMLG's efforts include co-coordinating with other international organizations concerned with combating money laundering, studying emerging regional typologies, developing institutional and human resource capacities to deal with these issues, and co-coordinating technical assistance where necessary. ESAAMLG enables regional factors to be taken into account in the implementation of anti-money laundering measures. The Intergovernmental Anti-Money Laundering Group in Africa, GIABA , was established on 10 December 1999 by a decision of the Authority of Heads of State and government of the ECOWAS. GIABA's mandate was revised in January 2006 to fully incorporate and properly reflect the imperative to fight the financing of terrorism. GIABA members acknowledge that money laundering and financing of terrorism are issues of critical importance to the world community which require global action. Further, that the economies and financial systems of the countries need to be protected from laundered money and proceeds from terrorist activities. GIABA members recognize that West Africa needs to address these issues and find global solutions to them

- **Ghana-** GIABA
- **Zambia -** ESAAMLG
- **Tanzania -** ESAAMLG
- **Nigeria – Egmont,** GIABA
- **Kenya -** ESAAMLG
- **Rwanda – N/A**
- **Uganda-** ESAAMLG

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x	x	x		x			

Risk-based Policy Matrix – Appendix

7.6. Risk (National Regulators):

"National regulators and/or law enforcement authorities unable to effectively investigate fraud or criminal activity due to lack of authority."

Description:

In many country contexts, the regulatory framework for mobile payment service provision has not been established. Thus, it is unclear whether the financial regulators have the authority to oversee the payment network, or if it is the responsibility of the telecommunications regulators, or if anyone has the requisite authority.

Jurisdictional concerns may be exaggerated, since the service functions are distinct. For instance, in the United States, many grocery stores provide access to financial services (credit unions, etc) but their core business is selling groceries. Their financial activities are easily overseen by financial authorities and their core business is overseen by state food safety regulators.

Objective:

- Clearly defined centralized regulatory authority for mobile payment networks.
- Clearly defined authority to refer breaches of public trust or illicit activities to law enforcement authorities for prosecution.

Policy Table:

Options	Implications
1. Empower through law/regulation either the financial regulator or telecommunications regulator as the sole regulatory authority over mobile payment system.	• Sole authority limits confusion regarding investigative authority. • However, different issues may require different subject matter expertise which may not be resident in the sole regulator. • Capacity/Budget of sole regulator may need to be adjusted to accommodate increased responsibility.
2. Harmonize enforcement and penalty authority framework across Communications and Financial Services regulatory authorities.	• Harmonization process defines which regulator is responsible for which tasks, mitigating risks of issues "falling between the cracks" or of overlapping or contradictory activities. • However, emerging risks may create confusion regarding responsibility. • Authorities may lack capacity to implement across institutional silos.
3. No Formal System (Ad hoc – on a case-by-case basis as determined).	• Lack of defined responsibility regarding specific risks will create confusion and uncovered areas, creating risk for the financial sector.

Policy Narrative:

FATF Recommendations 29-31 address adequate powers, adequate resources and effective mechanisms regarding human capacity of both appropriate authorities to monitor and mitigate illicit financial activity. Compliance by financial institutions is addressed by Recommendation 29; Supervisors should be "authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose adequate administrative sanctions for failure to comply with such requirements." Countries, as well, should both provide their competent authorities involved in AML and CFT with sufficient "financial, human, and technical resources" (Rec. 30) and well as ensuring that "policy makers, the FIU, law enforcement and supervisors" can effectively and efficiently develop and implement AML and CFT policies (Rec 31).

Market Examples:

- **Malawi:** The Malawi FIU was established under the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Act, Number 11 of 2006 and became operational in July 2007. The FIU is an autonomous national body which reports directly to the Malawi Minister of Finance. Under the auspices of the Act, the FIU is responsible for identifying the proceeds of serious crime and combating money laundering and terrorist financing activities. To meet these obligations, it works in coordination with investigative authorities, such as the Anti-Corruption Bureau (ACB), the Director of Public Prosecution (DPP), Fiscal and Fraud Police Unit (FFU), the National Intelligence Unit (NIS) and the Malawi Revenue Authority (MRA).[165] The Act itself imposes reporting obligations, such as KYC of the customer and beneficial owner when, for instance, carrying out an electronic funds transfer.[166]
- **India:** The law governing AML/CFT issues was promulgated in 2002 under the Prevention of Money Launder Act and applies to banks and financial institutions. The Reserve Bank of India (RBI), the Central Bank, has experimented with the use of third party business correspondent (BCs) regulations to deliver financial services outside bank branches, though this met with limited success and the original circular issued in 2006 was subsequently revised in 2009 to lessen the restrictions on BCs. While the AML/CFT regulations regarding KYC and residency requirements for small value accounts were relaxed in 2005 for banks, the potential for MNOs and mobile financial services was less optimistic until 2008. The Payment and Settlement System Act went into effect then and RBI issued guidance regarding the issuance of prepaid payment instruments, which would permit MNOs in partnership with banks, to issue mobile wallets.[167] The Financial Intelligence Unit of India (FIU-IND) was established by the government in 2004 as the central agency responsible for receiving, processing, analyzing, and disseminating information relating to suspicious financial transactions. FIU-

Risk-based Policy Matrix – Appendix

IND is an independent body reporting directly to the Economic Intelligence Council (EIC), which is headed by the Finance Minister. FIU-IND is currently staffed at 43 individuals.[168]

- **Pakistan:** The State Bank of Pakistan (SBP) supports legal and regulatory adaptations facilitating branchless banking, which uses information and communication technologies and non-bank retail agents, while also remaining cognizant of potential risks that may arise from these models. The Ministry of Information Technology (MoIT) expressed interest during a CGAP assessment in lessons learned from international experience of such models. The Pakistan Telecommunications Authority (PTA), as the telecommunications regulator, requires notification prior to the introduction of m-banking services as with any value-added service launch. Should an MNO provide financial services, this would fall under the auspices of the SBP or the Securities and Exchange Commission of Pakistan (SECP).[169] In November 2009, the "Ordinance to Provide for the Prevention of Money Laundering (AML Ordinance) established a Financial Monitoring Unit (FMU) to receive and analyze reports of suspicious transactions, assist in investigations, and exercise general AML responsibility. Strategic oversight and administration of the FMU was established by the AML Ordinance with creation of the National Executive Committee, which publishes an annual AML strategy.[170]
- **Philippines:** The Anti-Money Laundering Council (AMLC), The Philippines' Financial Intelligence Unit, is composed of the Governor of the Bangko Sentral ng Pilipinas (BSP) as Chairman and the Commissioner of the Insurance Commission (IC) and the Chairman of the Securities and Exchange Commission (SEC) as members. AMLC was established in 2001 with Republic Act No. 9160, otherwise known as The Anti-Money Laundering Act of 2001. In addition to creating the FIU, the Act, a) criminalizes money laundering; b) imposes customer ID, record and reporting of covered and suspicious transaction requirements; c) provides for freezing/seizure/forfeiture/recovery of dirty money/property; d)provides for international cooperation; e) relates bank deposit secrecy laws.[171] Several Resolutions were passed in 2004 by AMLC to combat text messaging scams (No. 361), where deceiving messages were sent to prospective victims through cell phones using the names of the Bangko Sentral ng Pilipinas, the Philippine Charity Sweepstakes Office, the Philippine Amusement and Gaming Corp., and other institutions, advising recipients about an alleged raffle drawing with purported winnings of millions of pesos.[172]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x		x		x	x	x	x

Risk-based Policy Matrix – Appendix

7.7. Risk (National Regulators):

"Service provider may fail to institute appropriate safeguards against newly emerging risks."

Description:
Mobile financial services are a dynamically growing market with new account providers, new services and new vulnerabilities developing rapidly. Ensuring that information on the risk factors is disseminated and understood, and appropriate safeguards instituted, is a significant challenge.

Objective:

- Regulators to ensure account providers monitor evolving new risks, and institute appropriate risk mitigation.
- Regulators routinely disseminating warnings of new risks as these are identified.

Policy Table:

Options	Implications
1. Regulatory authority, or financial intelligence unit (FIU), monitors emerging risk for financial sector, including mobile payment systems.	• Emerging risk monitoring will help the providers be vigilant with regards to emerging risk, so they can develop mitigation strategies early. • Would benefit from integration into the global FIU network. • FIU may not have the skills / capacity necessary to analyze risks associated with this new channel. • FIU may not have the budget to cover this area.
2. Association of account providers monitors emerging risk for financial sector, including mobile payment systems.	• Emerging risk monitoring will help the account providers be vigilant with regards to emerging risk, so they can develop mitigation strategies early. • Individual account providers generally linked to international institutions operating in multiple countries, allowing for cross fertilization. • There may be no association at the country level - but account providers linked to the GSM Association.
3. No oversight of emerging risks	• Emerging risks may not be spotted until the risk is has become a significant problem.

Policy Narrative:

According to FATF Recommendation 8, financial institutions should pay special attention to any money laundering threats that may arise from new or developing technologies that might favor anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, financial institutions should have policies and procedures in place to address any specific risks associated with non-face-to-face business relationships or transactions. Further to Chaitlan et al's work, is the prudent aim that, prior to instituting regulatory controls, competent authorities should conduct risk-based assessments as risk mitigation factors will vary by jurisdiction and services provided. Consequently, this necessitates analysis for national regulators to " (i) better understand the issues, (ii) gauge the magnitude of risks, and (iii) take the appropriate policy measures."

Market Examples:

- **Zambia:** THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS BILL, 2009, "An Act to develop a safe, secure and effective environment for the consumer, business sector and the Government to conduct and use electronic communications; promote legal certainty and confidence, and encourage investment and innovation, in the electronic communications industry; facilitate the creation of secure communication systems and networks; establish the Central Monitoring and Coordination Centre and define its functions; repeal the Computer Misuse and Crimes Act, 2004; and provide for matters connected with or incidental to the foregoing."
- **El Salvador:** Providing service offerings via electronic channels, banks are required to submit their respective service level contracts for review to the Superintendence of the Financial System (SupFin). SupFin may request contract changes. Under Article 56 of the Banking Law, banks must clarify the rights and obligations for electronic transactions, as well as provide customers with instructions for the use of the technology and institute systems for the substitution of the client's signature substitution in electronic records.[173]
- **Pakistan:** Under the Commercial Bank Regulations, commercial and Islamic banks must collect additional information on their Level 2 and 3 customers, which may include:

a) an attested photocopy of the computerized national identity card (CNIC), verified by NADRA,
b) if the CNIC does not contain a photograph, then an additional ID, such as a driver's license,
c) if no other photo ID is available, then a photograph attested by a bank officer and the CNIC attested by the same individual, with a written confirmation attesting there is no other photo ID extant,
d) an attested copy of a service card or certification from an employer,
e) for an illiterate person, a passport size photo with both the right and left thumb print on the signature card. CNIC verification may be completed online. In terms of the transactions, the banks must obtain "accurate and meaningful" information on the originator, including the name, address, and account number. This information should follow the funds transfer throughout the course of the payment chain. Further, these financial institutions should both track and report all suspicious transactions and retain all identifying records and transaction data for at least five years.[174]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model

Risk-based Policy Matrix – Appendix

	x		x	x	x	x	x	

Risk-based Policy Matrix – Appendix

7.8. Risk (Account Providers):

"The ability to track/investigate illicit transactions is made difficult by the number of financial intermediaries (e.g. agents, super agents, providers, banks managing the trust accounts); and as these various actors are not vertically integrated, the lack of transparency between them exacerbates the challenge for regulators."

Description:

Criminal elements can utilize the lack of standard processes in conducting transactions, particularly in commingled accounts and instances where it is difficult to identify the beneficial owner. This risk may be heightened with remote and non-face-to-face transactions, particularly in the cross-border context of some MFS business segments.

Objective:

- Minimum standard audit trail for SMS/USSD (Unstructured Support Service Data) transactions to enable investigation through account providers' payment transaction processing system consistent with international standards, with accurate and meaningful information that travels with each transaction.
- Contracts clearly identify the responsibilities of each party in the transaction and provide clear channels for sharing information.

Policy Table:

Options	Implications
1. Regulatory authority mandates inclusion of accurate and meaningful information with transfer or related message through the payment chain.	• Implies regulatory involvement in data standards and oversight over account provider data transmission and retention policies and procedures.
2. Regulatory authorities prohibit mobile financial services outside of the same account providers or bank.	• Would limit the complexity of transactions. • Prohibits the expansion of low cost mobile financial services and would inhibit service innovation and outreach.
3. No regulatory action	• Regulatory authorities would rely on account provider records.

Policy Narrative:

The Basel Committee on Banking Supervision recommendations on CDD/KYC for such financial intermediaries corresponds in this regard to similar due diligence to mitigate risks for mobile financial services accounts opened or operated by professional intermediaries. Where funds/value are held by an intermediary and are not co-mingled in pooled accounts, but can be attributed to a beneficial owner, then beneficial owners should be identified. If funds/value are co-mingled in pooled accounts, the mobile financial services providers should look through to the beneficial owner.[175]

Such financial intermediaries should be identified in the case of alternative remittances as well. FATF Special Recommendation VI states that "each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanctions."

Account providers should be sure that accurate and meaningful information travels with the transfer or related message through the payment chain to mitigate risks.

Seven countries were the subject of a multi-year, regulatory diagnostic study by CGAP on the emergence of branchless banking.[176] The two models identified in the CGAP study – bank-based and non-bank based – employ the use of professional intermediaries to deliver mobile financial services.

The key distinction between the two models examined in the CGAP study is that in the non-bank based model, the customer has no direct contractual relationship with a prudentially licensed and regulated financial institution. Rather, the customer exchanges cash or value with a retail agent, such as a merchant or retail market, in exchange for an electronic record of value. This virtual transaction record is stored on the server of the non-bank intermediary, such as a mobile operator or stored value card issuer. A more limited version of the non-bank based model exists in the form of the payment networks, which utilize either ATMs or merchant point-of-sale terminals to conduct transactions.[177]

Market Examples:

- **Kenya:** Draft CBK bill impact on remittance sector, according to authors of Genesis, would be dramatic. Complying with FATF Special Recommendations VI and IX will be pose a burden for informal money remitters, given that these recommendations specify that governments "should license or register all informal transfer operators and ensure that they are AML/CFT compliant to the level of banks (SRVI), and should put measures in place to detect the physical cross border transportation of currency (SRIX). The informal sector exists in part because the right to transfer money formally is reserved for license-holders (banks, partners of banks, Postbank or POSTA). For an informal provider to become "formalized", it would be necessary to register as a bank or partner with a bank – both difficult options for current informal players."[178]
- **India:** Prior to 2009, only banks and financial institutions were allowed to issue e-money and collect funds for payment to third parties. The Reserve Bank of India (RBI) issued further payment guidance relative to the Payment and Settlement Systems Act of 2007 in the form of the April 2009 Prepayment Instrument Guidelines. Only banks may issue the three types of payment instruments identified by the Guidelines and only those authorized by RBI may provide mobile banking transactions or launch mobile wallets. The three categories of prepaid instruments include the terms paper vouchers, smart cards, magnetic stripe cards, Internet wallets, and mobile accounts and wallets. The categories include: (1) closed system payment instruments, utilized only for purchase of

Risk-based Policy Matrix – Appendix

goods and services; (2) semi-closed payment instruments, which may be either used at identified merchant locations, but not for cash withdrawal/redemption; (3) open payment instruments, which may be used at any point-of-sale (POS) enabled merchant and for ATM cash withdrawals. In August 2009, RBI expanded the Guidelines so that "other persons" where permitted to issue mobile phone-based semi-closed prepaid instruments restricted to Rs 5,000 ($110) value, with no P2P transfers or airtime recharges. RBI relaxed the KYC procedures in the interest of financial inclusion, with semi-closed instruments of Rs 1,000 or less issued against any identity document, provided the issuer confirms the customer holds only one instrument at a time; any prepaid instrument of Rs 5,000 or less issued against any officially valid ID document defined in the Prevention of Money Laundering Act and semi-closed instruments of up to Rs 5,000 issued to companies, which may, in turn, issue them to employees or other beneficiaries provided they maintain full details of the reissuance. Issuers must comply with existing AML/CFT rules, as well as maintain a transaction log of prepaid instruments available for review by RBI. [179]

- **Indonesia:** The E-Money Circular details licensing specifications for both bank and non-bank issuers of e-money. Among the risk mitigation factors which may assist in identifying financial intermediaries are requirements for among the required documentation of obtaining licensing, such as first year business projections, written agreements with key partners, proof of liquidity risk management, independent IT risk auditing, disaster recovery planning, accounting systems used for e-money issuance, and "identification of product risk and other risks like operational, legal and reputational risks."[180]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
x		x	x		x	x	x	

Risk-based Policy Matrix – Appendix

7.9. Risk (National Regulators):

"Account provider suspends operations or collapses, disrupting service."

Description:

Temporary or permanent failure of a systemically important account provider could trigger loss of public confidence that could spread beyond the account provider, causing a general crisis of confidence among the public.

As communication networks are relied upon for financial services, disaster recovery is critical and it may become increasingly dependent upon regulatory authorities to set redundancy requirements.

Objective:

- Contingency response policies and procedures to ensure continuity of operations and rapid recovery in case of failure.

Policy Table:

Options	Implications
1. Regulatory authority mandates system redundancy requirements and disaster recovery policies and procedures to ensure continued public access.	• Redundancy and continuity will mitigate the risk of system availability and limit the duration when a failure occurs. • Documented alternative access procedures in the event of system failures for providers
2. For cell phone based systems, regulator requires off-site storage of backup data in a format that would enable an orderly liquidation of the trust account(s) through repayment to system users. For bank based systems based on individual bank accounts, normal bank processes required.	• Implies an orderly liquidation process or transfer to an alternate account provider similar to that used for a failed financial institution.
3. Providers establish their own redundancy requirements and disaster recovery to ensure continued financial system access.	• Redundancy and continuity will mitigate the risk of loss of system availability and limit the duration when a failure occurs. • Documented alternative access procedures in the event of system failures for providers. • Lack of regulatory requirement will allow each institution to define the extent of their contingency plans, which will leave some less protected than may be appropriate for the payment system. However, it will also allow individual institutions to innovate.

Policy Narrative:

The core components of any payment system must ensure availability, capacity, operational continuity, and security to the public that is being served. This may necessitate both integrating existing technologies in new ways, as well as providing interoperability among new actors with innovative technologies. The National Fire Prevention Association NFPA 1600 defines Business Continuity Program (BCP) in its general definitions as follows: An ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and recovery plans, and ensure continuity of services through personnel training, plan testing, and maintenance. An enhancement to NFPA includes recovery actions, which often extend long after the incident itself and the related programs should be designed to include mitigation components for avoiding damage from future incidents.[181] Contingency plans for e-government can mitigate the risks of external events, specifically if the BCP encompasses resilience in communications and financial services via mobile banking and payments.

Market Examples:

- **Brazil:** All clearing and settlement account providers are either banks or entities controlled by banks, with the largest ATM and POS networks controlled by the largest banking conglomerates. Access to these systems is self-regulated, with oversight by the Central Bank of Brazil (CBB). The interoperability among the 25 ATM and 4 POS networks, as well as the dominance of the large banks, is driving small and medium sized institutions to create an independent automated clearing house (ACH) for low value payments, including mobile banking. While in the nascent stages, it is nonetheless encouraged by CBB.[182]
- **El Salvador:** The Central Reserve Bank (BCR) has broad regulatory authority over check clearinghouses and other payment systems used and operated by financial institutions; however there is no national payments law in El Salvador. El Salvador is a signatory to the Central American Treaty on Payments, under which BCR maintains oversight of what it considers to be systemically important payment and settlement systems. BCR also defines the parameters of high and low value payments under the Treaty terms and conditions, though the Treaty does not specifically cover retail payments. The issuance of stored value instruments, such as prepaid cards and mobile banking, have not been clarified within the context of the regulatory framework for payment services.[183]
- **South Africa:** Under the auspices of The South African Reserve Bank Act, the South African Reserve Bank (SARB) is authorized to "perform the functions, implement the rules and procedures, and in general, take the steps necessary to establish, conduct, monitor, regulate, and supervise payment, clearing, and settlement systems. Access to the national payment and settlement systems is restricted to banks only, with non-bank actors able to access the system via joint ventures with banks that are existing members. Under the National Payment System Act of 1998, SARB can delegate its responsibilities to a self-regulatory industry body, while retaining oversight control, and has done so with respect to the Payments Association of South Africa (PASA); PASA has appointed Bankserv as the payment clearinghouse for the South African banking industry and Bankserv provides interbank electronic transaction switching services to the banking sector. The switching services are majority owned by the countries four largest banks, ABSA Bank, First National Bank of South Africa (FNB), Nedbank, and Standard Bank, with 90% of the market. [184]

Risk-based Policy Matrix – Appendix

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
x	x	x	x	x	x	x	x	x

Risk-based Policy Matrix – Appendix

7.10. Risk (National Regulators):

"Account provider employee sets up accounts on the system with balances not backed by currency. Such an act would create a liability for the MNO. Also, national regulators would be concerned of the impact on the economy if such a scheme were executed on a large scale."

