USAID FROM THE AMERICAN PEOPLE

BIZCLIR Business Climate Legal & Institutional Reform

Presentation

Promoting Responsible Financial Inclusion:

A Risk-based Approach to Supporting Mobile Money Transfer Services Expansion

Seattle, Washington
29 October 2010

Table of Contents

Promoting Financial Inclusion through MMT Services--Overview

Mobile payments (m-payments) are usually financial transfers between two individuals undertaken using a mobile device such as a mobile phone. Mobile banking (m-banking) includes m-payments but involves access by mobile devices to a broader range of banking services. Typical m-banking offerings allow users to:

- Check their account balances
- ***Transfer money between accounts***
- ***Send money to other people (P2P)***
- Pay bills (P2B)
- Receive salary or government payments(G2P)
- Buy airtime

Examples of mobile payment systems include:

- Smart Money, G-Cash (Philippines)
- ***M-Pesa (Kenya)***
- Wizzit (South Africa)
- M-Paisa (Afghanistan)

Introduction: Current Regulatory Situation

- As mobile financial services comprise both banking and telecommunications activities, disagreement exists on the appropriate regulatory framework as well as the appropriate regulator(s).

- One critical regulatory issue hinges on the question, "Is the stored value money?" or "Is the stored value (and associated payment capability) a service?"

- "AML and CFT procedures for m-FS providers should be designed in proportion to assessed risks. It is the duty of policy makers and regulators to determine within the different m-FS providers the higher risk areas that should be subject to enhanced procedures. Conversely, this implies also in instances where risks are low, simplified or reduced controls may be applied. (Integrity in Mobile Phone Financial Services, No. 146, *World Bank, 2007*)

- Results in questions for stakeholders of each country and decisions, based on a balanced risk identification and assessment, how best to harmonize the legal and regulatory environments for mobile financial services

Navigating the balancing act of encouraging financial innovation while simultaneously adopting a risk-based approach to regulating MMT services

- Creating a truly inclusive financial system alongside the introduction of technology driven services that have led to high rates of growth
- Need for a well-defined, well-articulated, well-regulated framework to create a “safe space”
- Framework should be flexible enough to accommodate various models, while maintaining a structural integrity applicable to all within MMT services ecosystem.

Table of Contents

Setting the Scene: Financial Technologies Past and Present

- The "shock and awe" factor of technology based financing
- The complexity of technology based products and risk models
- The tendency to create "too big to fail" institutions
- The potential for rapid and high rates of return and growth
- Lack of robust supervision of inherently risky financial transactions

Table of Contents

MMT Services Transfer Risk Environment: Global Challenges

- Global regulatory challenges resulting from converged banking and telecom industries in a cross-border context
- National central bank capacity to supervise and monitor for compliance
- Need for clear legal and governance structure in MMT service institutions

Table of Contents

USAID Project: Mobile Financial Services Risk Analysis

Objective:

To identify and develop the opportunities that the innovation of mobile payments presents for emerging markets, USAID hopes to assist Central Banks and other regulators interested in the mobile ecosystem by:

- *Identifying and classifying the risks associated with mobile payments by stakeholder group*
- *Identifying policy options and implications by risk*
- *Identifying market examples as a resource for regulators to consider*

Though the initial operating model analysis was Africa – centric, ongoing discussion with stakeholders indicates broad ranging applicability of the Matrix:

- In many other countries, regulators must balance the assurance of an enabling environment that is conducive to innovation and economic development against consumer protection concerns

- Given the lack of a common standard for the enabling environment, different regulators have responded in different ways