Description:
Generally, when a customer sets up a prepaid mobile payment account, they make a deposit of real currency for an equivalent balance of mobile money. However, an employee of the MNO with access to the backend systems could set up fraudulent new accounts that were not backed by currency. The employee could then either cash-out or spend their mobile money creating a liability for the MNO that could go unnoticed without proper internal safeguards. Since e-money is backed by real money deposited in the trust account (or the capital of the account provider, if deficient), creation of e-money may increase the velocity of money, but not the volume.

Objective:

- Account providers ensure sufficient internal controls and monitoring of the trust balances against the amount in transit to discourage such defalcations and rapidly identify them should they occur.
- Subject to regulatory oversight.

Policy Table:

Options	Implications
1. Regulatory authority requires account providers to conduct due diligence screening on key employees and obtain fraud insurance (bonding) to protect against insider fraud.	• Insurance will mitigate the risk to account providers and the financial system of fraud. • Fraud insurance may not be available or be expensive. • Bonding costs lower if the legal system has the capacity to arrest, prosecute and convict those who commit fraud.
2. Providers implement institution specific fraud detection systems.	• Account providers have a vested interest in protecting themselves from internal fraud and in implementing appropriate internal controls. • Fraud detection allows for issue identification, investigation and prosecution. • Variance across institutions may let criminals target weak systems; however, competition will allow for innovation.
3. No required regulatory response to insider employee fraud.	• Small-scale insider manipulation is unlikely to have much impact. • Systemic fraud by insiders could damage the stability of the financial system and will significantly damage the reputation of the mobile system.

Policy Narrative:
Fundamental to most business models is the integrity of the employees. However, without proper safeguards, employees may be tempted to steal from their employer. If an employee of a service provider set up new mobile money accounts with mobile money balances which were not backed by currency, they could use that mobile money, whether through a cash-out, merchant purchase, or person-to-person transaction, and create a liability for the service provider. In effect, they are stealing from their employer. Without proper safeguards (i.e. daily settlement and fraud protection, which would identify unbacked balance increases or account set-ups), such liabilities could go unnoticed, as the trust fund would not routinely be fully drawn down. Employees should be subject, whether by regulatory requirement or firm policy, to due diligence screening which would identify those with a criminal history. Further, fraud insurance could be purchased to hedge against such behavior. Again, either by regulatory requirement or firm policy, internal controls should be in place that would quickly identify cash-in transactions that were not backed by physical currency. Daily settlement across the agent network should highlight any anomalies and allow for investigation. With the legal and reputation risk that exists, account providers have no incentive to manipulate mobile money balances; however, employees may attempt to do so at their employer's expense. As such, regulators and providers must be diligent in establishing the proper controls that can mitigate the potential for any systemic impact.

Market Examples:

- ***Please Note:*** *A market example of a policy action associated with this risk was not identified during the literature review or the in-country consultations included in this project's scope. We welcome your suggestions of relevant examples for inclusion in subsequent versions.*

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x	x	x	x		x	x	x

Risk-based Policy Matrix – Appendix

7.11. Risk (National Regulators):

"In economies where minutes are exchanged like currency, and could be cashed-out for currency, distributor of airtime vouchers or distributor employee could increase the amount of airtime on the market."

Description:

In some economies, mobile minutes have been used as a means of exchange. Generally, an MNO will provide mobile minutes as a service for a specific price. However, an MNO could increase the number of minutes on the market without compensation for various reasons, such as extra minutes to reward customer loyalty. MNO employees could also set up accounts with minutes for which they did not pay. An increase in the number of minutes on the market will depreciate their worth overtime. If a cash-out opportunity is available, an individual that set up fraudulent accounts could make quick money.

Objective:

- The account provider's business model will determine the extent of service discounts they wish to provide to their customers. Not a regulatory issue.

Policy Table:

Options	Implications
1. No regulatory action	• Hopefully cell phone company "sales" that reduce the cost of airtime will result in increased business rather than losses.

Policy Narrative:

FATF's 9 Special Recommendations, specifically on Alternative Remittances (SRVI) stress that each country should "take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including the transmission through an informal money or value transfer system or network" should be subject to licensing or registration, as well as subject to all FATF recommendations that apply to banks and non-bank financial institutions. Further to the interpretive notes provided, a money or value transfer service may be defined as including "persons providing either through the formally regulated financial system or informally through non-bank financial institutions or other business entities or any other mechanism either through the regulated financial system (for example, use of bank accounts) or through a network or mechanism that operates outside the regulated system." Considering SRVI in its entirety, including the interpretive notes, which elaborate that these alternative remittances may be defined as including underground banking systems such as hawala, then airtime value transfers may be considered an informal value transfer mechanism.

Market Examples:

- **Indonesia:** It is estimated by the World Bank that approximately 205 of total Indonesian remittances occur through formal channels. The predominant forms of remittance are returning migrants (hand delivery), courier, employment agencies, and money changers, according to a recent CGAP survey. In an effort to address this issue, the E-Money Regulation does distinguish between registered and unregistered issuance of e-money, with registered e-money requiring substantial data capture on the customer. For instance, issuers must record the name, address, date of birth and other data as listed in the customer's identity card. Unregistered e-money is limited to IDR 1,000,000 or USD 100 with the top value of 5,000,000 (approximately USD 500). While e-money loads may be performed by agents, cash-outs require a money remitters license.[185]
- **Kenya, South Africa, Tanzania**: Me2U, offered by MTN in South Africa, or Sambaza, offered by Safaricom in Kenya, offer popular airtime transfer services whereby for a small fee one prepaid customer may transfer a portion of airtime to another customer on the same network. This phenomenon has led some pundits to comment that airtime has become an alternative form of e-currency. The Economist reported in 2005 that a woman in the Democratic Republic of the Congo settled a bribe to officials across the country by sending them airtime. While airtime is not redeemable at par into cash and a telco commission for redemption is typically 15% on the face value of airtime at first sale. An airtime vendor, according to anecdotal interview with a Super Agent in Tanzania, indicated that "second hand" airtime transfers at a 15-20% discount that he could re-sell to other users effectively match or exceed his commission. This compensates for the loss of his network commission. He noted that this method of airtime re-sell is frequently used by parents to, with him as intermediary, to earn funds for their college age students.[186]
- **Saudi Arabia:** The company, TransferTo, advertises international airtime transfers as "an effective compliment to money remittance." The company has initially identified 25 mobile operator airtime transfer corridors in 7 countries (Jordan, Egypt, India, Pakistan, Sri Lanka, Indonesia, and the Philippines) between Saudi Arabia. There are potentially over 100 migration corridors where the service could be deployed.[187]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x	x	x	x	x	x		

Risk-based Policy Matrix – Appendix

7.12. Risk (National Regulators):

"Increasing reliance on mobile financial services may result in a concentration of deposits in one or a few trustee financial institutions, leading to disintermediation from smaller institutions and reductions in access to finance from those institutions."

Description:
Rather than having funds dispersed across the financial system, or outside of the financial system entirely, the uptake of mobile payment services will concentrate payment account funds in the trust funds held in only a few institutions. The financial institutions where some of these funds would have been deposited will have fewer resources with which to make loans. The institutions holding these funds could be restricted by regulations, or their own credit policy decisions, from using these funds for lending. The institutions holding these funds could be restricted by regulations, or their own credit policy decisions, from using these funds for lending, thus reducing the level of loan funding available to the economy. This could lead to consolidation within the financial system resulting from those institutions that are not able to keep up with the technology having increasing difficulty competing. However, the conversion of cash in circulation to deposits in the trust accounts would increase the resources of the banking system as a whole.

Objective:

- Application of prudential guidelines on risk concentrations/dependencies to account provider trust accounts.
- Expansion of larger financial institutions down-market as the technology lowers transaction costs and service break even points.

Policy Table:

Options	Implications
1. Law/Regulation that limits the size of a trust account or group of trust accounts from any account provider in any one trustee institution to a percentage of the trustee's risk weighted capital.	• Diversification of trust accounts holdings across multiple financial institutions reduces risk concentrations. • Spreading trust funds across multiple financial institutions will add complexity for account providers, increasing operating costs. • Implies regulatory oversight to ensure compliance.
2. No regulatory action	• account providers hedge their risk relating to concentration of deposits based on profit motive, which may not align with what is best for the market as a whole.

Policy Narrative:

With the increasing demand for mobile financial services, customers will have a broader range of financial products and services from which to choose and will likely have the opportunity to "bundle" this new mobile financial service with other financial services and products offered through the same financial institution. As a result, there could be a significant move of customers away from smaller deposit taking institutions (such as the savings and loan model) or a cooperative, toward a larger commercial bank that is safer, and which offers the convenience and reduced costs associated with cell phone banking. New funds will flow into a bank account if they are in a savings account linked to the mobile phone banking service, or a trust account if they are just payments in process. Either way, both the savings account and the trust account are considered bank accounts, and so form part of the deposit base of the bank. The bank may choose to invest some of these funds in government paper which would, in the short run, reduce the funds available in the bank account. However, the remaining balance would still be available as part of the bank's overall deposit and lending base. The net result would be an increase in the commercial bank's lending capital base, and a corresponding decrease in the lending capital base of the smaller, less competitive financial institutions, particularly those that are unlicensed and that lack core back office technological and human capacity necessary to adopt front-end mobile phone banking technologies. Should the larger commercial banks choose to extend their market into rural regions through mobile phone banking that does not require the setting up of costly rural bricks-and-mortar branches, they will likely crowd out the smaller institutions, including those smaller unregulated microfinance institutions that lack the core technology capacity to become integrated into the cell phone banking ecosystem. MFIs can consider partnering as an agent network with a mobile network operator, taking advantage of the MNO's comparative advantage in having in place many of the technological and payment systems necessary to engage in mobile phone banking. Moreover, the commercial banks can capitalize on the MFI's ability to reach down-market into rural communities, and maintain a strong client base through their comparative advantage in utilizing relationship banking as part of their core operating strategy.

Market Examples:

- **Kenya:** In May 2010 a new product was launched in Kenya that links M-PESA cell phone users with one of Kenya's leading commercial banks, Equity Bank, through an interest-bearing savings account. "M-Kesho" will now allow M-PESA users to have direct access to mobile microsavings, microinsurance, and other banking services with and through a regulated commercial bank.[188]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
						x		

Risk-based Policy Matrix – Appendix

7.13. Risk (National Regulators):

"Single dominant player in a closed-loop environment abuses market power (predatory pricing)."

Description:
A single telecom company can dominate the market in the absence of adequate competition. The first player to enter the market can create a monopoly, which can potentially lead to anti-competitive pricing and restricted services/innovation.

Objective:

- Fair competition among providers on products/services.
- No unreasonable barriers to the flow of funds between account providers.
- Predictable market entry for qualified applicants to ensure that the prospect of competition discourages predatory pricing.
- National and regional payment systems able to transmit payments between account providers and between countries.

Policy Table:

Options	Implications
1. Regulators require interoperability of payment networks (through inter-provider links or through a switch)	• Requirement of interoperability could raise a barrier to entry as the technology requirements could be more challenging than a simple closed network. Further, the requirement could stifle innovation in a new technology through keeping new entrants out. • Customers would benefit as there would be no network limitations on sending mobile money. • Providers would be forced to compete on cost, products, and service, rather than size of network which could represent a first mover advantage. • By reducing the first mover advantage, could discourage potential first movers from entering the market.
2. Competition agency empowered to investigate non-competitive behavior	• Implies a competition agency with the capacity to investigate and enforce non-competitive behavior, such as predatory pricing, to counteract the incentive for monopoly pricing, thus protecting the consumer. • However, may impede development of cross network transaction capability.
3. No regulatory action	• Predatory pricing and expanded monopoly power are possible. However, experience with networked technologies (cell phones/ATMs) suggests that the market will move toward interoperability without regulatory action. • Provided that account providers are given consistent market entry requirements, abuse of the first mover advantage will encourage competition to enter the market.

Policy Narrative:
This risk focuses on the concept of interoperability among competing national and international MFS systems. Universal acceptance by all consumers, regardless of mobile network operator or MFS platform affiliation, will impact penetration growth and the overall sustainability of MFS.

In markets where MFS services are being led by mobile network operators (MNOs) interoperability is limited to peer to peer transfers to rival MNO subscribers through a mechanism that requires cash out, switching to and registering with the sender's service.

In markets where a third party is the dominant MFS provider (e.g., Wizzit) specific MNO affiliation is not a requirement. However, all transactions must be made through the third party platform and connectivity to other MFS providers is not possible.

In markets where banks are the leading players, the existing financial sector clearing processes act as a catalyst for interoperability. However, to date this has not translated into an effective interoperable MFS system.

In other fields, consumer demand typically drives the development of industry standards and interoperability (e.g., GSM operations). With respect to MFS, financial regulators are positioned to regulate interoperability, but thus far, have not done so.

Market Examples:

- **El Salvador:** According to a CGAP interview with the Central Reserve Bank (BCR), limited interoperability for retail payments hampers customers from cash-based deposit and withdrawal services in bank branches, as well as transferring funds from bank-to-bank using the Internet channel. Mobile banking is in the embryonic stages, and similar to Internet banking, is available only to those who already have bank accounts.[189]
- **Pakistan:** The State Bank of Pakistan (SBP) considered several branchless banking models before initially deciding to allow only bank-led models. In all cases, the customer has an account relationship

Risk-based Policy Matrix – Appendix

with the bank through establishment of a branchless banking account. The many-to-many model involves a central transaction processing system or switch, providing total interoperability. Though not yet implemented, this is the preferred model of SBP and allows multiple banks to offer services to customers of multiple agent networks or MNOs. The switch must be controlled by the bank, an agent or a subsidiary of the bank or group of banks. Banks can purchase access to the switch, similar to access to an ATM network, which would reduce the technology investment burden placed on any single bank.[190]

- **Indonesia:** Article 27 of the E-Money Regulation mandates that e-money providers must offer systems that are interoperable with other e-money systems.[191]
- **Iraq:** The U.S. Department of Defense funded a $2 million initiative in cooperation with private banks to develop a shared, multi-channel electronic funds transfer switch to enable m-banking, Mastercard/VISA POS, and ATM services. M-banking features include a USSD user interface with P2P transfers, airtime top-up, and balance inquiry services. As of 2010, five banks and one MNO were participating in the system.[192]
- **South Africa:** WIZZIT, founded in 2004 by two entrepreneurs and operating in partnership with the Bank of Athens, offers mobile banking services to approximately 300,000 customers. The company is mobile phone agnostic, so that customers can use phones operated by any of South Africa's mobile operators, for services ranging from transferring money to third parties, loading electricity with prepaid cards, and buying airtime for prepaid mobile phone subscriptions. Since WIZZIT has no brick and mortar branches of its own, it operates 3,500 deposit taking sites in conjunction with the Post Office and ABSA Bank. Customers are issued a Maestro-branded debit card, which they may use for cash withdrawals at any South African ATM.[193]
- **Spain:** Mobipay, was launched as mobile payments platform, as a result of a joint venture between Spain's largest telco, Telefonica, and a bank, BBVA. At the time this venture, the Spanish Competition Authority (SDC) was concerned that m-payments would affect not only e-commerce but also mobile telephony; it approved the JV with certain stipulations:
  -other mobile operators must be allowed to participate;
  -the interoperability of any mobile operator and any financial institution had to be technically possible;
  -customers could not be limited in their choice of other MNOs or financial account providers by the service contract;
  -SDC had approval authority for interchange fees.
  While initially slow to market in Spain, BBVA, took the product to Mexico and North Africa in 2005.[194]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
						x	x	

Risk-based Policy Matrix – Appendix

7.14. Risk (National Regulators):

"Illicit actors conduct high volume transactions using multiple accounts, bypassing monitoring systems before regulators can step in."

Description:
Because of the speed of the payment process using a mobile system, it is possible to make multiple transactions quickly, in a near real-time transaction environment.

Objective:

- Account providers flag and limit opening multiple accounts based on similar KYC/ CDD data.
- Subject to regulatory oversight.

Policy Table:

Options	Implications
1. Account providers required to flag and block multiple accounts with similar KYC/ CDD data.	• Monitoring systems can deter most illicit activity • Implies regulatory verification of account provider policies, procedures and its capacity to comply.
2. Rely on account monitoring as another alternative to KYC.	• . Multiple accounts of the same owner can be identified via pattern identification systems that recognize activity similarities (e.g. several account all sending money to the same place/agent/customer or e.g. an unusual level of transactions from one place to another in a given timeframe.) • Enables expanded access where national ID systems may be weak.
3 No regulatory action.	• Providers will institute risk mitigation systems in line with their perceived risk to abuse of their system.

Policy Narrative:
The alleged Madoff $50 billion dollar Ponzi scheme is perhaps a classic example of massive fraud, both in terms of scope and duration, where monitoring systems and human capacity failed on a systemic level.[195] Madoff founded his investment advisory business (Bernard Madoff Investment Securities) in 1960 and maintained a prominent standing in the securities industry throughout his career until the fraud was exposed in 2008. Not only was he a member of the NASDAQ Stock Market's board of governors and its executive committee, he also served as chairman of its trading committee and vice chairman of the NASD. When educated of such schemes, public awareness campaigns may provide the best, first line of defense.

Market Examples:

- **Tanzania:** During investigations of operations, the DECI (T) Limited company did not operate a microfinance bank account in its name, but apparently collected funds from its members and deposited them in personal bank accounts.[196] "The public is also notified that the capital markets and securities authority (CMSA) has not granted a license to DECI (T) Limited to operated collective investment schemes in Tanzania. It should be noted that promotion and participation in any pyramid schemes is an offence in terms of the provision of the penal code (as amended in 2006) While authorities are still carrying out investigation to establish the scope and nature of operations of DECI (T) Limited in the country, the general public is warned to desist from participating in the scheme operated by DECI (T) Limited."[197]
- **Pakistan:** The Financial Monitoring Unit (FMU) provides the following functions related to suspicious transactions: (b) to analyze the Suspicious Transaction Reports and CTRs and in that respect may call for record and information from any agency or person in Pakistan (with exception of income tax information) related to the transaction in question. All such agencies or persons shall be required to promptly provide the requested information. (j) to engage a financial institution or an intermediary or such other. non-financial businesses and professions or any of its officers as may be necessary for facilitating implementation of the provisions of this-Act, the rules or regulations made hereunder…"[198]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
x		x	x			x		

Risk-based Policy Matrix – Appendix

7.15. Risk (National Regulators):
"Financial terrorists target payment network to disrupt financial system."

Description:
Financial terrorists hack into mobile payment network to disrupt the economy. The mobile payment network may be targeted, as the security is perceived as less than that of the financial system. Alternatively, terrorists may target the data center of the account provider to damage or destroy service capacity.

Objective:

- Mobile payment networks' security requirements, including possible redundancy, to be commensurate with the proportionate systemic importance of the account provider.

Policy Table:

Options	Implications
1. Regulatory authority mandates system redundancy requirements and disaster recovery to ensure continued financial system access, particularly for significant Account Providers.	• Redundancy and continuity will mitigate the risk of impaired system availability and limit the duration when a failure occurs. • Documented alternative data access and recovery procedures in the event of system failures for account providers
2. Providers establish their own redundancy requirements and disaster recovery to ensure continued financial system access.	• Redundancy and continuity will mitigate the risk of impaired system availability and limit the duration when a failure occurs. • Documented alternative data access and recovery procedures in the event of system failures for providers • Lack of regulatory requirement will allow each institution to define the extent of its contingency plans, which will leave some less protected than may be appropriate for the payment system. However, it will also allow individual institutions to innovate.

Policy Narrative:
Recognizing the imperative nature of combating the financing of terrorism, the FATF outlined and agreed to nine Special Recommendations, which, when combined with the FATF Forty Recommendations on money laundering, set out the basic framework to detect, prevent and suppress the financing of terrorism and terrorist acts which seek to disrupt financial systems.

Market Examples:

- **United States:** The Al Qaida attacks of September 11, 2001, specifically targeted the hub of acknowledged seat of U.S. financial operations, both for sites such as the NY Stock Exchange, The Clearing House, and SWIFT NY HQ, and major commercial financial institutions. Disaster recovery was aided, in large part, due to long standing attention to cyberprotection issues by financial institutions. In 1999, industry participants established and funded one of the first information sharing and analysis centers (ISACs). More than forty of the U.S. largest banks, securities and insurance firms, investment companies, and financial utilities, representing a significant portion of assets in the financial system, participate in the ISAC. The ISAC maintains an industry wide database of electronic security threats, vulnerabilities, incidents, and solutions. Security specialists analyze reports and distribute to members warnings and information about threats and solutions or mitigation procedures. Financial institutions also actively participate in a number of other information-sharing organizations, such as the Federal Computer Incident Response Center (FedCIRC) and the System Administration, Networking, and Security Institute (SANS).[199]
- **Kenya:** In a recent presentation entitled "10 YEARS ON FROM THE US EMBASSY BOMB BLAST" in Nairobi, Kenya,"[200] Director Samuel Mutungi provided a case study on lessons learned for terrorist attacks regarding disaster recovery and business continuity planning for financial services. One of the main mitigating strategies aiding in recovery for Co-Operative Bank, despite the fact that the ICT equipment was damaged and networks/systems were destabilized, was that the Bank's systems back-up e.g , redundancies, had recently been moved off site. The 1998 attack disrupted Co-Operative Bank operations alone for 4 years; terrorist acts are not covered by insurance and rent alone cost an additional 400 million Kenyan shillings per annum for this period.

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
x	x	x	x	x	x	x	x	x

Risk-based Policy Matrix – Appendix

7.16. Risk (National Regulators):

"Account provider fails / enters insolvency limiting customer access to funds and potentially destabilizing financial system."

Description:
Mobile payment Account providers, like other companies, may fail / enter insolvency for a variety of reasons. However, unlike normal companies, their service provision is a component of the financial system and their insolvency can destabilize the economy if not properly managed.

Objective:

- Mobile payment Account providers' insolvency procedures should mimic those of financial institutions.
- Established process for obtaining records of items in transit and enabling rapid cash out liquidation or transfer to another account provider using the trust funds.
- Clear regulatory policies and procedures to manage such events.

Policy Table:

Options	Implications
1. Incorporate winding up provisions in the Law / Regulation covering mobile financial account providers, particularly on assuring regulatory access to transaction records and trust funds that back items in transit.	• Protection of payment system assets and records in case of insolvency would minimize the systemic impact of a mobile payment system failure. • Assets of clients, as in customer funds in transit or temporary storage, should be kept out of the general pool of assets available to satisfy creditors. This is particularly important in countries under statute law that does not accommodate separation of assets into trusts.
2. Insolvency handled like any other business.	• Financial system stability would be at risk depending on the size of the network. • Consumer protection for payment account holders would be a significant issue if the insolvency process did not protect these accounts differently from the general assets of the account provider.

Policy Narrative:
While mobile network operators are not subject to national banking regulation and supervision, they do, in a practical sense, undertake activities that at least mimic banking functions that would warrant such oversight. And while mobile network operators are one of several agents interacting within a mobile phone banking ecosystem, they are in many countries arguably one of the larger and more significant of actors in terms of their ability to move forward—or bring down—the entire system. As such, service providers of this size and level of market importance will need to be monitored as if they are an actual component of the financial system. Moreover, acknowledging the bailout that resulted from the fear of the systemic risk that could have been brought on by the collapse of Lehman Brothers, any one actor in the mobile banking ecosystem should not be permitted to grow "too big to fail" so as to pose a systemic risk to the entire system. At a minimum, guidelines should be established for a service provider that are similar in function to those used to identify and rehabilitate problem banks, to enact resolution management and address accounting issues in problem banks, and to address problems in large and multi-charter banking companies.[201]

Market Examples:

- **United States:** The downfall of a large Orange County investment fund in December 1994 was the harbinger of the more recent financial crisis brought on by the interaction of large market players taking excessive risks with derivatives and other highly leveraged instruments. In the Orange County case, the losses to the fund were high mainly because 60 percent of its assets were bought on credit with fund managers borrowing short-term to buy bonds maturing as far of as 1998. Soon after the collapse of the investment fund, U.S. government officials began looking closely at other large market players—such as pension funds—with the rightful concern that a sudden sell-off of derivatives from such large market players could lead to systemic risk viz. the financial markets. These market examples can provide valuable lessons to the mobile phone banking system, particularly related to the development of appropriate and prudent investment and fund management guidelines for key players in the system, including service providers and the corresponding bank partners holding the trust accounts.

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
x	x	x	x	x	x	x	x	x

Risk-based Policy Matrix – Appendix

7.17. Risk (National Regulators):
"Counterfeit funds accepted by an agent.

Description:
Agents will be targeted as an entry point for counterfeiters to unload money into the system. Counterfeiters will perceive agents as less knowledgeable than bank employees, the security/monitoring of agents to be less than banks, and yet still have a high enough transaction volume that they would be difficult to identify.

Objective:

- Agent training on counterfeits to be modeled on bank teller training and provided by account providers commensurate to the perceived risk.

Policy Table:

Options	Implications
1. Regulatory authority provides mechanism for reporting, retrieval, and criminal investigation of suspect counterfeit notes. Regulatory authority sets parameters for training material for use by account providers with their agents.	• May incentivize agent to report counterfeit activity. • Reporting facilitates identification of issues, investigation, and apprehension of counterfeiters. • Regulatory authority requires capacity/budget to support anti-counterfeiting training and enforcement.
2. Account providers required, as part of AML/CFT/Fraud training programs, to institute and monitor agent compliance commensurate with perceived risk.	• Training facilitates identification of issues, investigation, and apprehension of counterfeiters. • Active program will deter use of agents to pass counterfeit notes.
3. No regulatory response to counterfeit currency in circulation.	• Increasing circulation of counterfeit currency.

Policy Narrative:
As international authorities dealing with this issue reiterate, the crime of counterfeiting national currency is as old as the creation of money itself. With the advent advanced personal computer graphics programs and low-cost, high quality photographic and printing technologies and equipment available to the lay person, the ability to reproduce complex images on paper stock has never been easier. The resultant effect of this bogus currency introduced into circulation poses problems not only for national economies, but also for financial institutions, consumers, and economies worldwide. The intersection of mobile financial services and the use of national currencies, in this regard, pose similar need for international cooperation and private/public partnerships. These may be encouraged through such law enforcement organizations as INTERPOL, which maintains expertise through their Counterfeit and Security Documents Branch (CSDB), providing forensic support, operational assistance, and technical databases to assist the 188 member countries of INTERPOL regarding counterfeit national currencies[202]

Market Examples:

- **Kenya:** "Sec. 373 Any person who – (a) utters any counterfeit coin knowing it to be counterfeit, and at the time of such uttering has in his possession any other counterfeit coin; or (b) utters any counterfeit coin knowing it to be counterfeit, and either on the same day or on any of the ten day next ensuing utters any other counterfeit coin knowing it to be counterfeit; or (c) receives, obtains or has in his possession any counterfeit coin knowing it to be counterfeit, with intent to utter it, is guilty of a felony and is liable to imprisonment of three years."[203]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		x	x	x	x	x	x	x

Risk-based Policy Matrix – Appendix

7.18. Risk (National Regulators):

"Counterfeit funds distributed by an agent."

Description:
Counterfeiters may try to recruit agents into their networks to distribute counterfeit currency into the economy.

Objective:

- MNOs responsible for supervision of agents and collaborate with law enforcement authorities on investigation of counterfeit currency to enable criminal prosecution of agents.

Policy Table:

Options	Implications
1. Regulatory authorities should provide mechanism for reporting, retrieval, and criminal investigation of suspect counterfeit notes.	• **Reporting facilitates identification of issues, investigation, and apprehension of counterfeiters.** • **Regulatory authority requires capacity/budget to support anti-counterfeiting training and enforcement.**
2. Regulatory authorities to provide an incentive, or reward, system for reporting and retrieving counterfeit currency, possibly including cash payments.	• Financial incentives can increase cooperation of agent network in identifying and pursuing counterfeiters. • Regulatory authority requires budget to support incentive program. • Financial rewards may encourage agents to collaborate with counterfeiters; however, authorities will monitor agents more closely that consistently turn in counterfeits for reward.
3. Account providers required, as part of AML/CFT/Fraud training programs, to institute and monitor agent compliance commensurate with perceived risk	• Training facilitates identification of counterfeit currency and deters acceptance/distribution. • Agents may recirculate counterfeit currency if not incentivized or required to report it.
4. Regulatory authority or account provider could reward agents for identifying counterfeit currency or providing information on counterfeiters.	• Reward could provide the incentive for identification and the disincentive for passing the currency along. • Agents with frequent identification would need monitoring to ensure they were not involved in a counterfeit scheme. • Cost/capacity to implement such a scheme would need to be evaluated.
5. No regulatory oversight or training by account provider of agent	• Increased circulation of counterfeit currency.

Policy Narrative:
As international authorities dealing with this issue reiterate, the crime of counterfeiting national currency is as old as the creation of money itself. With the advent advanced personal computer graphics programs and low-cost, high quality photographic and printing technologies and equipment available to the lay person, the ability to reproduce complex images on paper stock has never been easier. The resultant effect of this bogus currency introduced into circulation poses problems not only for national economies, but also for financial institutions, consumers, and economies worldwide. The intersection of mobile financial services and the use of national currencies, in this regard, pose similar need for international cooperation and private/public partnerships. These may be encouraged through such law enforcement organizations as INTERPOL, which maintains expertise through their Counterfeit and Security Documents Branch (CSDB), providing forensic support, operational assistance, and technical databases to assist the 188 member countries of INTERPOL regarding counterfeit national currencies[204]

Market Examples:

- **Kenya:** "Sec. 373 Any person who – (a) utters any counterfeit coin knowing it to be counterfeit, and at the time of such uttering has in his possession any other counterfeit coin; or (b) utters any counterfeit coin knowing it to be counterfeit, and either on the same day or on any of the ten day next ensuing utters any other counterfeit coin knowing it to be counterfeit; or (c) receives, obtains or has in his possession any counterfeit coin knowing it to be counterfeit, with intent to utter it, is guilty of a felony and is liable to imprisonment of three years."[205]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x	x	x	x	x	x	x	x

Risk-based Policy Matrix – Appendix

7.19. Risk (National Regulators):

"Currency redenominated while in transit."

Description:
When a country redenominates its currency, often after a period of high inflation, service users may lose much of the value of payments in transit unless these transit amounts are also redenominated.

Objective:

- Treat items in transit in the same was as deposits in the banking system are treated in case of redenomination of the currency.

Policy Table:

Options	Implications
1. Financial regulators include mobile payment system in any implementation plans for currency redenomination and handle them as they do deposits in the banking system.	• Implies account provider capacity to adjust the nominal value of items in transit during a redenomination. • Regulatory requirements mandating that capacity may send a message to the market that redenomination is likely, possibly undermining confidence in the national currency. • May complicate the public education process during redenomination by bunching the impact for people who may be less financially sophisticated.
2. No regulatory action	• An incentive is created for moving money into or out of the mobile payment system around redenomination to benefit from arbitrage opportunity - could bankrupt the account provider and deplete the trust funds so that only the first to cash out could be paid.

Policy Narrative:
In a bank-led model, the issue of currency redenomination of electronic funds while in transit should be handled in a way similar to the manner in which deposits in the banking system are treated in the case of a sudden revaluation (up or down) of the underlying currency. The issuer of electronic cash is exposed to a number of risks related to its development and operation of a stored value system, (namely strategic, transaction, compliance, and reputation risk) as well as risks associated with its ownership of electronic cash and investing proceeds from the "sale" of electronic cash (or the holding of an account backing up the value of electronic cash). These latter risks include credit, liquidity, interest rate, and foreign exchange risk. The investment policy of the initiating entity should dictate the extent of credit, liquidity, and interest rate risk exposure that the bank can reasonably take on. Any foreign exchange risk associated with currency redenomination of mobile banking funds while in transit relates to the bank's ability to acquire and maintain the necessary expertise, such as the ability to conduct ongoing revaluations of currency through a strong internal controls system backed by adequate capital reserves.[206]

A bank's ability to manage any risk—including foreign exchange risks—rests on the fact that sound management of internal operations and risks requires appropriately qualified and well-trained staff which upholds sound business practices. Failure of staff to observe appropriate internal controls, as well as failure of the control environment, will likely lead to significant financial losses for the institution (and its partner institutions, if applicable) and will likely tarnish the reputation of the reserve management entity.

In a MNO-led model, the remittance transfer provider should be required to disclose to the customer the amount that will be received at the other end of the transaction prior to the initiation of any transfer of funds.

Market Examples:

- **United States:** The recently passed U.S. "Wall Street Reform and Consumer Protection Act of 2010" is expected, among other things, to provide federal oversight for remittance transfers through the creation of a new "Consumer Financial Protection Bureau." This proposed legislation addresses the issue of currency redenomination of a remittance transfer while in transit through a transfer provider using mobile phones. In this case, the remittance transfer provider must tell the consumer what the value on the receiving end will be in the recipient's country. (The exception to this rule pertains to countries with fixed currency exchange rates.) Remittance transfer providers are required to disclose, prior to initiating a transaction for a consumer, the amount that will be received at the other end, making it possible for consumers to comparison shop. This will address the finding of much research that consumers frequently have difficulty understanding the total cost of sending a remittance—including the exchange rate and fees charged by the provider—before they engage in a transaction. (Appleseed, "The Fair Exchange," April 2009). Currently, U.S. federal regulations that apply to many consumer payments transactions, chiefly under the Electronic Funds Transfer Act (EFTA), generally do not apply to remittance transfers. The Consumer Protection Act of 2010 proposes to provide consumer protection to remittance transfers that is similar to protection found in the EFTA that covers many other consumer payments transactions.[207]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		x				x	x	

Risk-based Policy Matrix – Appendix

7.20. Risk (National Regulators):

"Regulator unreasonably blocks a particular service model."

Description:
The extraordinary success of some cell phone based systems have raised concerns in other countries based on "loss of control" over uncertain risks or resistance to competition with exiting formal financial institutions.

Objective:

- Enable all proven business models within a predictable legal and regulatory environment.

Policy Table:

Options	Implications
1. Limit mobile financial services to bank based models requiring users to pass all transactions over individual bank accounts	• Restricts usage to those who have reason to have a full bank account, effectively excluding the poor. • Little or no developmental impact.
2. Allow both cell phone company and bank based services.	• Opens access to financial services to the poor through low cost payment services that do not require a full bank account – significant developmental impact. • Acts as a catalyst for building confidence in the financial system and in using formal financial services rather than dependence on cash.

Policy Narrative:
If a bank is holding a trust account on behalf of a mobile network operator, then interest is earned from investments made on a joint account held in multiple names and would, in a normal trust situation, be divided equally among all account holders on a periodic basis. Practically speaking, imposing such a mechanism on a mobile phone trust account system would impose a high accounting burden on the service provider and supervisory burden on national regulators monitoring the bank-led portion of the transaction. Nonetheless, the issue of who "owns" the interest earned from investments of trust account holdings is a significant one, and should be addressed from a consumer protection and overall transparency context.

At a minimum, both the service provider and bank should undertake monthly reconciliation of flows into and out of trust accounts. The minimum information to be included in the monthly reconciliation statement shall be the date the reconciliation was undertaken, the date used to reconcile the balances, the name of the bank(s) holding the trust account(s), the name(s) of the account(s), the account number(s), the account balance(s) and date(s), any deposit(s) in transit, and an itemization of the outstanding trust liability showing the amount and source of funds received and not yet disbursed, and other items necessary to reconcile the bank account balance(s) with those of the service provider's accounts. These monthly reconciliations should be retained for a specified period of time, and be subject to banking regulatory review.

Market Examples:

- **General:** The dynamics of the relationship between the account provider and bank acting as fund trustee is somewhat comparable to that found in trust accounts for property management or association management. In this context, brokers who manage real property or community associations may maintain designated rental or assessment trust or escrow accounts separate from their other trust or escrow accounts. The account would be utilized for paying bills on behalf of an owner or an association from any designated rental or assessment escrow or trust account, and there would need to be sufficient funds credited and deposited to the owner's or the association's account to cover such bills. Security deposits would be clearly identified and credited to tenants, and there would always need to be a balance in the account equal to the total of the accumulated security deposits. In such an arrangement, monthly reconciliation of trust accounts is maintained and the trust account is subject to periodic external examination and audit.**Mexico:** In early 2009, Mexico's supervisory Comisión Nacional Bancaria y de Valores (National Banking and Securities Commission or CNBV) began preparing a new e-money regulations which facilitate mobile payments and internet banking by credit institutions. The new regulations will not broaden the non-bank role in regards to e-money issuance. The resolution loosened consent requirements for credit institutions in offering mobile payment, ATM and POS terminal services (such as prepaid cards) and internet banking. Rather than requiring explicit consent by signature, users may consent to additional services with a second form of electronic authentication once they have started the relevant electronic session or, for mobile payment, through call centers. In order for credit institutions to avail themselves of these loosened requirements in regards to mobile payments, they must institute controls to prevent the association of more than one mobile phone line to the account of a user, and of one number of a mobile phone line to several users. The e-money regulation issuance was delayed in part due to concerns as to potential unfair competition concerning the future provision of e-money by mobile network operators, given Telcel's dominant position of the Mexican mobile telephony market, with 85% market share [Notes on Branchless Banking Policy and Regulation in Mexico, CGAP, March 2009]. These concerns may ultimately be the reason why the current regulation did not, in fact, extend mobile payments to non-banks such as MTOs.[208]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x	x	x		x	x	x	

Risk-based Policy Matrix – Appendix

7.21. Risk (National Regulators):

"Interest income on service users' trust funds is improperly allocated to the detriment of service users."

Description:
The trustee will invest the trust funds in interest bearing instruments, such as government securities or interest bearing deposit or savings accounts with financial intermediaries. So the trustee, the account provider or the service users will benefit from this interest.

Objective:
Ensure that the benefit of income generated by the trust funds is most efficiently allocated back to the benefit of service users, based on the account provider's business model.

Policy Table:

Options	Implications
1. Require that interest income be credited back to individual service user's accounts, based on the average amounts in transit during the period.	• Adds an additional level of complexity to the account provider's service by requiring calculation of the interest and crediting back to the service users' individual accounts, adding to the cost of providing the service. • Complicates account reconciliation for service users by adding transactions not originated by service users. • Could encourage service users to leave funds "on deposit" in lieu of opening a formal savings account, reducing the incentive to move savings into the formal financial sector.
2. Allocate some or all of the interest income to the trustee to cover trustee fees for managing the trust account.	• Motivates trustees to provide the trustee services. • Eliminates pass back of trustee fees to the account provider. • Implies monitoring by the account provider to avoid over-charging by the trustee. • May motivate trustee to reach for higher yield, higher risk investments, implying a need for regulatory oversight of investments.
3. Allocate some or all of the interest income to the account provider as additional revenue.	• Augments the revenue stream for the account provider, in principle enabling lower direct service fees to service users. • Benefit will vary with market interest rates.

Policy Narrative:
If a bank is holding a trust account on behalf of a mobile network operator, then interest is earned from investments made on a joint account held in multiple names and would, in a normal trust situation, be divided equally among all account holders on a periodic basis. Practically speaking, imposing such a mechanism on a mobile phone trust account system would impose a high accounting burden on the account provider and supervisory burden on national regulators monitoring the bank-led portion of the transaction. Nonetheless, the issue of who "owns" the interest earned from investments of trust account holdings is a significant one, and should be addressed from a consumer protection and overall transparency context.

At a minimum, both the account provider and bank should undertake monthly reconciliation of flows into and out of trust accounts. The minimum information to be included in the monthly reconciliation statement shall be the date the reconciliation was undertaken, the date used to reconcile the balances, the name of the bank(s) holding the trust account(s), the name(s) of the account(s), the account number(s), the account balance(s) and date(s), any deposit(s) in transit, and an itemization of the outstanding trust liability showing the amount and source of funds received and not yet disbursed, and other items necessary to reconcile the bank account balance(s) with those of the account provider's accounts. These monthly reconciliations should be retained for a specified period of time, and be subject to banking regulatory review.

Market Examples:

- ***Please Note:*** *A market example of a policy action associated with this risk was not identified during the literature review or the in-country consultations included in this project's scope. We welcome your suggestions of relevant examples for inclusion in subsequent versions.*

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
	x	x			x	x		

Risk-based Policy Matrix – Appendix

8.1. Risk (International Regulatory Issues):

"Heightened difficulty tracking and prosecuting illicit cross-border transactions given the new cross border payment capability with a national regulatory framework and enforcement mechanism."

Description:

Illicit financial activities, such as money laundering and the financing of terrorist activities, can be facilitated (and more difficult to prevent) when cross-border transactions are allowed where different regulatory systems are in place. The incompatible regulation can prevent, or make more complicated, identifying suspicious transactions, investigating the transactions, as well as prosecuting and convicting those involved in illicit transactions. This risk applies to any cross border payment system, not just those using mobile financial services.