- Result is 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

Mobile Financial Services – Operating Models

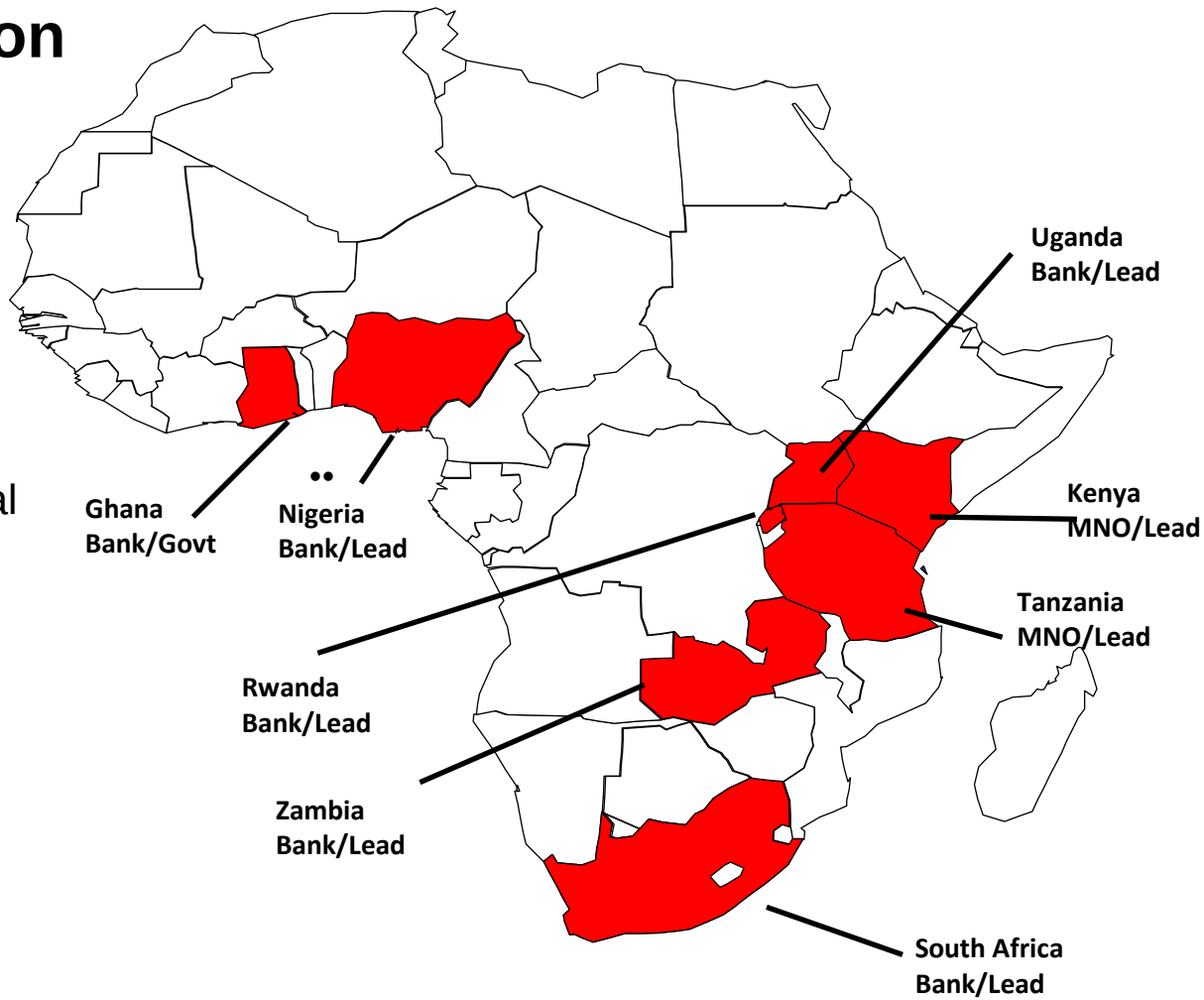
Operating Model	Observations	Examples
Bank	Primarily an additive model linked to an existing transactional account (e.g., debit card)	NMB, EQUITY Bank, easy pay
Mobile Network Operator (MNO)	A cell phone company (MNO) service extends the wireless network messaging functionality to provide payment services enabling customers to remit funds to each other that can be settled through the MNO's agent network.	M-PESA, Zap Pesa Mkononi
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.	**M-KESHO** EQUITY Bank • Your Listening, Caring Partner, Safaricom

Model Identification

Research Observations

- Extension of credit to agents by non-bank actors to meet liquidity needs of the agents;
- Group ownership of individual accounts and issues of beneficial ownership and access to credit;
- Cross border mobile value transfers

Countries of Models Identified



Definitions of Risks

- **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.
- **Operational:** A risk which damages the ability of one of the stakeholders to effectively operate their business or a risk which results in a direct or indirect loss from failed internal processes, people, systems or external events
- **Reputation:** A risk that damages the image of one of the stakeholders, the mobile system, the financial system, or of a specific product
- **Legal:** A risk which could result in unforeseeable lawsuits, judgment or contracts that could disrupt or affect MFS business practices
- **Liquidity:** A risk that lessens the ability of a bank or MFS provider/agent to meet cash obligations upon demand
- **International:** A systemic risk (as defined above) that could have cross-border contagion effect