Objective:

- Regional harmonization of the legal and regulatory framework for mobile financial services.

Policy Table:

Options	Implications
1. Regulatory authority harmonizes mobile financial service definitions in the context of FATF Special Recommendation VII (SRVII) within their own AML/CFT regimes.	• Harmonization with FATF standards facilitates tracking and prosecution. • New requirement imposes a new cost on stakeholders
2. No regulatory action	• Continued, or possibly, increased ability of terrorist and/or criminal elements to leverage mobile payment network and avoid prosecution for illicit cross-border financial crimes. • However, transaction size and volume limits mitigate this risk, particularly versus other payment systems that can handle larger amounts.

Policy Narrative:

In crafting the revised interpretive notes for SR VII, FATF specifically stipulated that it is not the intent of the organization to impose "rigid standards or to mandate a single operating process that would negatively affect the payment system." This is particularly important to note, as the revisions were undertaken, in part, to consider the effects posed by small wire transfers and the continued ability to trace them through the financial system. Given the low thresholds of payments associated with most mobile financial services, harmonization of this FATF standard in AML/CFT regimes may facilitate the future tracking, detection, and prosecution of illicit financial crimes that may be associated with this payment channel.

Market Examples:

- ***Please Note:*** *A market example of a policy action associated with this risk was not identified during the literature review or the in-country consultations included in this project's scope. We welcome your suggestions of relevant examples for inclusion in subsequent versions.*

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
x	x		x		x	x	x	x

Risk-based Policy Matrix – Appendix

8.2. Risk (International Regulatory Issues):

"Small-scale traders face a theft risk due to their 'cash & carry' business."

Description:
Currently, in-country and regional traders conduct a cash and carry business that relies on cash settlement of trade transactions outside of any financial institution, with no audit trails and with theft risk to the traders.

Objective:

- Regional harmonization of the legal and regulatory framework for mobile financial services.

Policy Table:

Options	Implications
1. Regulatory authorities prevent the larger transactions needed for traders or businesses via mobile payments.	• Regulatory authorities limit mobile payment system to small-scale personal transactions, limiting its usefulness for commerce. • Risk of mobile system use for ML/TF is limited by the small scale of transactions. • Traders continue to use cash for commerce and the risk of theft and lack of audit trails persists.
2. Regulatory authorities to allow for a separate user category for traders that allow for larger scale transactions.	• Regulatory authorities enable traders and businesses to use mobile payments through stepped user categories. • Implies higher level of monitoring to contain the risk of mobile system use for ML/TF. • Risk of theft reduced by access to non-cash, mobile channel.
3. Regulatory authorities do not restrict transaction size.	• Regulatory authorities enable traders and businesses to use mobile payments as transaction limits do not restrict their capacity. • Risk of mobile system use for KYC/CDD increases, as large transactions enabled without segregated from general consumer transactions. • Risk of theft reduced by access to non-cash, mobile channel.

Policy Narrative:
One of the key benefits of mobile payments is the reduced risk of theft, as individuals no longer have to carry cash. However, transaction thresholds may limit the ability of traders to use mobile for their transactions, which tend to be larger. For small scale traders who trade across the borders, the issue is exacerbated, as they cannot conduct even small scale transactions from one national network to the other. (Clearly, some workarounds can be used where a national network has coverage in a bordering country, or an individual has accounts on both national networks and acts as the 'go-between', but this does not resolve the eventual need to change currencies.) To facilitate mobile-commerce, rather than simply small-scale person-to-person transactions, regulatory authorities could allow for separate user categories that allow for larger transaction sizes. These users may be subject to more extensive KYC/CDD requirements, and their accounts may be monitored more closely, but this flexibility would enable traders to leverage the technology to facilitate trade. Eventual regional harmonization efforts should be considered that allows for interoperability between national providers and a legal and regulatory framework that can facilitate mobile payment use in trade while mitigating risks associated with cross-border financial transactions.

Market Examples:

- **Ghana, Nigeria, Senegal:** The USAID-funded West Africa Trade Hub Project's Mobile Money Transfer Initiative attempted to leverage the interconnected region, which has approximately $10 billion in cash crossing borders annually. Targeting intraregional traders and remittance senders, the project initially focused on the countries of Ghana, Nigeria, and Senegal and attempted to facilitating cross-border, multi-currency transactions via the mobile phone channel. Among the enabling challenges encountered were regional bank settlements and foreign exchange convertibility and controls. Technology issues included regional payment switch integration, interconnectivity and roaming.[209]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
		x						

Risk-based Policy Matrix – Appendix

8.3. Risk (International Regulatory Issues):

"Cross-border payments through a mobile financial service could be seen as bypassing a country's foreign exchange restrictions."

Description:

Convenience and safety may encourage cross-border traders to tap into a neighboring country's mobile payment system to settle trade payments. If both buyer and seller use the same system, then the funds will remain in the country hosting the buyer's system. The seller will either have to buy goods or services using the e-money from the system host country, or cash out through an exchange office that can use the buyer's currency of origin.

If a foreign exchange conversion facility is built into the service, then transactions that otherwise would be settled in cash move into electronic form.

Objective:

- Enable use of mobile financial services in cross border trade transactions without unreasonable foreign exchange restrictions.

Policy Table:

Options	Implications
1. Regulatory authorities prohibit foreign exchange conversion using mobile financial services.	• Cross border traders limited to using cash or a currency both buyer and seller can use. • May encourage use of a larger neighboring country's currency, as for cash transactions, lowering acceptance of the domestic currency.
2. Regulatory authorities specifically allow foreign exchange conversion using mobile financial services.	• Facilitates monitoring of foreign exchange flows. • Implies development of linkages between neighboring services that enable currency conversion.
3. No Regulatory Action	• Market for mobile financial services across borders may be impeded by lack of clarity on the potential regulatory response.

Policy Narrative:

As noted in 8.2, utilization of mobile financial services for cross border trade transactions can reduce the risk of theft to the trader. Further, encouraging the usage of a mobile network, formalizes what used to be untraceable 'hand-to-hand' cash transactions, allowing regulatory authorities to more easily monitor foreign exchange flows. If regulatory authorities establish a low-risk mechanism for interoperability between national networks, including a foreign exchange conversion, regulators could simultaneously lower the cost of cross-border trade and increase transparency. Prohibition of foreign exchange conversion through mobile will simply force the informal cash transactions to continue, and could potentially lead to other workarounds such as relying on a dominant national network with coverage in both countries, or adoption of the strongest currency for all trade transactions.

Market Examples:

- **Ghana, Nigeria, Senegal:** The USAID-funded West Africa Trade Hub Project's Mobile Money Transfer Initiative attempted to leverage the interconnected region, which has approximately $10 billion in cash crossing borders annually. Targeting intraregional traders and remittance senders, the project initially focused on the countries of Ghana, Nigeria, and Senegal and attempted to facilitating cross-border, multi-currency transactions via the mobile phone channel. Among the enabling challenges encountered were regional bank settlements and foreign exchange convertibility and controls. Technology issues included regional payment switch integration, interconnectivity and roaming.[210]

Risk Type:

International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
x	x	x		x	x	x	x	x

Risk-based Policy Matrix – Appendix

End Notes

[1] http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236930_33658140_1_1_1_1,00.html. Hereafter: FATF 40. Recommendations 5, 6 and 8 and interpretive notes, where applicable.
[2] CGAP. (2008) "Notes on Branchless Banking Policy and Regulation in Brazil," Consultative Group to Assist the Poor, Washington DC.
[Online] http://www.cgap.org/gm/document-1.9.2319/Brazil-Notes-On-Regulation-Branchless-Banking-2008.pdf. pg. 16.
[3] Chatain, Pierre-Laurent. (June 24-26, 2008) "Applying the FATF International standards to Mobile Financial Services." Workshop on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) for Mobile Financial Services (m-FS). Bangkok, Thailand. Hereafter: Chatain.
[4] CGAP. (2008) "Notes on Branchless Banking Policy and Regulation in India," Consultative Group to Assist the Poor, Washington DC.
[Online] http://www.cgap.org/gm/document-1.9.2322/India-Notes-On-Regulation-Branchless-Banking-2008.pdf. pg. 8.
[5] "Update on Regulation of Branchless Banking in South Africa," CGAP, January 2010, pgs. 10-11.
[6] Flaming, Mark, Prochaska, Klaus, and Staschen, Stefan. (June 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in Indonesia," CGAP in cooperation with IFC and GTZ, p. 16.
[7] Aguirre, Ernesto, Dias, Denise, Seltzer, Yanina. (August 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in El Salvador," CGAP, pgs. 8 and 11.
[8] "Update on Regulation of Branchless Banking in Pakistan," CGAP, February 2010, pg. 9.
[9] Bester, Hennie, Chamberlian, Doubell, Koker de, Louis, Hougaard, Christine, Short, Ryan, Smith, Anja, Walker, Richard, G:ENESIS: Implementing FATF Standards in Developing Countries and Financial Inclusion: Findings and Guidelines," Final Report, www.firstinitative.org, February 2008, pg. 39.
[10] Aguirre, Ernesto, Dias, Denise, Seltzer, Yanina. (August 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in El Salvador," CGAP, pg 14.
[11] Mas, Ignacio, Siedek, Hannah, "Banking Through Networks of Retail Agents", CGAP, Focus Notes NO 47, May 2008, pg.4.
[12] "Cloud Based Voice Biometrics E-commerce Platform", 15 June 2010, http://www.infosecurity-magazine.com/view/10223/couldbased-voice-biometrics-ecommerce-platform-introduced/
[13] "Best Practices for Mobile Device Banking Security: International minimum security guidelines for mobile device banking applications," ATMIA, ATM Industry Association, pg. 3.
[14] "Update on Regulation of Branchless Banking in India," CGAP, January 2010, pg.8.
[15] Oliver, Rich, "Synthesizing the mobile ecosystem: Resolving customer problems in mobile payments clearing and settlement models," March 29, 2010. [online} http://portalsandrails.frbatlanta.org/2-1-/03/consumer-confidence-vital-to-mobile-payments-success.html
[16] Rishikko, Juha, Choudhary, Bishwajit, "Mobile Financial Services Business Ecosystem Scenarios & Consequences: Summary Document," Mobey Forum, Mobile Financial Services Ltd., 2006, pgs. 1-8.
[17] Porteous, David, "The Enabling Environment for Mobile Banking in Africa," Report commissioned by Department for International Development (DFID), Bankable Frontier Associates, Boston, MA, May 2006, pg 29.
[18] The Electronic Transactions and Communications Bill, 2009, Section 6 (1) and (2).
[19] [19] "Best Practices for Mobile Device Banking Security: International minimum security guidelines for mobile device banking applications," ATMIA, ATM Industry Association, pg. 3.
[20] USAID interviews, Zambia, February 16-17, 2010.
[21] Aguirre, Ernesto, Dias, Denise, Seltzer, Yanina. (August 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in El Salvador," CGAP, pg 13.
[22] Flaming, Mark, Prochaska, Klaus, and Staschen, Stefan. (June 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in Indonesia," CGAP in cooperation with IFC and GTZ, p. 18.
[23] Porteous, David, "The Enabling Environment for Mobile Banking in Africa," Report commissioned by Department for International Development (DFID), Bankable Frontier Associates, Boston, MA, May 2006, pg 45.
[24] Davidson, Neil, Leishman, Paul, "Building, Incentivizing and Managing a Network of Mobile Money Agents: A Handbook for Mobile Network Operators,"GSMA, Vol. 2, mmu@gsm.org, accessed July 7, 2010, pg. 6-7.
[25] Wishart, Neville. (2006) "Micro-Payment Systems and Their Application to Mobile Networks: Examples of Mobile Enabled Financial Services in the Philippines," The World Bank/*Info*Dev, Washington DC.
[Online] http://www.infodev.org/en/Publication.43.html, pg. 31.
[26] Davidson, Neil, Leishman, Paul, "Building, Incentivizing and Managing a Network of Mobile Money Agents: A Handbook for Mobile Network Operators,"GSMA, Vol. 2, mmu@gsm.org, accessed July 7, 2010, pg. 6-7.
[27] http://www.centralbank.go.ke/downloads.bsd/GUIDELINES520ON%20AGENT20BANKING-CBK%20PG%2015.pdf
[28] Porteous, David, "The Enabling Environment for Mobile Banking in Africa," Report commissioned by Department for International Development (DFID), Bankable Frontier Associates, Boston, MA, May 2006, pgs. 30-31.
[29] Mas, Ignacio, Siedek, Hannah, "Banking Through Networks of Retail Agents", CGAP, Focus Notes NO 47, May 2008, pg. 9.
[30] Davidson, Neil, Leishman, Paul, "Building, Incentivizing and Managing a Network of Mobile Money Agents: A Handbook for Mobile Network Operators,"GSMA, Vol. 3, mmu@gsm.org, accessed July 7, 2010, pg. 2
[31] Davidson, Neil, Leishman, Paul, "Building, Incentivizing and Managing a Network of Mobile Money Agents: A Handbook for Mobile Network Operators,"GSMA, mmu@gsm.org, accessed July 7, 2010, pg. 2-3.
[32] Davidson, Neil, Leishman, Paul, "Managing a Network of Mobile Money Agents,"GSMA, mmu@gsm.org, accessed July 7, 2010, pg. 3-5.
[33] Lynch, Maureen, "Kenya: National Registration Processes Leave Minorities on the Edge of Statelessness," Refugees International, 5/23/2008 [online] http://www.refugeesinternational.org/policy/field-report/kenya-national-registration-processes-leave-minorities-edge-statelessness
[34] Davidson, Neil, Leishman, Paul, "Building, Incentivizing and Managing a Network of Mobile Money Agents: A Handbook for Mobile Network Operators,"GSMA, mmu@gsm.org, accessed July 7, 2010, pg. 5-6.
[35] Davidson, Neil, Leishman, Paul, "Building, Incentivizing and Managing a Network of Mobile Money Agents: A Handbook for Mobile Network Operators,"GSMA, mmu@gsm.org, accessed July 7, 2010, pg. 6.
[36] USAID Street Interviews, February 16-17, 2010, Zambia.
[37] Aguirre, Ernesto, Dias, Denise, Seltzer, Yanina. (August 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in El Salvador," CGAP, pgs. 8 and 11.
[38] "Update on Regulation of Branchless Banking in India," CGAP, January 2010, pg. 10.
[39] Pyler, Megan G., Haas, Sherri, and Nagarajan, Geetha, "Community-Level Economic Effects of M-PESA in Kenya: Initial Findings," IRIS Center, University of Maryland, June 2010 [online]http://www.fassessment.umd.edu/publications/Community%20Effects%Paper%Final.pdf, pgs. 20-21.
[40] http://www.bsp.gov.ph.downloads/Regulations/attachments/2009/c649.pdf, pg. 2-3.
[41] Wishart, Neville, "Micro-Payment Systems and Their Applicatin to Mobile Networks: Examples of Mobile-Enabled Financial Services in the Philippines," IBRD/The World Bank, 2006, pgs, 13-20.
[42] http://www.bsp.gov.ph.downloads/Regulations/attachments/2009/c649.pdf, pg. 2.

Risk-based Policy Matrix – Appendix

[43] Aguirre, Ernesto, Dias, Denise, Seltzer, Yanina. (August 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in El Salvador," CGAP, pg 8.
[44] "Update on Regulation of Branchless Banking in Pakistan," CGAP, February 2010, pg. 4-5.
[45] Flaming, Mark, Prochaska, Klaus, and Staschen, Stefan. (June 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in Indonesia," CGAP in cooperation with IFC and GTZ, p. 19.
[46] "Update on Regulation of Branchless Banking in South Africa," CGAP, January 2010, pg. 5.
[47] Porteous, David, "The Enabling Environment for Mobile Banking in Africa," Report commissioned by Department for International Development (DFID), Bankable Frontier Associates, Boston, MA, May 2006, pg 46.
[48] DIRECTIVE 2000/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 September2000, Articles 1, Section 5b and 4, Sections 2 and 3.
[49] Abbassi, Ala'a, Mohammed Khaled, Klaus Prochaska, and Michael Tarazi. (2009) "Access to Finance: Microcredit and Branchless Banking in The Hashemite Kingdom of Jordan," CGAP, Washington, DC.
[Online] http://www.cgap.org/gm/document-1.1.1304/Jordan_Diagnostic_Report_2009.pdf, p. 17.
[50] Hernandez-Coss, Raul, Egwauagu, Chinyere, Isern, Jennifer, Porteuous, David, "AML/CFT Regulation: Implications for Financial Service ProviderAccount Providers that Serve Low-Income People," IBRD/The World Bank, 2005, pgs. 9-18.
[5151] http://www.bsp.gov.ph.downloads/Regulations/attachments/2009/c649.pdf, pg. 2.
[52] Flaming, Mark, Prochaska, Klaus, and Staschen, Stefan. (June 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in Indonesia," CGAP in cooperation with IFC and GTZ, p. 12.
[53] http://www.bsp.gov.ph.downloads/Regulations/attachments/2009/c649.pdf, pg. 4.
[54] Abbassi, Ala'a, Mohammed Khaled, Klaus Prochaska, and Michael Tarazi. (2009) "Access to Finance: Microcredit and Branchless Banking in The Hashemite Kingdom of Jordan," CGAP, Washington, DC.
[Online] http://www.cgap.org/gm/document-1.1.1304/Jordan_Diagnostic_Report_2009.pdf, p. 17.
[55] http://www.safaricom.co.ke/fileadmin/template/main/downloads/m-pesa_resource_centre/mkesho_FAQs/M-KESHO%20FAQS.pdf
[56] http://www.wolfsberg-principles.com/faq-ownership.html
[57] USAID interview, Tanzania, February 19, 2010.
[58] http://www.reuters.com/article/idUSMAN3795092009091O
[59] http://www.gsmworld.com/newsroom/press-releases/2041.htm
[60] FS SERIES #9: ENABLING MOBILE MONEY INTERVENTIONS PRIMER, DIAGNOSTIC CHECKLIST, AND MODEL SCOPES OF WORK, USAID and Financial Sector Knowledge Sharing, April 2010, pg. 20.
[61] Aguirre, Ernesto, Dias, Denise, Seltzer, Yanina. (August 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in El Salvador," CGAP, pgs. 8 and 11.
[62] "Update on Regulation of Branchless Banking in India," CGAP, January 2010, pg. 10.
[63] Pyler, Megan G., Haas, Sherri, and Nagarajan, Geetha, "Community-Level Economic Effects of M-PESA in Kenya: Initial Findings," IRIS Center, University of Maryland, June 2010 [online]http://www.fassessment.umd.edu/publications/Community%20Effects%Paper%Final.pdf, pgs. 20-21.
[64] http://www.interpol.int/pv_obj_cache/pv_obj_id_7DA31F4675F7441C17F0BB94D705DB7DDEF40200/filename/FHT04.pdf
[65] Http://www.centralbank.go.ke/currency/currencylaws.aspx
[66] http://www.interpol.int/pv_obj_cache/pv_obj_id_7DA31F4675F7441C17F0BB94D705DB7DDEF40200/filename/FHT04.pdf
[67] Http://www.centralbank.go.ke/currency/currencylaws.aspx
[6868] FS SERIES #9: ENABLING MOBILE MONEY INTERVENTIONS PRIMER, DIAGNOSTIC CHECKLIST, AND MODEL SCOPES OF WORK, USAID and Financial Sector Knowledge Sharing, April 2010, pg. 33.
[69] USAID interview, Tanzania, February 17, 2010.
[70] Davidson, Neil, Leishman, Paul, "Managing a Network of Mobile Money Agents,"GSMA, mmu@gsm.org, accessed July 7, 2010, pg. 7.
[71] "Update on Regulation of Branchless Banking in Pakistan," CGAP, February 2010, pg. 9.
[72] Bank for International Settlements. (2001) "Customer Due Diligence for Banks," Basel Committee on International Settlements, Basel, Switzerland. [Online] http://www.bis.org/publ/bcbs85.htm, pgs. 3-5.
[73] Flaming, Mark, Prochaska, Klaus, and Staschen, Stefan. (June 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in Indonesia," CGAP in cooperation with IFC and GTZ, p. 13.
[74] http://www.identity.go.ke.
[75] Liu, Alice and Mithika, Michael, "Mobile Banking –The Key to Building Credit History for the Poor? Kenya Case Study: Linking Mobile Banking and Mobile Payment Platforms to Credit Bureaus," USAID, April 2009, pg. 7.
[76] http://www.pma.ps/pdf/anti-money%20laundry%20law%20eng.pdf
[77] "Updated on Regulation of Branchless Banking in South Africa," CGAP, January 2010, pg. 9.
[78] USAID interview, Zambia, February 17, 2010.
[79] FATF 40, Interpretive Notes.
[80] FS SERIES #9: ENABLING MOBILE MONEY INTERVENTIONS PRIMER, DIAGNOSTIC CHECKLIST, AND MODEL SCOPES OF WORK, USAID and Financial Sector Knowledge Sharing, April 2010, pg. 25-27.
[81] CGAP. (2008) "Notes on Branchless Banking Policy and Regulation in India," Consultative Group to Assist the Poor, Washington DC.
[Online] http://www.cgap.org/gm/document-1.9.2322/India-Notes-On-Regulation-Branchless-Banking-2008.pdf. pg. 8.

[82] Kenya: National Registration Processes Leave Minorities on the Edge of Statelessness, Maureen Lynch and Katherine Southwick, ***05/23/2008, http://refugeesinternational.org/policy/field-report/kenya-national-registration-processes-leave-minorities-edge-statelessness.***

[83] M-Pesa interview, Nairobi, Kenya, February 20, 2010.

[84] WP416. 35-36.

[85] FS SERIES #9: ENABLING MOBILE MONEY INTERVENTIONS PRIMER, DIAGNOSTIC CHECKLIST, AND MODEL SCOPES OF WORK, USAID and Financial Sector Knowledge Sharing, April 2010, pg. 24.

[86] See the "Asset Securitization" booklet of the *Comptroller's Handbook* and OCC Bulletin 99-46, "Interagency Guidance on Asset Securitization Activities" (December 16, 2999) and *An Examiner's Guide to Problem Bank Identification, Rehabilitation, and Resolution: A Guide for Examiners.* (OCC, January 2001).

[87] WP416. pgs 43-47.

[88] Chaitain, Pierre-Laurent. (June 24-26, 2008). "Applying the FATF International standards to Mobile Financial Services." Workshop on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) for Mobile Financial Services (m-FS).

[89] AITEC PRESENTATION SESSION, 17TH–25TH, FEBRUARY, 2010, Samuel Mutungi, The Co-Operative Bank of Kenya, Ltd.

[90] "Notes on AML-CFT Compliance: Challenges with Branchless Banking and Examples of Industry and Regulatory Responses." http://www.cgap.org/technology. (2007). pg. 3.

[91] Forbes, John (19 April 2007). "The Convergence of Telecom and Financial Services and its Effects on AML/Wire Remittance Operations." United States Treasury, Office of Technical Assistance. Presentation.

[92] Forbes, John (March 2007) "Effects of Cell phones on Anti-Money Laundering/Combating Financial Terrorism (AML/CFT)Wire Remittance Operations." ADB Working Paper, pg. 43.

[93] Chatain.

[94] WP416. pgs 38.

[95] Flaming, Mark, Prochaska, Klaus, and Staschen, Stefan. (June 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in Indonesia," CGAP in cooperation with IFC and GTZ, p. 16.

[96] Khan, Zain, "Developing ICT Capacities," AITEC Banking & Mobile Money COMESA, February 25, 2010, Nairobi, Kenya.

[97] CGAP. (2008) "Notes on Branchless Banking Policy and Regulation in Brazil," CGAP, Washington DC. [Online] http://www.cgap.org/gm/document-1.9.2319/Brazil-Notes-On-Regulation-Branchless-Banking-2008.pdf. pg. 9

[98] Aguirre, Ernesto, Dias, Denise, Seltzer, Yanina. (August 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in El Salvador," CGAP, pg 12.

[99] "Update on the Regulation of Branchless Banking in South Africa," CGAP, January 2010, pgs 3-4.

[100] Aguirre, Ernesto, Dias, Denise, Seltzer, Yanina. (August 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in El Salvador," CGAP, pgs. 8 and 11.

[101] "Update on Regulation of Branchless Banking in India," CGAP, January 2010, pg. 10.

[102] Pyler, Megan G., Haas, Sherri, and Nagarajan, Geetha, "Community-Level Economic Effects of M-PESA in Kenya: Initial Findings," IRIS Center, University of Maryland, June 2010 [online]http://www.fassessment.umd.edu/publications/Community%20Effects%Paper%Final.pdf, pgs. 20-21.

[103] http://www.fatf-gafi.org/document/9/0,3343,en_32250379_32236920_34032073_1_1_1_1,00.html. Hereafter: Special Recommendations. Special Recommendation VI.

[104] FATF 40. Recommendation 23.

[105] Special Recommendations VI.

[106] WP416. pgs 43-47.

[107] CGAP. (2007) "Notes on Branchless Banking Policy and Regulation in Kenya," Consultative Group to Assist the Poor, Washington DC.
[Online] http://www.cgap.org/gm/document-1.9.2321/Kenya-Notes-On-Regulation-Branchless-Banking-2007.pdf. pg 7.

[108] Lyman, Timothy R., Gautman Ivatury, and Stefan Staschen. (2006) "Use of Agents in Branchless Banking for the Poor: Rewards, Risks and Regulation." CGAP Focus Note 38. pg. 10-11.

[109] Chatain, Pierre-Laurent, et al. "Integrity in Mobile Phone Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing." World Bank, Washington, DC
[Online] http://siteresources.worldbank.org/INTAML/Resources/WP146_Web.pdf. pg. 51.

[110] CGAP. (2008) "Notes on Branchless Banking Policy and Regulation in Brazil," Consultative Group to Assist the Poor, Washington DC.
[Online] http://www.cgap.org/gm/document-1.9.2319/Brazil-Notes-On-Regulation-Branchless-Banking-2008.pdf. Pgs. 7-8.

[111] CGAP. (2008) "Notes on Branchless Banking Policy and Regulation in India," Consultative Group to Assist the Poor, Washington DC.
[Online] http://www.cgap.org/gm/document-1.9.2322/India-Notes-On-Regulation-Branchless-Banking-2008.pdf. pgs. 7-8.

[112] See the "Asset Securitization" booklet of the *Comptroller's Handbook* and OCC Bulletin 99-46, "Interagency Guidance on Asset Securitization Activities" (December 16, 2999) and *An Examiner's Guide to Problem Bank Identification, Rehabilitation, and Resolution: A Guide for Examiners.* (OCC, January 2001).

[113] See *General Guide to Account Opening and Customer Identification,* Attachment to Basel Committee publication No. 85 "Customer due diligence for banks", February 2003. (http://www.bis.org/publ/bcbs85annex.htm).

[114] See Ignacio Mas and Daniel Radcliffe Mobile Payments Go Viral: The Story of M-PESA and Ignacio Mas and Amolo Ng'weno Three Keys to M-PESA's Success: Branding, Channel Management, and Pricing.

[115] Report on the Technical Committee on Electronic Banking, Central Bank of Nigeria, February 2003, pg. 22.

[116] http://www.ifir1000.com/legislationguide/192/the-e-zwich-electronic-clearing-and-payment-system.html

[117] E-Zwich Becoming a Colossal Waste of Resources? http://allafrica.com/stories/201002091058.html

[118] CGAP. (2009) "Notes on Branchless Banking Policy and Regulation in Mexico," Consultative Group to Assist the Poor, Washington DC.

[Online] http://www.cgap.org/gm/document-1.1.1306/Mexico%20Branchless%20Banking%20Notes.pdf.
[119] Vodafone (2007) "The Transformational Potential of m-Transactions," *Policy Paper Series, No. 6*, Vodaphone, London
[Online] http://www.gsmworld.com/documents/VOD833_Policy_Paper_Series_FINAL.pdf.
[120] Economist Intelligence Unit. (2009) "Kenya Telecoms: Banking on M-Banking." *Industry Briefing*.
[121] http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236930_33658140_1_1_1_1,00.html. Hereafter: FATF 40. Recommendations 5, 6 and 8 and interpretive notes, where applicable.
[122] Basel Committee on Banking Supervision. (October 2001) "Customer Due Diligence for Banks." Bank for International Settlements. Pgs. 2. Hereafter: Basel.
[123] FATF 40, Interpretive Notes.
[124] FATF 40, Interpretive Notes.

[125] Kenya: National Registration Processes Leave Minorities on the Edge of Statelessness, Maureen Lynch and Katherine Southwick, ***05/23/2008, http://refugeesinternational.org/policy/field-report/kenya-national-registration-processes-leave-minorities-edge-statelessness.***
[126] M-Pesa interview, Nairobi, Kenya, February 20, 2010.
[127] Hernandez-Coss, Raul, and Chinyere Egwuagu, Jennifer Isern, and David Porteous (2005) "AML/CFT Regulation: Implications for Financial Account Providers that Serve Low-income People." World Bank and CGAP. Pg. 17.
[128] Chatain, Pierre-Laurent, et al. "Integrity in Mobile Phone Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing." World Bank, Washington, DC
[Online] http://siteresources.worldbank.org/INTAML/Resources/WP146_Web.pdf. pg. 22-27. Hereafer WP416.
[129] WP416. 35-36.
[130] CGAP. (2008) "Notes on Branchless Banking Policy and Regulation in India," Consultative Group to Assist the Poor, Washington DC.
[Online] http://www.cgap.org/gm/document-1.9.2322/India-Notes-On-Regulation-Branchless-Banking-2008.pdf. pg. 8.
[131] WP416 pg. 27.
[132] CGAP. (2009) "Notes on Branchless Banking Policy and Regulation in Mexico," Consultative Group to Assist the Poor, Washington DC.
[Online] http://www.cgap.org/gm/document-1.1.1306/Mexico%20Branchless%20Banking%20Notes.pdf.
[133] Abbassi, Ala'a, et. al. (March 16, 2009) "Access to Finance: Microcredit and Branchless Banking in the Hashemite Kingdom of Jordan." Pgs. 32-33.
[134] http://www.egmontgroup.org/about/what-is-an-fiu
[135] Including terrorist acts or organizations.
[136] Special Recommendations IV.
[137] Hereafter: FATF 40. Recommendations 25 and 26.
[138]WP416 pg. 13.
[139] USAID Field Visits, Zambia, Kenya, February 9-28, 2010.
[140] Estioko, Raymond. (June 24-26, 2008). "Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) for Mobile Financial Services (m-FS): The Philippine Experience." Bangkok, Thailand.
[141] Forbes, John (March 2007) "Effects of Cell phones on Anti-Money Laundering/Combating Financial Terrorism (AML/CFT)Wire Remittance Operations." ADB Working Paper, pg. 26. Hereafter: Effects.
[142]WP416. pgs. 50-51.
[143] Korean Financial Intelligence Unit, Financial Services Commission (June 24-26, 2008) , "Countering the Use of Mobile-FS in the Money Laundering." Workshop on AML/CFT, Bangkok, Thailand.
[144] WP416. pgs. 13-14.
[145] Aguirre, Ernesto, Dias, Denise, Seltzer, Yanina. (August 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in El Salvador," CGAP, pgs. 8 and 11.
[146] http://www.fatf-gafi.org/document/9/0,3343,en_32250379_32236920_34032073_1_1_1_1,00.html. Hereafter: Special Recommendations. Special Recommendation VI.
[147] FATF 40. Recommendation 23.
[148] Special Recommendations VI.
[149] WP416. pgs 43-47.
[150] CGAP. (2007) "Notes on Branchless Banking Policy and Regulation in Kenya," Consultative Group to Assist the Poor, Washington DC.
[Online] http://www.cgap.org/gm/document-1.9.2321/Kenya-Notes-On-Regulation-Branchless-Banking-2007.pdf. pg 7.
[151] Lyman, Timothy R., Gautman Ivatury, and Stefan Staschen. (2006) "Use of Agents in Branchless Banking for the Poor: Rewards, Risks and Regulation." CGAP Focus Note 38. pg. 10-11.
[152] Chatain, Pierre-Laurent, et al. "Integrity in Mobile Phone Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing." World Bank, Washington, DC
[Online] http://siteresources.worldbank.org/INTAML/Resources/WP146_Web.pdf. pg. 51.
[153] CGAP. (2008) "Notes on Branchless Banking Policy and Regulation in Brazil," Consultative Group to Assist the Poor, Washington DC.
[Online] http://www.cgap.org/gm/document-1.9.2319/Brazil-Notes-On-Regulation-Branchless-Banking-2008.pdf. Pgs. 7-8.

[154] CGAP. (2008) "Notes on Branchless Banking Policy and Regulation in India," Consultative Group to Assist the Poor, Washington DC.
[Online] http://www.cgap.org/gm/document-1.9.2322/India-Notes-On-Regulation-Branchless-Banking-2008.pdf. pgs. 7-8.
[155] Also, see Special Recommendations VI and VII.
[156] FATF 40. Recommendation 10.
[157] WP416. pgs 43-47.
[158] Chaitain, Pierre-Laurent. (June 24-26, 2008). "Applying the FATF International standards to Mobile Financial Services." Workshop on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) for Mobile Financial Services (m-FS).
[159] AITEC PRESENTATION SESSION, 17TH–25TH, FEBRUARY, 2010, Samuel Mutungi, The Co-Operative Bank of Kenya, Ltd.
[160] "Notes on AML-CFT Compliance: Challenges with Branchless Banking and Examples of Industry and Regulatory Responses." http://www.cgap.org/technology. (2007). pg. 3.
[161] Forbes, John (19 April 2007). "The Convergence of Telecom and Financial Services and its Effects on AML/Wire Remittance Operations." United States Treasury, Office of Technical Assistance. Presentation.
[162] Forbes, John (March 2007) "Effects of Cell phones on Anti-Money Laundering/Combating Financial Terrorism (AML/CFT)Wire Remittance Operations." ADB Working Paper, pg. 43.
[163] Chatain.
[164] WP416. pgs 38.
[165] http://www.fiumalawi.gov.mw/fiu2/index.php?option=com_content&view=article&id=19&itemid=27
[166] http://www.fiumalawi.gov.mw/fiu2/documents/money_laundering_act.pdf
[167] "Update of Regulation of Branchless Banking in India," CGAP, January 2010, pgs. 6-7.
[168] http://fiuindia.gov.in/about-overview.htm
[169] CGAP. (2008) "Notes on Branchless Banking Policy and Regulation in Pakistan," CGAP, Washington DC. [Online] http://www.cgap.org/gm/document-1.9.2304/PKNotes_RegulationBranchless_2007.pdf, pgs 1-3.
[170] "Update on Regulation of Branchless Banking in Pakistan," CGAP, February 2010, pg. 10.
[171] http://www.amlc.gov.ph/amla.html
[172] http://www.amlc.gov.ph/archive/reso361.pdf
[173] Aguirre, Ernesto, Dias, Denise, Seltzer, Yanina. (August 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in El Salvador," CGAP, pg 13.
[174] "Update on Regulation of Branchless Banking in Pakistan," CGAP, February 2010, pg. 9.
[175] Basel Pgs. 7-11.
[176] Isern, Jennifer, and Louis de Koker. (August 2009) "AML/CFT: Strengthening Financial Inclusion and Integrity." *Focus Note 56*. CGAP, Washington, D.C. [Online], pg. 1-2.
[177] CGAP. (2008) "Notes on Branchless Banking Policy and Regulation in South Africa," Consultative Group to Assist the Poor, Washington DC.
[Online] http://www.cgap.org/gm/document-1.9.2320/SouthAfrica-Notes-On-Regulation-Branchless-Banking-2008.pdf. pg. 1-3.
[178] Genesis, Implementing FATF standards in developing countries and financial inclusion: Findings and guidelines Final report May 2008, 74-90.
[179] "Updated on Regulation of Branchless Banking in India," CGAP, January 2010, pgs 8-9.
[180] Flaming, Mark, Prochaska, Klaus, and Staschen, Stefan. (June 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in Indonesia," CGAP in cooperation with IFC and GTZ, p. 8.
[181] Khan, Zain, "Developing ICT Capacities," AITEC Banking & Mobile Money COMESA, February 25, 2010, Nairobi, Kenya.
[182] CGAP. (2008) "Notes on Branchless Banking Policy and Regulation in Brazil," CGAP, Washington DC. [Online] http://www.cgap.org/gm/document-1.9.2319/Brazil-Notes-On-Regulation-Branchless-Banking-2008.pdf. pg. 9
[183] Aguirre, Ernesto, Dias, Denise, Seltzer, Yanina. (August 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in El Salvador," CGAP, pg 12.
[184] "Update on the Regulation of Branchless Banking in South Africa," CGAP, January 2010, pgs 3-4.
[185] Flaming, Mark, Prochaska, Klaus, and Staschen, Stefan. (June 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in Indonesia," CGAP in cooperation with IFC and GTZ, p. 9.
[186] Porteous, David, "The Enabling Environment for Mobile Banking in Africa," Report commissioned by Department for International Development (DFID), Bankable Frontier Associates, Boston, MA, May 2006, pgs. 22-23 and USAID Interview for the Mobile Financial Services Risk Matrix, February 2010, Tanzania.
[187] Barbier, Eric, "TransferTo," MMT09 Conference and Expo, JW Marriot, Dubai, 26-27 October 09.
[188] http://technology.cgap.org/2010/05/18/m-pesa-meets-microsavings-with-equity-bank-deal-in-kenya/.
[189] Aguirre, Ernesto, Dias, Denise, Seltzer, Yanina. (August 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in El Salvador," CGAP, pg 8.
[190] "Update on Regulation of Branchless Banking in Pakistan," CGAP, February 2010, pg. 4-5.
[191] Flaming, Mark, Prochaska, Klaus, and Staschen, Stefan. (June 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in Indonesia," CGAP in cooperation with IFC and GTZ, p. 19.
[192] FS SERIES #9: ENABLING MOBILE MONEY INTERVENTIONS PRIMER, DIAGNOSTIC CHECKLIST, AND MODEL SCOPES OF WORK, USAID and Financial Sector Knowledge Sharing, April 2010, pg. 16.
[193] "Update on Regulation of Branchless Banking in South Africa," CGAP, January 2010, pg. 5.
[194] Porteous, David, "The Enabling Environment for Mobile Banking in Africa," Report commissioned by Department for International Development (DFID), Bankable Frontier Associates, Boston, MA, May 2006, pg 46.
[195] http://www.sec.gov/litigation/complaints/2008/comp-madoff121108.pdf

Risk-based Policy Matrix – Appendix

[196] http://ringofquality.choseit.com/revealeddeci-has-no-account/
[197] http://www.bot-tx.org/Adverts/PressRelease/2009-Apr%2003-Press%20Release.pdf.
[198] Anti-Money Laundering Act, 2010, State Bank of Pakistan, http://www.sbp.org.pk/about/act/Anti-Act-2010.pdf, [online] pg. 107.
[199] "Implications of 9/11 for the Financial Services Sector," Remarks by Vice Chairman Roger W. Ferguson, Jr. At the Conference on Bank Structure and Competition, Chicago, Illinois May 9, 2002, http://www.federalreserve.gov/boarddocs/speeches/2002/20020509/default.htm
[200] AITEC PRESENTATION SESSION, 17TH–25TH, FEBRUARY, 2010, Samuel Mutungi, The Co-Operative Bank of Kenya, Ltd.
[201] For a useful template, see the U.S, Comptroller of the Currency, Administrator of National Banks "An Examiner's Guide to Problem Bank Identification, Rehabilitation, and Resolution: A Guide for Examiners." (OCC, January 2001).
[202] http://www.interpol.int/pv_obj_cache/pv_obj_id_7DA31F4675F7441C17F0BB94D705DB7DDEF40200/filename/FHT04.pdf
[203] Http://www.centralbank.go.ke/currency/currencylaws.aspx
[204] http://www.interpol.int/pv_obj_cache/pv_obj_id_7DA31F4675F7441C17F0BB94D705DB7DDEF40200/filename/FHT04.pdf
[205] Http://www.centralbank.go.ke/currency/currencylaws.aspx
[206] U.S. Office of the Comptroller of the Currency provides sound guidance that could relate to mobile banking agent networks in relation to currency redenomination of funds while in transit (see http://www.occ.treas.gov/ftp/bulletin/96-48.txt).
[207] See http://www.financialstability.gov/roadtostability/regulatoryreformhtml.
[208] E-Money Regulation in Mexico, April 8, 2010 [online] http://www.mobilemoneyexchange.org/Feeds/Research/Read/e-money-regulation-in-mexico.aspx
[209] FS SERIES #9: ENABLING MOBILE MONEY INTERVENTIONS PRIMER, DIAGNOSTIC CHECKLIST, AND MODEL SCOPES OF WORK, USAID and Financial Sector Knowledge Sharing, April 2010, pg. 5.
[210] FS SERIES #9: ENABLING MOBILE MONEY INTERVENTIONS PRIMER, DIAGNOSTIC CHECKLIST, AND MODEL SCOPES OF WORK, USAID and Financial Sector Knowledge Sharing, April 2010, pg. 5.