The Matrix Identifies Risk Categorized by Stakeholder

Mobile Financial Services
Capitalizing on the Opportunity by Ensuring Sustainability

Mobile Financial Services Policy Matrix: Consumers

	#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
L	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 service 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.	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 level, technical or political capacity to enforce.			X	X		X	X	X	X
					Financial ID system: In the absence of universal ID, financial service 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.									
					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 Policy Matrix v2.2 — 5/10/2010 8:57:12 AM

Comments

- *A team comprised of experts from BAH and USAID worked in concert with the Kenya School of Monetary Studies to develop a comprehensive stakeholder risk framework*
- *The framework examines various models, including both Mobile Network Operators (MNOs) and Bank led variants*
- *For each risk, our analysis recommends various policy options and associated implications to help guide policymakers*
- *Detailed market examples inform policymakers on policy experience*

Stakeholder: Risk(s)*

- *Potential or existing customers cannot access mobile payment services due to inability to prove his/her identity.*
- *Customer's identity is stolen and used to open a mobile payment account fraudulently.*
- *Customer's account security credentials are improperly released (e.g., PIN number, biometrics, and stolen phone/SIM).*
- *Customer is unable to efficiently dispute a transaction or account charge.*
- *Customer cannot access cash from mobile money account due to lack of agent availability.*
- *Customer cannot access cash from mobile money account due to lack of system availability.*
- *Customer loses balance due to bank/provider not maintaining a 1:1 coverage requirement in the payment account trust fund.*
- *Beneficial owner(s) of stored value and transactional accounts (mobile money) cannot be determined by authorities in the event of illicit account activity when group accounts are used*

Consumers
Merchants
Agents
Account Providers
Trust Acct Holders
Payment Systems
National Regulators
Int'l Regulatory Issues

*Risks listed are not exhaustive.

Stakeholder: Risk(s)*

- *Merchants are unable to easily convert Mobile Money into cash, limiting their flexibility to run their business / store.*
- *Merchant could be restricted by a contract with a payment provider from accepting payments for or from another account provider.*

*Risks listed are not exhaustive.

Stakeholder: Risk(s)*

- *Agent is unable to easily liquidate e-money inventory when the agency relationship is terminated.*
- *Agent is robbed.*
- *Agent receives cash from client but fails to provide/transfer e-money.*
- *Agent experiencing customer protests due to inability to cash out for clients.*
- *Agent takes in cash that proves to be counterfeit.*
- *Agent pays out cash that proves to be counterfeit.*

*Risks listed are not exhaustive.

Stakeholder: Risk(s)*

- *Provider employee manipulates agent credit allowances, agent e-money balances, or customer e-money balances for financial gain.*
- *Provider fails to adequately select, train and supervise agents.*
- *Provider does not meet required regulatory responsibilities in a regulated environment.*
- *Trust fund is inadequately funded.*
- *Agent fraud untraceable due to poor records.*
- *System availability not being maintained by account provider.*
- *Agents are consistently out of cash.*
- *Agent contracted to multiple actors (i.e. cell phone provider and a bank) with different regulatory requirements (e.g. KYC) does not meet responsibilities for one or more.*

*Risks listed are not exhaustive.

Stakeholder: Risk(s)*

- *The reputation of the financial institution which holds the trust account for the mobile financial account provider is damaged due to their mismanagement of the trust account.*
- *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.*

*Risks listed are not exhaustive.

Stakeholder: Risk(s)*

- *Commerce across providers unavailable due to lack of a switch (clearing and settlement system).*

*Risks listed are not exhaustive.

Stakeholder: Risk(s)*

- *Illicit financial activities enabled by weak KYC/CDD requirements/enforcement.*
- *Identification of illicit financial activities hampered by insufficient reporting requirements.*
- *Illicit financial activities facilitated by unlicensed/ unmonitored agent network.*
- *Inadequate transaction records impair investigation of fraud or criminal activity.*
- *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*
- *National regulators and/or law enforcement authorities unable to effectively investigate fraud or criminal activity due to lack of authority.*
- *Ability to track/investigate illicit transactions made difficult by the number of financial intermediaries (e.g. agents, super agents, acct providers, banks managing trust accts) and potential lack of transparency between these parties may exacerbate challenges for regulators*
- *Account provider suspends operations or collapses, disrupting service.*
- *Financial terrorists' target payment network to destabilize financial system.*

*Risks listed are not exhaustive.