Annotated Bibliography

Country Specific Reports

Abbassi, Ala'a, Mohammed Khaled, Klaus Prochaska, and Michael Tarazi. (2009) "Access to Finance: Microcredit and Branchless Banking in The Hashemite Kingdom of Jordan," CGAP, Washington, DC. [Online] http://www.cgap.org/gm/document-1.1.1304/Jordan_Diagnostic_Report_2009.pdf

> This CGAP country diagnostic focuses on the policy and regulatory environment for microcredit and branchless banking in Jordan. Jordanian MFIs offer only small loans and some minor business development services to entrepreneurs and are not involved in payment transfers. While Jordan has one of the highest market coverage rates in the region, there is a significant gap between the supply of microfinance and potential demand in the market. The same can be said of branchless banking, which is still a relatively new concept in Jordan and the Central Bank remains hesitant to authorize the use of non-bank led branchless banking models.

Berger, Estelle. (2009) "Expanding Outreach in Malawi: OIBM's Efforts to Launch a Mobile Banking Program," The SEEP Network and Opportunity International, Washington, DC. [Online] http://www.seepnetwork.org/Resources/M-banking_Case.pdf

> This case study presents the efforts, still in progress, of Opportunity International Bank of Malawi (OIBM) to develop its own m-banking program. The country had no telco-led programs when this project began in 2008. As a result, OIBM had to construct a bank-led model in order to offer Malawi's poor people the benefits of access to financial services through m-banking. At the time of writing, OIBM's program was near launch, but not yet in operation. This study documents some of the challenges faced and solutions developed prior to implementation.*

Bruynse, Dirk and Jeremiah Grossman. (2008) "Mobile Money Study: Palestine," IRIS Center, University of Maryland.[Online]http://www.microlinks.org/file_download.php/FIELD_Report_No_6_Mobile_Money_Study_in_WBG.pdf?URL_ID=29737&filename=12283246521FIELD_Report_No_6_Mobile_Money_Study_in_WBG.pdf&filetype=application%2Fpdf&filesize=1217392&name=FIELD_Report_No_6_Mobile_Money_Study_in_WBG.pdf&location=user-S/

> Branchless banking in Palestine is still in the early stages of development. Services in Palestine are limited to customers performing debit/credit transactions on POS devices and accessing certain account information via SMS, but it does not allow the customer to transfer funds to another individual or pay bills on the phone. Currently, there are no regulations defining e-money or providing guidelines on the types of providers who can issue e-money. However, the Palestinian Monetary Authority does not intend to permit non-banks to issue e-money. The authors argue that branchless banking would particularly benefit Palestine because of the restrictions on the movement of people, goods, services, and cash.

CGAP. (2009) "Notes on Branchless Banking Policy and Regulation in Mexico," CGAP, Washington DC. [Online] http://www.cgap.org/gm/document-1.1.1306/Mexico%20Branchless%20Banking%20Notes.pdf.

> This CGAP country note is the latest in a series of country diagnostics that review mobile banking models in various countries. Of importance to highlight from this study is that non-banks in Mexico are currently not allowed to issue e-money, but preparations to create e-money regulation are underway. Further issues affecting branchless banking and financial access are: lack of a national identification document, a new tax on cash deposits, low competition in banking and payments services, and weak enforcement of rules against digital crimes.

CGAP. (2008) "Notes on Branchless Banking Policy and Regulation in Brazil," CGAP, Washington DC. [Online] http://www.cgap.org/gm/document-1.9.2319/Brazil-Notes-On-Regulation-Branchless-Banking-2008.pdf.

> This CGAP country note focuses on the potential for non-bank-based branchless banking in Brazil given the country's long history of banks using agents. However, like in Mexico, some obstacles are that non-banks are not permitted to issue e-money and mobile network operators and other non-bank e-money and prepaid card issuers are not covered by the AML/CFT law.

CGAP. (2008) "Notes on Branchless Banking Policy and Regulation in India," CGAP, Washington DC. [Online] http://www.cgap.org/gm/document-1.9.2322/India-Notes-On-Regulation-Branchless-Banking-2008.pdf.

> This CGAP country note asserts that the potential for payment and m-banking services to be provided by mobile network operators and other non-banks has not yet been realized in India due to restrictions on non-banks from accepting funds from the public and the prohibition on any e-money issuance by non-banks. There have been indications, however, that change is on the horizon. In 2007, the Reserve Bank of India issued two reports showing its willingness to consider the possible use of mobile phones and prepaid cards for banking purposes. (see "country specific regulations" section)

CGAP. (2008) "Notes on Branchless Banking Policy and Regulation in Pakistan," CGAP, Washington DC. [Online] http://www.cgap.org/gm/document-1.9.2304/PKNotes_RegulationBranchless_2007.pdf.

> Pakistan was selected as the pilot for the CGAP country diagnostic series because regulators and policymakers are keenly interested in branchless banking and several private operators (banks and

* Summary taken from abstract

Annotated Bibliography

mobile network operators) are exploring various business models. However, to date, only banks are allowed to accept deposits withdrawable by check from the public and current AML/CFT laws do not cover non-banks.

CGAP. (2008) "Notes on Branchless Banking Policy and Regulation in South Africa," CGAP, Washington DC. [Online] http://www.cgap.org/gm/document-1.9.2320/SouthAfrica-Notes-On-Regulation-Branchless-Banking-2008.pdf.

South Africa has a variety of successful branchless banking models – from mobile banking to Non-bank payment services, despite regulations which limit electronic money issuance to banks only. By easing the documentation requirements for opening an account while capping transaction limits on such accounts, South Africa has became a model for addressing financial security concerns while allowing the poor to have greater access to financial services. The authors believe that pending telecommunications regulations threaten to limit South Africa's branchless banking potential.

CGAP. (2007) "Notes on Branchless Banking Policy and Regulation in Kenya," CGAP, Washington DC. [Online] http://www.cgap.org/gm/document-1.9.2321/Kenya-Notes-On-Regulation-Branchless-Banking-2007.pdf.

Branchless banking in Kenya is dominated by mobile operator, Safaricom's M-PESA service. The non-bank-based model appears to be free of any financial regulation as long as services provided are not deemed to fall within the definition of banking business under the Banking Act. The general lack of regulatory guidance and oversight is problematic because it may lead to increased risk to customers and the financial sector. The authors believe that these concerns could be addressed by requiring reporting regulations, minimum capital and liquidity requirements, and restrictions on how e-money proceeds may be held.

Economist Intelligence Unit. (2007) "South Africa: From Mattress to Mobile Banking." *Industry Briefing*. [Online] http://globaltechforum.eiu.com/index.asp?layout=rich_story&doc_id=11066&title=South+Africa%3A+From+mattress+to+mobile+banking&categoryid=31&channelid=4

This article explores some of the reasons behind the success of Wizzit in South Africa, particularly among the poor. Wizzit charges lower fees than many retail banks in South Africa, making it easy for the poor to access credit. Opening an account with Wizzit is also very simple, as agents are sent to the applicant's home or workplace. To transfer money, Wizzit uses the South African inter-bank clearing house system. This feature gives Wizzit account-holders the ability to transact with any mobile user regardless of the identity of their network operator or their bank.

Flaming, Mark, Klaus Prochaska, and Stefan Staschen. (2009) "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in Indonesia," CGAP, in cooperation with IFC and GTZ. [Online] http://www.cgap.org/gm/document-1.9.34817/Branchless%20Banking%20Diagnostic%20in%20Indonesia.pdf

Indonesia does not have any outstanding examples of bank or non-bank providers successfully providing financial services to low-income customers through branchless banking. The Bank of Indonesia has recently issued regulations on e-money, including limits on the use of e-money to making retail payments. Neither banks nor non-banks are allowed to use agents to provide financial services, posing a significant barrier to branchless banking.

Hughes, Nick and Susie Lonie. (2007)"M-PESA: Mobile Money for the "Unbanked" Turning Cellphones into 24-Hour Tellers in Kenya." *Innovations: Technology, Governance, Globalization*. [Online] http://www.policyinnovations.org/ideas/policy_library/data/m_pesa/_res/id=sa_File1/INNOV0201_pp-63-81_hughes-lonie_1.pdf

Written by a Vodafone executive who started M-PESA, Nick Hughes, this paper explores the company's commitment to the Millennium Development goals and the steps Hughes took to convince senior executives about his idea for M-PESA. The second section of the paper is written by Susie Lonie, an m-commerce expert who was brought into Kenya to manage the overall delivery of M-PESA from pilot into commercial operation. She describes the day-to-day obstacles she faced while managing this process.

Isern, Jennifer, et al. (2009) "Access to Finance in Nigeria: Microfinance, Branchless Banking and SME Finance," CGAP, Washington DC. [Online] http://www.cgap.org/gm/document-1.1.1706/Access_to_finance_in_Nigeria_25_feb_09.pdf

This paper provides a high level description of the supply of microfinance services, branchless banking , and SME finance in Nigeria. Five over-arching issues are covered in all of the areas: the need for transparency of financial performance and market information; the need for capacity within the Central Bank of Nigeria to supervise financial service provision; the need to ensure that the payment system, private credit registries and collateral registries are upgraded; the need to promote consumer protection; and the need to continue coordinating efforts between funders, the federal government and state governments.

Ivatury, Gautam and Mark Pickens. (2006) "Mobile-Phone Banking and Low-Income Customers - Evidence from South Africa," supported by CGAP, UN Foundation and Vodafone Group Foundation. [Online] http://www.globalproblems-globalsolutions-files.org/unf_website/PDF/mobile_phone_bank_low_income_customers.pdf

Annotated Bibliography

This paper presents findings on how low-income people in South Africa view Wizzit. Wizzit's low income customers give m-banking high marks for its convenience, accessibility, and affordability. The study found that while the poor do use Wizzit, they are not among South Africa's poorest people, who still remain unbanked. Part one of this paper introduces Wizzit; part two details findings from the survey in South Africa; and part three puts this research into a broader context to assist banks, mobile network operators, and other parties interested in extending financial services to low-income people.

Kumar, Anjali, et al. (2006) "Expanding Bank Outreach through Retail Partnerships: Correspondent Banking in Brazil." *World Bank Working Paper, No. 85*.
[Online]
http://siteresources.worldbank.org/INTTOPCONF3/Resources/363980Retail0p101OFFICIAL0USE0ONLY1.pdf

This paper explores the extent to which formal, regulated financial institutions such as banks have been able to partner with "correspondents," using the case of Brazil, where banks have recently developed extensive networks of such correspondents. It shows that such arrangements result in lower costs and shared risks for participating financial institutions. The example from Brazil may be replicable elsewhere if appropriate regulatory adjustments are undertaken.*

Liu, Alice and Michael Mithika. (2009) "Mobile Banking – The Key to Building Credit History for the Poor? Kenya Case Study: Linking Mobile Banking and Mobile Payment Platforms to Credit Bureaus," Prepared by DAI for USAID. [Online] http://fletchermbanking.com/Kenya_PACT-Final%20Report-5-19-09.pdf.

The hypothesis of this study is that mobile transaction data may potentially help Kenyans establish a formal credit history, help lenders more accurately evaluate credit risk, and lead to increased access to financial services for the poor. However, current telecom regulations prohibit the disclosure of statement and account data, including m-payment data that credit bureaus would be interested in using. The author's main conclusion is that there is potential for MNO data to be used to support a credit information system, but current telecom regulations are preventing this.

Mendes, Shawn, Erwin Alampay, Edwin Soriano and Cheryll Soriano. (2007) "The Innovative Use of Mobile Applications in the Philippines—Lessons for Africa," Swedish International Development Agency.
[Online] http://siteresources.worldbank.org/EXTEDEVELOPMENT/Resources/20071129-Mobiles_PH_Lessons_for_Africa.pdf?resourceurlname=20071129-Mobiles_PH_Lessons_for_Africa.pdf.

The article discusses the factors that led to the rapid growth of mobile banking in the Philippines, including favorable telecommunications policies and the widespread use of mobile phones and SMS. A precursor to m-Commerce in the Philippines was Pasaload, or the capability of individuals to transfer between users load. The authors also discuss the pros and cons of G-Cash and Smart Money, and conclude the article with a discussion of how market conditions in Africa are similar to those in the Philippines prior to the growth of mobile banking.

Mjojo, Angela. (2008) "Financial Inclusion Through Micro-finance Services Provision and Information Communications Technology (ICT) Pertinent Issues for Malawi," *MIT Working Paper* (website not available)

This working paper explores the possibility of employing ICT, specifically in the form of cell phone services, in micro-financial services provision to aid in the financial inclusion process. Using Malawi as an example, the paper highlights the high demand that exists for microfinance services, defines the challenges that are encountered in micro financial services provision such as high transactions costs; and proposes that mobile phone financial services (m-FS) in Malawi may be one possible low cost solution that can be pursued in order to attain financial inclusion. The paper does however point out the risks that are likely to be encountered in m-FS, and the possible mitigation measures that exist to counter these risks. The paper concludes with recommendations for the stakeholders that would need to be involved in this process.*

Morawczynski, Olga and Mark Pickens. (2009) "Poor People Using Mobile Financial Services: Observations on Customer Usage and Impact from M-PESA," *CGAP Brief,* Washington DC.
[Online] http://www.cgap.org/gm/document-1.9.36723/MPESA_Brief.pdf

This CGAP brief draws on some of the first ethnographic research on M-PESA and offers insights into how poor people use M-PESA and its impact on their lives. One noteworthy finding of the research is that poor customers are increasingly using M-PESA as a savings account, which reveals a latent demand for appropriate savings products. This is an important opportunity for Safaricom as it looks to broaden its services.

Morawczynski, Olga. (2008) "Surviving the Dual System: How M-PESA is Fostering Urban-to-Rural Remittances in a Kenyan Slum," University of Edinburgh, UK.
[Online] http://www.gsmworld.com/documents/Olga_Morawczynski-M-PESA-2008.pdf.

The 'dual system' thesis has been used to describe the continuing commitment of urban migrants to the village in various African countries. According to literature, urban workers maintain strong ties with the rural area, even after spending a substantial amount of time in the city. This study uses ethnographic data collected in a Kenyan slum to show that MPESA is becoming a tool for the maintenance of urban-rural relations. It further asserts that because it is helping migrants to maintain such relations, it is facilitating survival in the 'dual system'.*

Annotated Bibliography

State Bank of Pakistan. (2007) "Draft Policy Paper on Regulatory Framework for Mobile Banking in Pakistan," Banking Policy & Regulations Department.
[Online] http://www.sbp.org.pk/bprd/2007/Policy_Paper_RF_Mobile_Banking_07-Jun-07.pdf.

This State Bank of Pakistan policy paper outlines three mobile banking models: bank-focused, bank-led and non-bank-led, and discusses the risks involved with each model. Agent related risks are common to all transformational models; however, e-money risks are more typical in the non-bank-led model because non-bank entities are not subjected to prudential regulation and supervision. The State Bank of Pakistan's conclusion is that Pakistan should start with the basic bank led model and gradually move to the other models as its regulations are expanded.

Wishart, Neville. (2006) "Micro-Payment Systems and Their Application to Mobile Networks: Examples of Mobile Enabled Financial Services in the Philippines," The World Bank/*Info*Dev, Washington DC.
[Online] http://www.infodev.org/en/Publication.43.html.

This article explores some of the reasons behind the success of mobile financial services in the Philippines, including the ability to load prepaid airtime credits, the ability to transfer both cash and airtime credits between customers, and low values set by the operator for prepaid top-ups or credit transfers. The author also discuss some of the similarities between successful mobile banking models used in the Philippines, South Africa and Kenya, including provisions for cash deposits and withdrawals, the ability for third parties to make deposits into a user account and the ability to make retail purchases at selected outlets.

AML/CFT

ATM Industry Association. (2008) "Best Practices for Mobile Device Banking Security: International Minimum Security Guidelines for Mobile Device Banking Applications."
[Online]
http://www.atmia.com/ClassLibrary/Page/Information/DataInstances/1556/Files/525/Best_Practices_for_Mobile_Phone_Banking_Security_-_Published_version.pdf.

This article identifies the key steps that consumers of mobile banking, including users of mobile phones and the internet, should take to prevent fraud. The article provides practical advice on using a PIN number to protect information on SIM cards, dealing with lost or stolen mobile phones/devices, and the use of voice biometrics to provide an added layer of security. Of most importance to this audience is the discussion on know your customer (KYC) requirements and AML/CFT requirements to protect the customer and financial institution.

Bank for International Settlements. (2001) "Customer Due Diligence for Banks," Basel Committee on International Settlements, Basel, Switzerland.
[Online] http://www.bis.org/publ/bcbs85.htm.

This paper reinforces the principles established in earlier Basel Committee papers by providing more precise guidance on the essential elements of KYC standards and their implementation. In developing this guidance, the Working Group has drawn on practices in member countries and taken into account evolving supervisory developments. The essential elements presented in this paper are guidance on minimum standards for worldwide implementation for all banks. For example, enhanced diligence is required in the case of higher-risk accounts or for banks that specifically aim to attract high net-worth customers. In a number of specific sections in this paper, there are recommendations for higher standards of due diligence for higher risk areas within a bank, where applicable.*

Bankable Frontiers Associates. (2008) "Managing the Risk of Mobile Banking Technologies," commissioned by FinMark Trust. [Online] www.bankablefrontier.com/assets/MB**Technologies_risks**.pdf.

This report provides a process for identifying, assessing and mitigating risks in mobile banking. It also reviews the particular technologies relevant to the mobile environment and benchmarks these against other electronic systems such as e-banking and ATMs. Four main Use Cases are outlined and are differentiated by the key factors related to the technological choices which have a fundamental impact on risk. The report concludes with the choice of business model and the question of environmental risk factors which need to be taken into account in reaching a final adjusted and scaled risk rating.*

Bester, Hennie, et al. (2008) "Implementing FATF Standards in Developing Countries and Financial Inclusion: Findings and Guidelines," FIRST Initiative, Washington, D.C.
[Online]
http://www.firstinitiative.org/Projects/_actProjectDocumentDownload.cfm?iDocumentID=5370&iProjectID=373.

This report considers the impact of the implementation of AML/CFT controls on financial inclusion in five countries (Indonesia, Kenya, Mexico, Pakistan and South Africa). Based on these findings, it develops a set of guidelines to assist the authorities in developing countries to design effective AML/CFT regimes that are compliant with Financial Action Task Force (FATF) standards and support financial inclusion.

Annotated Bibliography

Chatain, Pierre-Laurent, et al. (2008) "Integrity in Mobile Phone Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing," World Bank, Washington, DC.
[Online] http://siteresources.worldbank.org/INTAML/Resources/WP146_Web.pdf.

This working paper explores strategies to identify and manage potential money laundering and terrorist financing risks in mobile financial services. Using fieldwork in seven economies (Brazil, Hong Kong, Macao, Malaysia, Philippines, South Africa, South Korea) as a basis, the paper provides guidance on the best means of assessing perceived versus actual ML and TF risks, then identifies specific measures to mitigate the actual risks. The paper concludes with recommendations that aim to promote a regulatory balance to foster an enabling environment for business while minimizing ML and TF.*

Chatain, Pierre-Laurent, et al. (2009) "Preventing Money Laundering and Terrorist Financing," World Bank, Washington, D.C. [Online]
http://siteresources.worldbank.org/EXTFINANCIALSECTOR/Resources/Preventing_Money_Laundering_Terrorist_Financing.pdf.

This World Bank publication is specifically designed for bank supervisors who may be looking for ways to devise a program of AML/CFT supervision or who are looking for alternatives to their current system of supervision. The objective of this book is to provide a "how to" reference for practitioners of financial regulation and supervision. The authors have attempted to conceive a *practical* guide, with the purpose of resolving strategic and operational supervisory issues. The authors cover topics including supervision objectives, the design and carrying out of onsite and offsite inspection programs, cooperation with other domestic and international AML/CFT authorities, sanctions and enforcement.

Financial Action Task Force. (2007) "Guidance on the Risk Based Approach to Combating Money Laundering and Terrorist Financing." [Online] http://www.fatf-gafi.org/LongAbstract/0,3425,en_32250379_32235720_38960577_1_1_1_1,00.html

The Guidance was developed by the FATF in close consultation with representatives of the international banking and securities sectors. The Guidance supports the development of a common understanding of what the risk-based approach involves, outlines the high-level principles involved in applying the risk-based approach, and indicates good public and private sector practice in the design and implementation of an effective risk-based approach.*

Isern, Jennifer, et al. (2005) "AML/CFT Regulation: Implications for Financial Service Providers That Serve Low-Income People," CGAP/World Bank, Washington, D.C.
[Online] http://siteresources.worldbank.org/EXTAML/Resources/396511-1146581427871/AML_implications_complete.pdf.

This article explores how the introduction of new or tightened AML/CFT regulations may have the unintended and undesirable consequence of reducing the access of low income people to formal financial services. In order to avoid this outcome, this paper argues in favor of (1) gradual implementation of new measures; (2) the adoption of a risk-based approach to regulation; and (3) the use of exemptions for low-risk categories of transactions. The authors cite the South African model as an example of how a country's AML/CFT regulations can be modified to take into account the needs of low-income clients.*

Mobey Forum, Mobile Financial Services. (2003) "Mobile Device Security Element: Key Findings from Technical Analysis, V 1.0."
[Online]
http://www.mobeyforum.org/files/Mobey%20Forum%20White%20Paper%20on%20Mobile%20Financial%20Services%20v1_14.pdf.

This paper discusses the security requirements and technical aspects of mobile financial services. Furthermore, current and emerging mobile technologies are evaluated together with Mobey Forum requirements. The main goal of the document is to give advice and information for the financial industry on how they can start offering mobile services to customers.*

Country Specific Regulations

Central Bank of the Philippines. (2009) "Circular No. 649."
[Online] http://www.bsp.gov.ph/downloads/Regulations/attachments/2009/c649.pdf

This recently released Circular provides guidelines on minimum requirements for Electronic Money Issuer (EMI), which includes non-banks registered by the Central Bank as a money transfer agent.

Among other things, the Circular states that (1) EMIs should maintain accurate and complete records of e-money transactions; (2.) E-money instruments are subject to an aggregate monthly load limit of PhP100k; (3) EMIs must comply with KYC and AML standards.

Annotated Bibliography

Reserve Bank of India (2009) **"**Policy Guidelines for Issuance and Operation of Prepaid Payment Instruments in India." [Online] http://www.rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=5216

This Reserve Bank of India guideline states that mobile phone based semi-closed system pre-paid payment instruments are permitted in India, given that operators fully comply with KYC provisions, there is no person-to-person transfer of value, and the maximum value of such instruments does not exceed Rs 5000.

Reserve Bank of India. (2009) "Mobile Payment in India - Operative Guidelines for Banks." [Online] http://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=1365

This guideline states that it is responsibility of the banks offering mobile payment service to ensure compliance to these guidelines, including KYC and AML. To promote interoperability between banks and mobile payments service providers, the RBI recommends that banks adopt the message formats being developed by Mobile Payments Forum of India (MPFI) concerning switching of ATM transactions, which may be suitably adapted for communication between switches where the source and destination are credit card/ debit cards/pre-paid cards.

South African Reserve Bank. (2006) "Banks Act Circular 6/2006: Cell-Phone Banking." [Online] http://www.icbs.co.za/internet/Publication.nsf/LADV/E690E58853D2A429422571AA00458CCE/$File/Banks+Act+Circ+6+of+2006.pdf.

This circular deals with bank accounts that are operated by cell phone operators. It sets out minimum criteria that must be met in order for such products to be offered to clients including: (1) the bank account must meet all the parameters and conditions of exemption under the Financial Intelligence Centre Act; (2) debits must be limited to R1,000 per day; (3) control measures must be included to prevent a person from opening more than one account.

Mobile Operator Reports

CTIA, The Wireless Association. (2009) "Best Practices and Guidelines for Mobile Financial Services." [Online] files.ctia.org/pdf/CTIA_MFS_**Guidelines**_BP_Final_1_14_09.pdf.

This report provides guidelines to MFS providers regarding industry best practices to authenticate user identity and obtain user authorization. Some of the best practices specific to mobile banking include multifactor authentication, PINs, challenge questions, one-time use passwords and codes, and express authorization of transactions. General guidelines for theft protection, dispute resolution and security of data transmissions are also provided.

Vodafone. (2009) "India: The Impact of Mobile Phones," *Policy Paper Series, No. 9*, Vodafone, London [Online] http://www.vodafone.com/etc/medialib/public_policy_series.Par.56572.File.dat/public_policy_series_9.pdf.

This report explores the economic impact of telecommunications in India, particularly in the area of agricultural productivity. The report provides compelling findings on the correlation between mobile phone penetration and a rise in per capita income. While the report does not focus on mobile banking, it does clearly show that mobile phone usage is widespread both in urban and rural settings, which is an important precondition for the success of mobile financial services.

Vodafone. (2007) "The Transformational Potential of m-Transactions," *Policy Paper Series, No. 6*, Vodafone, London. [Online] http://www.gsmworld.com/documents/VOD833_Policy_Paper_Series_FINAL.pdf.

This Vodafone policy paper is made up of six articles, including those that discuss early lessons from the M-PESA model, the regulatory implications of MFS convergence, competition issues in the development of m-transaction schemes, and using a two-sided-platforms approach toward mobile transactions.

Vodafone. (2005) "Africa: The Impact of Mobile Phones," *Policy Paper Series, No. 2*, Vodafone, London [Online] http://www.vodafone.com/etc/medialib/public_policy_series.Par.77697.File.dat/public_policy_series_2.pdf.

This report is similar in structure to the Vodafone report written on mobile phones in India, in that it evaluates the connection between an increase in mobile phone usage and economic growth and FDI in Africa. This report also includes a discussion on the impact of mobile phone use on social capital in rural South Africa and Tanzania and presents the findings from community and business surveys on mobile communications in South Africa, Tanzania and Egypt.

Annotated Bibliography

Consumer Related Documents

Meso, Peter, Phillip Musa and Victor Mbarika. (2005) "Towards a Model of Consumer Use of Mobile Information and Communication Technology in LDCs: the Case of Sub-Saharan Africa." *Information Systems Journal* (15). [Online] http://www.icitd.org/attachments/058_ISJ_Paper_in_PDF.pdf

> Using theories of technology acceptance and technology transfer, this article identifies factors affecting the use of mobile information and communication technology (mobile ICT) in sub- Saharan Africa. The researchers surveyed mobile ICT users in Kenya and Nigeria and found that access to mobile ICT and cultural influences on mobile ICT diffusion strongly influence individuals' perceptions of the usefulness and ease of use of mobile ICT. The results suggest that, although extensive ICT diffusion (high mobile ICT levels per capita) may be necessary for m-commerce, it may not be sufficient. Firms conducting business in sub-Saharan Africa need to pay attention to the factors that explain individual mobile ICT use because these factors will most likely determine the optimal market segmentation, business development and customer service strategies for leveraging m-commerce operations. For government units, the understanding of such factors would also be beneficial in aiding economic planning and commerce.*

Pousttchi, Key. (2003) "Conditions for the Acceptance and Usage of Mobile Payment Procedures," The Second International Conference on Mobile Business, Vienna. [Online] http://mpra.ub.uni-muenchen.de/2912/.

> This paper examines the conditions for acceptance and actual usage of mobile payment procedures by the customer. It identifies essential conditions such as cost, security and convenience. The authors propose a scheme for their representation and comparison and, based on these results, examine the relevance of the different criteria with empirical results. Additionally, they propose an approach for the usage of mobile payment procedures based on the theory of informational added values. Finally, applications and constrictions of the results are shown and an outlook on the future of mobile payment is given.*

Wright, Graham, et al. (2006) "Mobile Phone Based Banking: The Customer Value Proposition," *MicroSave Briefing Note 47.*
[Online]
http://www.ruralfinance.org/servlet/BinaryDownloaderServlet?filename=1145534725265_BN_47___Mobile_Phone_Banking_The_Custome1146149706.pdf.

> The main argument of this MicroSave briefing is that MFS providers will only be successful if they are able to respond to the needs of the low-income customer. These customers are mainly concerned about convenience, cost, security and being able to move money around quickly. Wizzit is cited as being a successful model because as part of its preparatory phase, Wizzit used focus groups to establish the spending patterns and financial transactions of its low-income target group. Based on this research, Wizzit learned that their clients wanted inter-operability with the mainstream ATM/POS-device based payments system, which is available in South Africa.

General Documents

Bank of International Settlements. (2006) "General Guidance for National Payment System Development," Committee on Payment and Settlement Systems, Basel, Switzerland.
[Online] http://www.bis.org/publ/cpss69.pdf?noframes=1.

> The purpose of this report is to assist countries that are building their national payment systems, and those that wish to develop their system further, with practical guidance for development. The report contains 14 guidelines, which are based on the experiences of a broad group of central banks from developed and developing countries around the world, and those of the World Bank and the IMF, with
> regard to the development of payment systems. It draws as well on earlier and current work of the CPSS, the World Bank, the IMF and other central banks on payment systems. However, unlike much of this work, which often refers to specific instruments, procedures and inter-bank transfer mechanisms, this report takes a broad perspective on the composition of a payment system.*

Bank for International Settlements. (2004) "Survey of Developments in Electronic Money and Internet and Mobile Payments," Committee on Payment and Settlement Systems, Basel, Switzerland.
[Online] http://www.bis.org/publ/cpss62.pdf?noframes=1.

> This report provides the findings from a survey conducted by the Committee on National Payment and Settlement Systems regarding developments in internet and mobile payments around the world. 95 central banks and monetary authorities from around the world participated in this survey. For each country, card-based products, software based products and mobile payments are discussed, as well as the policy responses to these new developments.

Annotated Bibliography

Bank of International Settlements. (2001) "Core Principles of Systemically Important Payment Systems," Committee on Payment and Settlement Systems, Basel, Switzerland.
[Online] http://www.bis.org/publ/cpss43.pdf?noframes=1.

This report outlines the core principles that govern the design and operation of payment systems in all countries, as established by the Committee on Payment and Settlement Systems. Guidance is also provided on how to interpret and implement the core principles. Some of the issues that the principles tackle concern settlement, security, operational reliability and efficiency. The core principles are not intended to be a blueprint for the design of a payment system; rather, they suggest the key characteristics that payment systems should have.

Choi, Sean and David Collins. (2007) "Mobile Payments in Asia Pacific," KPMG.
[Online[http://www.kpmginsiders.com/pdf/Mobile_payments.pdf.

This report explores the various types of m-payments systems in Asia, including MNO-centric, bank-centric, vendor-centric, and payments platform-centric. Different business models such as business-to-consumer, business-to-business, consumer-to-consumer, and remittances are discussed as well. These models are discussed in the context of the markets of Japan, Korea, China, India, Indonesia, Philippines, Hong Kong, Singapore, Malaysia, Thailand and Vietnam.

Cracknell, David. (2004) "Electronic Banking for the Poor- Panacea, Potential and Pitfalls," MicroSave, Nairobi
[Online] http://www.microfinancegateway.org/gm/document-1.9.29225/25231_file_MicroSave_ebanking.pdf

This article discusses the various forms of electronic banking including automatic teller machines and point of sale devices, personal digital assistants, magnetic stripe cards, smart cards and cell phones. The author argues that for any of these methods to be successful, the customer value proposition of accessibility, affordability and ease of use must be considered. There is also a business case for electronic banking which seeks to increase profitability through appropriate fees and charges and focusing on efficiency gains.

Davis, Ben and John Owens. "Incentivising 3rd Party Agents to Service Bank Customers," *MicroSave Briefing Note 69.*
[Online] http://www.microsave.org/briefing_notes/briefing-note-69-incentivising-3rd-party-agents-to-service-bank-customers

This article compares the two models for using agents: branchless banking service agents and mobile commerce providers. For both models, the agent's willingness to provide services is impacted by the complexity of services, expected volume of transactions, the impact on the agent's primary business, and fees generated. The authors argue that third party agents are crucial to the success of the mobile banking and considering the value proposition for this group is one of the most important issues that branchless banking operators face.

Davis, Ben and John Owens. "POS vs. Mobile Phone as a Channel for M-Banking," *MicroSave Briefing Note 66.*
[Online] http://www.microfinancegateway.org/gm/document-1.9.34160/1_POS%20vs.%20Mobile%20Phone%20as%20a%20Channel%20for%20M-Banking.pdf

This note focuses on the relative merits of using the point of sale (POS) system and the mobile phone for branchless banking. The two types of systems are assessed based on their transactional capabilities, convenience and product appropriateness. The authors conclude that a model that combines and offers the ease of a mobile phone-based system while offering a POS card, that builds on the existing network of POS and ATM terminals, will most likely offer a significant advantage to a mobile phone-based or POS-based only solution.

Duncombe, Richard and Richard Boeteng. (2009) "Mobile Phones and Financial Services in Developing Countries: A Review of Concepts, Methods, Issues, Evidence and Future Research Directions," Institute for Development Policy and Management, Manchester, UK.
[Online] http://www.sed.manchester.ac.uk/idpm/research/publications/wp/di/documents/di_wp37.pdf

This paper seeks to improve understanding of mobile financial services in developing countries by reviewing the content of 43 research articles related to this topic. A framework is developed that categorizes and analyses the research according to a socio-technical spectrum. Research weaknesses and gaps are identified suggesting that issues relating to financial needs and the measurement of impacts have been comparatively neglected, while application design and adoption have received greater attention. In order to correct this imbalance in research, the paper identifies key research gaps relating to concepts, methodologies, issues addressed and evidence presented and provides pointers to future research directions.*

Hoffmann, Jenny. "Issues in Mobile Banking 2: Regulatory and Technical Issues," *MicroSave Briefing Note 52.*
[Online] http://www.microsave.org/briefing_notes/bn52-regulatory-and-technical-issues-in-mobile-banking-

Meeting regulation requirements remains one of the key barriers for financial institutions to implementing mobile banking. In addition, many financial institutions struggle with technology issues around selecting appropriate systems and delivery channels. Whether it is picking the correct system, properly selecting and managing agents, or instituting appropriate face-to-face interactions with the customer, This Briefing Note provides examples from various countries to show how these challenges have been met.

Annotated Bibliography

Ivatury, Gautam and Ignacio Mas. (2008) "The Early Experience with Branchless Banking," CGAP, Washington DC. [Online] http://www.cgap.org/gm/document-1.9.2640/FocusNote_46.pdf

Using examples from Colombia, the Philippines, Kenya, Pakistan, South Africa and the Maldives, this CGAP paper discusses seven common trends observed in branchless banking in these countries. Some of the trends include: the first mover advantage for mobile operators, MFIs are largely being left out of this process, and branchless banking channels are used mainly for payments, not for savings or credit. The authors conclude the paper with four key uncertainties that remain with branchless banking, such as issues with interoperability and AML/CFT requirements.

Jefferis, Keith. (2009) "Product Innovation and Access to Finance in Africa," Econsult (Botswana) Pty Ltd, Gabarone. [website] http://www.econsult.co.bw/.

This paper provides an overview of the various types of financial products that have been made available in recent years (such as person to person money transfers, remote payments, e-commerce, agency banking, internet and mobile banking). Jefferis then questions the extent to which technology based products and services have extended access to finance for the poor. Using examples from Kenya and Botswana, Jefferis concludes by providing a list of conditions that support the development of innovative business models for accessing finance.

Krueger, Malte. (2001) "The Future of M-Payments—Business Options and Policy Issues," Institute for Prospective Technological Studies, Seville, Spain. [Online] ftp://ftp.jrc.es/pub/EURdoc/eur19934en.pdf.

The task of this background paper is to show that m-payments are likely to become an important section of the retail payment sector and to identify future policy issues related to their development. While there are many actors that might provide m-payment services, banks and telcos are the most obvious candidates. An effective functioning of m-payments will require co-operation and interoperability between these two players. This raises a number of competition policy issues in particular with respect to pricing that are discussed in this paper.*

Lyman, Timothy, Gautam Ivatury, and Stefan Staschen. (2006) "Use of Agents in Branchless Banking for the Poor: Rewards, Risks and Regulation," *CGAP Focus Note # 38*. CGAP, Washington, D.C. [Online] http://www.cgap.org/gm/document-1.9.2585/FocusNote_38.pdf

The authors discuss the main issues involved with branchless banking through retail agents, focusing on two main models: the bank-led model and nonblank-led model. They examine the various risks involved with the use of retail agents, including credit risk, operational risk, legal risk, liquidity risk, and reputational risk. Drawing from examples from Brazil, India, South Africa, the Philippines and Kenya, the article illustrates how banking regulators have responded to these agent-related risks thus far. It concludes by leaving policy makers and regulators with considerations for future branchless banking efforts.

Lyman, Timothy, Mark Pickens, and David Porteous. (2008) "Regulating Transformational Branchless Banking: Mobile Phones and Other Technology to Increase Access to Finance," *CGAP Focus Note #43*. CGAP, Washington, DC. [Online] http://cgap.org/gm/document-1.9.2583/FocusNote_43.pdf.

This CGAP article offers guidance and recommendations to policy makers and regulators regarding how to formulate regulatory policy that gives space for innovation and permits branchless banking to scale up safely. The authors outline "necessary but not sufficient" policies for transformational branchless banking, followed by policies that will ensure the sustainability of branchless banking. The authors' core recommendation for policy makers and regulators is to use proportionality as a guiding principle when regulating branchless banking.

Mas, Ignacio and Kabir Kumar. (2008) "Banking on Mobiles: Why, How, for Whom?" *CGAP Focus Note # 48*. CGAP, Washington DC. [Online] http://www.cgap.org/gm/document-1.9.4400/FN_48%20ENG_9-10-08.pdf

This CGAP article focuses on the advantages to using mobile banking for smaller banks and MFIs. The authors argue that using phones as an access tool is advantageous to banks because they can increase penetration, sell more services, retain the most valuable customers, and reduce the cost of providing services. Mobile banking stands apart from other types of m-banking options because the phone can be used as a virtual identity (PIN and account number) storage system and the phone can be used to check on account information, move money, and make payments.

Mas, Ignacio and Jim Rosenberg. (2009) "The Role of Mobile Operators in Expanding Access to Finance," *CGAP Brief*. CGAP, Washington DC. [Online] http://www.cgap.org/gm/document-1.9.34485/Mobileoperators_Brief.pdf.

This CGAP brief discusses why phone companies that operate mobile networks would want to provide financial services as well. While additional revenues and increased brand recognition may be motivating factors for mobile operators to offer payment services, the authors caution operators against risks such as fraudulent transactions. Mas and Rosenberg provide various value chain options for mobile operators in the delivery of mobile transactions that can mitigate these risks.

Mas, Ignacio and Sarah Rotman. (2008) "Going Cashless at the Point of Sale: Hits and Misses in Developing Countries," *CGAP Focus Note # 51*. CGAP, Washington DC. [Online] http://www.cgap.org/gm/document-1.9.7885/FN_51.pdf..

This CGAP focus note explores why some countries have been more successful than others in launching electronic payments. The objective of this report is to extract some lessons behind the

Annotated Bibliography

failures and the successes. The report discusses three broad approaches (smartcard-based electronic cash providers, mobile operators facilitating existing payment instruments, mobile operator-centric payment schemes), and in each case looks at two providers who met different degrees of acceptance in the marketplace.

Owens, John. "The Role of Partnerships and Strategic Alliance to Promote Mobile Phone Banking at the Bottom of the Pyramid," *MicroSave Briefing Note 68.* [Online] http://www.globaldevelopmentcommons.net/files/BN%2068%20Strategic%20Partnerships%20for%20M-banking.pdf.

This report discusses how smaller banks and MFIs can best provide mobile financial services. The author concludes that smaller banks and MFIs would benefit from working together to share a mobile phone banking platform, which creates economies of scale and a more promising business case for larger banks or MNOs that could host a mobile phone banking platform for the smaller banks. Smaller banks and MFIs can also outsource technical development and management of agent networks to a third-party mobile banking service provider.

Owens, John. "Pilot and Rollout Issues for Mobile Phone Banking Services," *MicroSave Briefing Note 70.* [Online] http://www.microsave.org/briefing_notes/bn70-pilot-and-rollout-issues-for-mobile-phone-banking.

This note echoes many of the issues raised in the MicroSave note above regarding the need for small MFIs to partner with other groups in order to be successful. Owens also adds that institutional issues, such as proper training for frontline and back office staff, is necessary when piloting mobile banking programs. Owens cautions against the potential for exponential uptake during pilot testing, which may make controlled pilot tests more difficult.

Pickens, Mark, David Porteous, Sarah Rotman. (2009) "Scenarios for Branchless Banking in 2020," *CGAP Focus Note #57.* CGAP, Washington DC. [Online] http://www.cgap.org/gm/document-1.9.40599/FN57.pdf.

For this CGAP note, the authors undertook a scenario-building project in which they attempt to answer the question "How can government and private sector most affect the uptake and usage of branchless banking among the poor by 2020?" To answer this question, the authors created four scenarios in different settings to produce very different trajectories over the next 10 years. The scenarios pertain to: (1) which types of entities will be allowed to provide branchless financial services; (2) will providers craft viable business models for services beyond payments?; (3) how will competition play out?; and (4) how will consumer, business, and regulator confidence be affected by the inevitable failures that will happen?

Porteous, David. (2007) "Just How Transformational is M-Banking?" Bankable Frontiers Association. [Online] http://www.finscope.co.za/documents/2007/transformational_mbanking.pdf.

This paper asks how mobile banking has changed access to basic banking accounts. It analyses recent data from South Africa on financial service use and attitudes, using the access frontier approach. Porteous finds that barriers around trust and ignorance must be overcome to encourage even existing banked people to use mobile phones. Rapid dispute resolution and a guarantee that consumer loss resulting from fraud will be limited is recommended. Porteous also finds that persuading existing banked customers to use mobile banking may in fact be harder than targeting unbanked customers, but does not provide a solution for addressing this challenge.

Porteous, David with Neville Wishart. (2006) "M-Banking: A Knowledge Map." [Online] http://www.mifos.org/knowledge/resources/development/mifos-mobile/prelim-info/infoDev%20m-BANKING%20A%20KNOWLEDGE%20MAP%28web%29.pdf.

This report considers why donors should support mobile banking, using the theory that links m-banking with poverty reduction. The authors also discuss the needs and gaps arising from the development of the sector to date, in the light of what donor funded programs are already doing. The report concludes with strategies and particular initiatives which donors may take to respond to the needs and gaps that are identified in the report.

Porteous, David. (2006) "The Enabling Environment for Mobile Banking in Africa," DFID, London. [Online] http://www.bankablefrontier.com/assets/ee.mobil.banking.report.v3.1.pdf

This report investigates the extent to which the expansion of mobile telephony is likely to lead to the expansion of access to appropriate financial services in developing countries. In particular, it seeks to answer two main questions: (1) Which models of mobile banking are emerging globally, and especially in Africa, and are they likely to be accelerate access? (2) Will it happen spontaneously or is enablement required for this to happen? To answer these questions, the report investigates emerging models of development in m-payments and m-banking through interviews with emerging African providers and the use of secondary material. It assesses the policy and regulatory elements of an enabling environment for this sector based in part on the analysis of circumstances in two pilot African countries (Kenya and South Africa).*

Saji, K.B and Aditya Agarwal. (2006) "Mobile Payments- Six Issues." *International Journal of Mobile Marketing* (awaiting publication). [Online] http://www.scribd.com/doc/2241323/Mobile-Payment-I-Six-Issues

The authors discuss six factors which they believe govern the success of mobile payment systems. These factors are: current payment relationships, relationship scenarios, sustainability, ubiquity,

regulatory and security concerns, and market segmentation. Drawing from the success of mobile banking in the Philippines, the researchers conclude that the numerous issues addressed in the paper have to be met before expecting mass adoption of mobile banking.

Mobile Banking Presentations

Windsor II Global Leadership Seminar on Regulating Transformational Branchless Banking, 2009:

Protecting Branchless Banking Consumers: Policy Responses to New Ways of Doing Business:
http://www.cgap.org/gm/document-1.1.1174/ConsumerProtection-BranchlessBanking-1.pdf

Defining Regulatory Space for Non-Bank Service Providers:
http://www.cgap.org/gm/document-1.9.9811/Defining%20Regulatory%20Space%20for%20Nonbank%20service%20providers.pdf

World Bank Conference on Mobile Financial Services, Bangkok 2008:
(For a full list of presentations, see:
http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTFINANCIALSECTOR/EXTAML/0,,contentMDK:21847685~isCURL:Y~pagePK:210058~piPK:210062~theSitePK:396512,00.html)

Updates as of July 2010

Rolling out of New Mobile Banking Business in Zambia and DRC:
http://siteresources.worldbank.org/INTAML/Resources/Mobile_Banking_Zambia_DRC.pdf

Countering the Use of Mobile-FS in the Money Laundering:
http://siteresources.worldbank.org/INTAML/Resources/Countering_ML_Mobile_Banking_Korea.pdf

Regulating and Overseeing Mobile Payments: A Payment Systems Perspective
http://siteresources.worldbank.org/INTAML/Resources/Regulating_and_Overseeing_Mobile_Payments.pdf

AITEC PRESENTATION SESSION, 17TH–25TH, FEBRUARY, 2010, Samuel Mutungi, The Co-Operative Bank of Kenya, Ltd.

Bank for International Settlements, Basel Committee on Banking Supervision (October 2001) - "Customer Due Diligence for Banks."

Barbier, Eric, "TransferTo," MMT09 Conference and Expo, JW Marriot, Dubai, 26-27 October 09.

CGAP Washington DC (2007) "Notes on Branchless Banking Policy and Regulation in Kenya," Consultative Group to Assist the Poor.

CGAP 2007 "Notes on AML-CFT Compliance: Challenges with Branchless Banking and Examples of Industry and Regulatory Responses." http://www.cgap.org/technology

CGAP, January 2010 "Update on Regulation of Branchless Banking in India".

CGAP, February 2010 "Update on Regulation of Branchless Banking in Pakistan".

CGAP, January 2010 "Update on the Regulation of Branchless Banking in South Africa"

CGAP, January 2010 "Updated on Regulation of Branchless Banking in India".

CGAP 2009, Washington, DC Abbassi, Ala'a, Mohammed Khaled, Klaus Prochaska, and Michael Tarazi. "Access to Finance: Microcredit and Branchless Banking in The Hashemite Kingdom of Jordan".

CGAP 2009, Washington, DC Abbassi, Ala'a, et. al. "Access to Finance: Microcredit and Branchless Banking in the Hashemite Kingdom of Jordan."

CGAP 2009, Aguirre, Ernesto, Dias, Denise, Seltzer, Yanina. "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in El Salvador".

CGAP Washington DC 2008 "Notes on Branchless Banking Policy and Regulation in Brazil," CGAP.
http://www.cgap.org/gm/document-1.9.2319/Brazil-Notes-On-Regulation-Branchless-Banking-2008.pdf

CGAP Washington DC 2008 "Notes on Branchless Banking Policy and Regulation in Brazil," Consultative Group to Assist the Poor.

Annotated Bibliography

CGAP Washington DC 2008 "Notes on Branchless Banking Policy and Regulation in South Africa," Consultative Group to Assist the Poor.

CGAP Washington DC 2009 "Notes on Branchless Banking Policy and Regulation in Mexico," Consultative Group to Assist the Poor.

CGAP, Washington, D.C 2009 "AML/CFT: Strengthening Financial Inclusion and Integrity" by Isern, Jennifer, and Louis de Koker Focus Note 56.

Chaitain, Pierre-Laurent. (June 24-26, 2008). "Applying the FATF International standards to Mobile Financial Services." Workshop on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) for Mobile Financial Services (m-FS).

Chaitain, Pierre-Laurent. (June 24-26, 2008). "Applying the FATF International standards to Mobile Financial Services." Workshop on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) for Mobile Financial Services (m-FS).

Chatain, Pierre-Laurent. (June 24-26, 2008) "Applying the FATF International standards to Mobile Financial Services." Workshop on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) for Mobile Financial Services (m-FS). Bangkok, Thailand.

"Cloud Based Voice Biometrics E-commerce Platform", 15 June 2010, http://www.infosecurity-magazine.com/view/10223/couldbased-voice-biometrics-ecommerce-platform-introduced/

Davidson, Neil, Leishman, Paul, "Building, Incentivizing and Managing a Network of Mobile Money Agents: A Handbook for Mobile Network Operators,"GSMA, mmu@gsm.org, accessed July 7, 2010.

Davidson, Neil, Leishman, Paul, "Building, Incentivizing and Managing a Network of Mobile Money Agents: A Handbook for Mobile Network Operators,"GSMA, Vol. 2, mmu@gsm.org, accessed July 7, 2010.

Davidson, Neil, Leishman, Paul, "Building, Incentivizing and Managing a Network of Mobile Money Agents: A Handbook for Mobile Network Operators,"GSMA, Vol. 3, mmu@gsm.org, accessed July 7, 2010.

Davidson, Neil, Leishman, Paul, "Managing a Network of Mobile Money Agents,"GSMA, mmu@gsm.org, accessed July 7, 2010.

Economist Intelligence Unit. (2009) "Kenya Telecoms: Banking on M-Banking." Industry Briefing.

E-Money Regulation in Mexico, April 8, 2010 - http://www.mobilemoneyexchange.org/Feeds/Research/Read/e-money-regulation-in-mexico.aspx

Estioko, Raymond. (June 24-26, 2008). "Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) for Mobile Financial Services (m-FS): The Philippine Experience." Bangkok, Thailand.

E-Zwich Becoming a Colossal Waste of Resources? - http://allafrica.com/stories/201002091058.html

Ferguson, Roger. "Implications of 9/11 for the Financial Services Sector," Remarks from the Conference on Bank Structure and Competition, Chicago, Illinois May 9, 2002.
http://www.federalreserve.gov/boarddocs/speeches/2002/20020509/default.htm

Flaming, Mark, Prochaska, Klaus, and Staschen, Stefan. (June 2009). "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in Indonesia," CGAP in cooperation with IFC and GTZ.

Forbes, John (19 April 2007). "The Convergence of Telecom and Financial Services and its Effects on AML/Wire Remittance Operations." United States Treasury, Office of Technical Assistance.

Forbes, John (March 2007) "Effects of Cell phones on Anti-Money Laundering/Combating Financial Terrorism (AML/CFT) Wire Remittance Operations."

FS SERIES #9: ENABLING MOBILE MONEY INTERVENTIONS PRIMER, DIAGNOSTIC CHECKLIST, AND MODEL SCOPES OF WORK, USAID and Financial Sector Knowledge Sharing, April 2010.

Genesis May 2008 "Implementing FATF standards in developing countries and financial inclusion" Findings and guidelines Final report.

Hernandez-Coss, Raul, Egwauagu, Chinyere, Isern, Jennifer, Porteuous, David, "AML/CFT Regulation: Implications for Financial Service Providers that Serve Low-Income People," IBRD/The World Bank, 2005.

Refugees International Kenya "National Registration Processes Leave Minorities on the Edge of Statelessness" Maureen Lynch and Katherine Southwick, May 2008 - http://refugeesinternational.org/policy/field-report/kenya-national-registration-processes-leave-minorities-edge-statelessness

Khan, Zain, "Developing ICT Capacities," AITEC Banking & Mobile Money COMESA, February 25, 2010, Nairobi, Kenya.

Korean Financial Intelligence Unit, Financial Services Commission (June 24-26, 2008) , "Countering the Use of Mobile-FS in the Money Laundering." Workshop on AML/CFT, Bangkok, Thailand.

Annotated Bibliography

Lynch, Maureen, "Kenya: National Registration Processes Leave Minorities on the Edge of Statelessness," Refugees International, 5/23/2008 http://www.refugeesinternational.org/policy/field-report/kenya-national-registration-processes-leave-minorities-edge-statelessness

Mas, Ignacio, Siedek, Hannah, "Banking Through Networks of Retail Agents", CGAP, Focus Notes NO 47, May 2008.

M-Pesa interview, Nairobi, Kenya, February 20, 2010.

Oliver, Rich, "Synthesizing the mobile ecosystem: Resolving customer problems in mobile payments clearing and settlement models," March 29, 2010. http://portalsandrails.frbatlanta.org/2-1-/03/consumer-confidence-vital-to-mobile-payments-success.html

Pyler, Megan G., Haas, Sherri, and Nagarajan, Geetha, "Community-Level Economic Effects of M-PESA in Kenya: Initial Findings," IRIS Center, University of Maryland, June 2010.

Report on the Technical Committee on Electronic Banking, Central Bank of Nigeria, February 2003.

Rishikko, Juha, Choudhary, Bishwajit, "Mobile Financial Services Business Ecosystem Scenarios & Consequences: Summary Document," Mobey Forum, Mobile Financial Services Ltd., 2006.

State Bank of Pakistan 2010 Anti-Money Laundering Act, http://www.sbp.org.pk/about/act/Anti-Act-2010.pdf

The Electronic Transactions and Communications Bill, 2009, Section 6 (1) and (2).

USAID Field Visits, Zambia, Kenya, February 9-28, 2010.

USAID interview, Tanzania, February 17, 2010.

USAID interviews, Zambia, February 16-17, 2010.

USAID Street Interviews, February 16-17, 2010, Zambia.

Wishart, Neville, "Micro-Payment Systems and Their Applicatin to Mobile Networks: Examples of Mobile-Enabled Financial Services in the Philippines," IBRD/The World Bank, 2006, pgs, 13-20.

FS SERIES #9: ENABLING MOBILE MONEY INTERVENTIONS PRIMER, DIAGNOSTIC CHECKLIST, AND MODEL SCOPES OF WORK, USAID and Financial Sector Knowledge Sharing, April 2010.

Websites Consulted:

CGAP
http://www.cgap.org/gm/document-1.1.1304/Jordan_Diagnostic_Report_2009.pdf

CGAP
http://www.cgap.org/gm/document-1.1.1306/Mexico%20Branchless%20Banking%20Notes.pdf

CGAP
http://www.cgap.org/gm/document-1.9.2319/Brazil-Notes-On-Regulation-Branchless-Banking-2008.pdf

CGAP
http://www.cgap.org/gm/document-1.9.2320/SouthAfrica-Notes-On-Regulation-Branchless-Banking-2008.pdf

CGAP
http://www.cgap.org/gm/document-1.9.2321/Kenya-Notes-On-Regulation-Branchless-Banking-2007.pdf

CGAP
http://www.cgap.org/gm/document-1.9.2322/India-Notes-On-Regulation-Branchless-Banking-2008

Financial services Assessment
http://www.fsassessment.umd.edu/

World Bank Working Paper 146
http://siteresources.worldbank.org/INTAML/Resources/WP146_Web.pdf

GSM World
http://www.gsmworld.com/documents/VOD833_Policy_Paper_Series_FINAL.pdf

Info/DEV – Innovate, Connect, Transform
http://www.infodev.org

Annotated Bibliography

MALAWI GOVERNMENT - Money Laundering, Proceeds of Serious Crime Terrorist Financing 1
http://www.fiumalawi.gov.mw/fiu2/documents/money_laundering_act.pdf

Financial Intelligence Unit
http://www.fiumalawi.gov.mw/fiu2/index.php?option=com_content&view=article&id=19&itemid=27

Kenyan Department of National Registration Bureau
http://www.identity.go.ke.

IFLR 1000 – The Guide to the World's Leading Financial Law Firms
http://www.iflr1000.com/legislationguide/192/the-e-zwich-electronic-clearing-and-payment-system.html

Interpol International
http://www.interpol.int/pv_obj_cache/pv_obj_id_7DA31F4675F7441C17F0BB94D705DB7DDEF40200/filename/FHT04.pdf

Palestinian National Authority - Anti-Money Laundering Decree Law
http://www.pma.ps/pdf/Anti-Money%20Laundry%20Law%20Eng.pdf

India Financial Intelligence Unit
http://fiuindia.gov.in/about-overview.htm

Anti-Money Laundering Council
http://www.amlc.gov.ph/amla.html

Anti-Money Laundering Council
http://www.amlc.gov.ph/archive/reso361.pdf

Central Bank of Kenya
http://www.centralbank.go.ke/currency/currencylaws.aspx

Central Bank of Kenya
http://www.centralbank.go.ke/downloads.bsd/GUIDELINES520ON%20AGENT20BANKING-CBK%20PG%2015.pdf

The Egmont Group of Financial Services Unit
http://www.egmontgroup.org/about/what-is-an-fiu

Financial Action Task Force (FATF) / Le Groupe d'Action financière (GAFI)
http://www.fatf-gafi.org/document/9/0,3343,en_32250379_32236920_34032073_1_1_1_1,00.html

Contributors

Name	Organization	E-Mail	Phone
Ghana			
Michael Fields	ACDI/VOCA	mfield@ghana-acdivoca.org	2.33544E+11
Ernest Addison	Bank of Ghana	ernest.addison@bog.gov.gh	663082 (work), 0202012723 (mobile)
John Mullenax	USAID/Ghana	jmullenax@usaid.gov	Mobile: 233 244 313 543 , Tel: 233 21 741 403
Dela Selormey	Formerly with Bank of Ghana	dela.selormey@gmail.com, dselorme@hotmail.com	020-8112519 / 233244311552 (mobile)
Sam Mensah	SEM International Associates Limited	smensah@semfinancial.com	Direct Line: +233-30-7010250, Main: +233-21-235400/238382 Cell: +233-24-4314428
Kenya			
Prof. Kinandu Muragu	KSMS	muraguk@ksms.or.ke	254-20-8646117
Moses Kiptui	KSMS		
Dr. Dulacha Galgallo Barako	KSMS	Barakodg@ksms.or.ke	
Stephen Mwaura Nduati	Head, National Payments System	MwauraSN@centralbank.go.ke	
Pauline Vaughan	Head, M-PESA	pvaughan@Safaricom.co.ke	
Brian Muthiora	Principal In House Counsel, M-PESA		
Mark Rostal	USAID/ Chief of Party	Mark_Rostal@dai.com	375-5541/42 (Mark)
Pharesh Ratego	USAID/Kenya	pratego@usaid.gov	
David Ferrand	Financial Sector Deepening	David@fsdkenya.org	+254 (20) 2718809/8814/2627, +254 (735) 319706, +254 (724) 319706
Nigeria			
Adedeji Adesemoye	Central Bank of Nigeria	aadesemoye@cenbank.org	234-8023220898 (mobile)
Charles Ifedi	Interswitch, Chief Strategy and Expansion Officer	cifedi@interswitchng.com	2.34802E+12
David Kaye	MoneyBox CEO	dkaye@moneyboxafrica.com	2.34803E+12
Adeniyi Elumaro (Niyi)	Integrated Captil Services Ltd	adeniyi.elumaro@gmail.com	2348034020993
Rwanda			
Angelique Kantengwa	National Bank of Rwanda	akantengwa@bnr.rw	00 250 573197 (office)

Contributors

Name	Organization	E-Mail	Phone
Steve Caley	Managing Director of FINA Bank; Chairman of Banker's Association	'steve.caley@finabank.co.rw'	250 598600
Fina Kayisanabo	USAID/Rwanda	fkayisanabo@usaid.gov	(250)78 830 4369 (mobile)
Tanzania			
Ben Christiaanse	National Microfinance Bank (NMB), CEO	Ben.Christiaanse@nmbtz.com	
Ian Robinson	Financial Sector Deepening	ian@fsdt.or.tz	255 (0)756 092564 (cell)
Patricia Mwangi	Financial Sector Deepening	patricia@fsdt.or.tz	
James Onyutta	FINCA		
Mark Staehle	CARE Access Africa		
Nadeem Juma	E-Fulusi Africa		
Steve Akwera	PUM-Netherlands Senior Experts		
Uganda			
Brian Conklin	USAID/Uganda	bconklin@usaid.gov	
Angela Kenyonza Kaula	Zain	Angela.Kenyonza@ug.zain.com	25675 2670777
Astollo Obbdo	Bank of Uganda, Director of Commercial Banking		2.56414E+11
Zambia			
Mark Wood	USAID/PROFIT	mark@profit.org.zm	260.976.919.938 (cell) 260.211.251.371 (office)
Rob Munro	USAID/PROFIT		
Mike Quinn	MTZL	mike@mtzl.net	+260976664643 (cell)
Binoy George	MTZL		
Dr. Denny Kalyalya	Bank of Zambia	dkalyaly@boz.zm	2601229928 (office)
Mrs. Edna Mudenda	Bank of Zambia		
Norbert Mumba	Bank of Zambia		
Chisha Mwanakatwe	Bank of Zambia		
Abraham Nyirongo	KPMG Africa		

Contributors

Name	Organization	E-Mail	Phone
Malala Simungala	KPMG Africa		
Roy Muyelu	Access Bank		
Mwaka Chilangi	Access Bank		
USAID Washington			
Chris Barltrop	USAID/EGAT/EG/EDFM	cbarltrop@verizon.net,	+1 202 368-1086 (cell)
Maria Stephens	USAID/EGAT/PR/MD	mstephens@afr-sd.org	
Booz Allen Hamilton			
Lisa Dawson	Booz Allen Hamilton	dawson_lisa@bah.com	
Michael Ingram	Booz Allen Hamilton	ingram_michael@bah.com	
Sameera Pochiraju	Booz Allen Hamilton	pochiraju_sameera@bah.com	
Michael Catalano	Open Revolution	mike@openrev.com	
Patrick Brennan	Independent		
US Treasury			
David Murray	U.S. Treasury	David.Murray@do.treas.gov	
Federal Reserve Bank of Atlanta			
Cynthia Merritt	Federal Reserve, Atlanta	Cynthia.Merritt@atl.frb.org	
GSMA			
Andrew Zerzan	GSM Association	AZerzan@gsm.org	