Stakeholder: Risk(s)*

- *Heightened difficulty tracking and prosecuting illicit cross-border transactions given the new payment capability with a nascent regulatory framework and enforcement mechanisms.*
- *Cross-border payments through a mobile financial service could be seen as bypassing a country's foreign exchange restrictions.*

*Risks listed are not exhaustive.

The Matrix Further Offers Policy Options and Implications Categorized by Stakeholder

Mobile Financial Services
Capitalizing on the Opportunity by Ensuring Sustainability

Mobile Financial Services Policy Matrix: Consumers

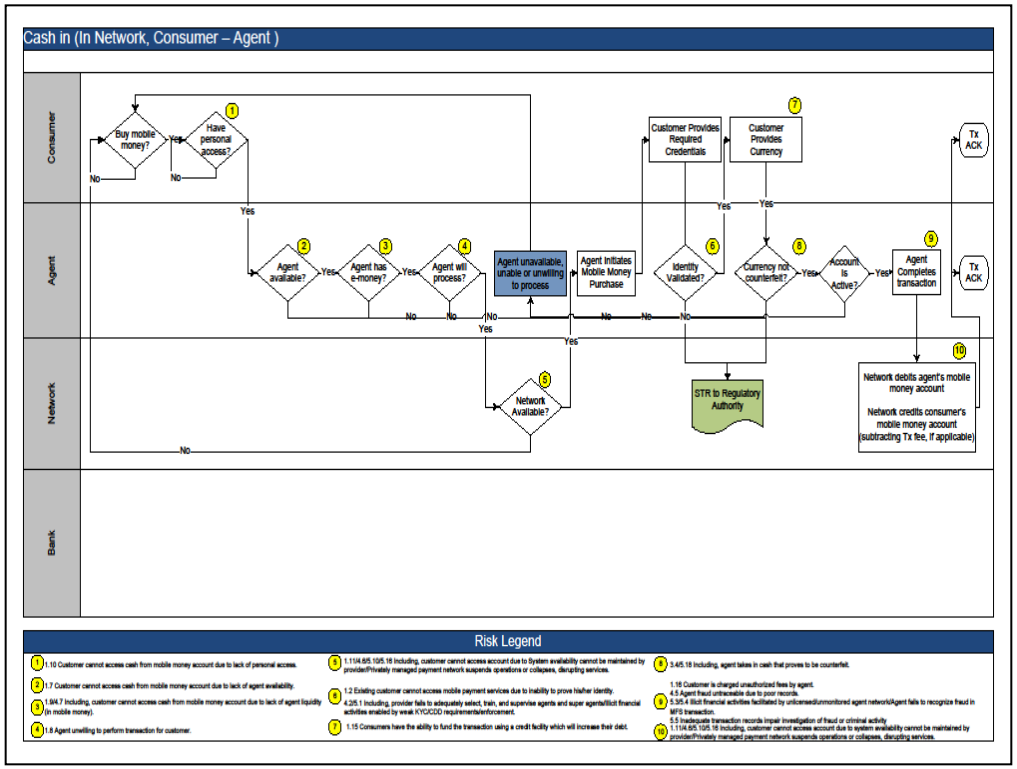
	#	Risk	Description	Objective(s)	Policy Options	Policy Implications	International	Systemic	Operational	Reputation	Liquidity	Legal	MNO Model	Bank Model	Hybrid Model
L	1.1	Potential customers cannot access mobile payment services due to inability to prove his/her identity.	When initially registering for mobile financial services (MFS), the inability of the service 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.	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 level, technical or political capacity to enforce.			X	X		X	X	X	X
					Financial ID system: In the absence of universal ID, financial service 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.									
					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 Policy Matrix v2.2 — 5/10/2010 8:57:12 AM

Comments

- *For each risk, our analysis recommends various policy options and associated implications to help guide policymakers*
- *Policy Options typically range from oversight or intervention at the National Regulator level – to graded action by the mid-tier of the mobile financial services ecosystem, usually the account provider- to no action or allowing a laissez faire mobile financial services environment*

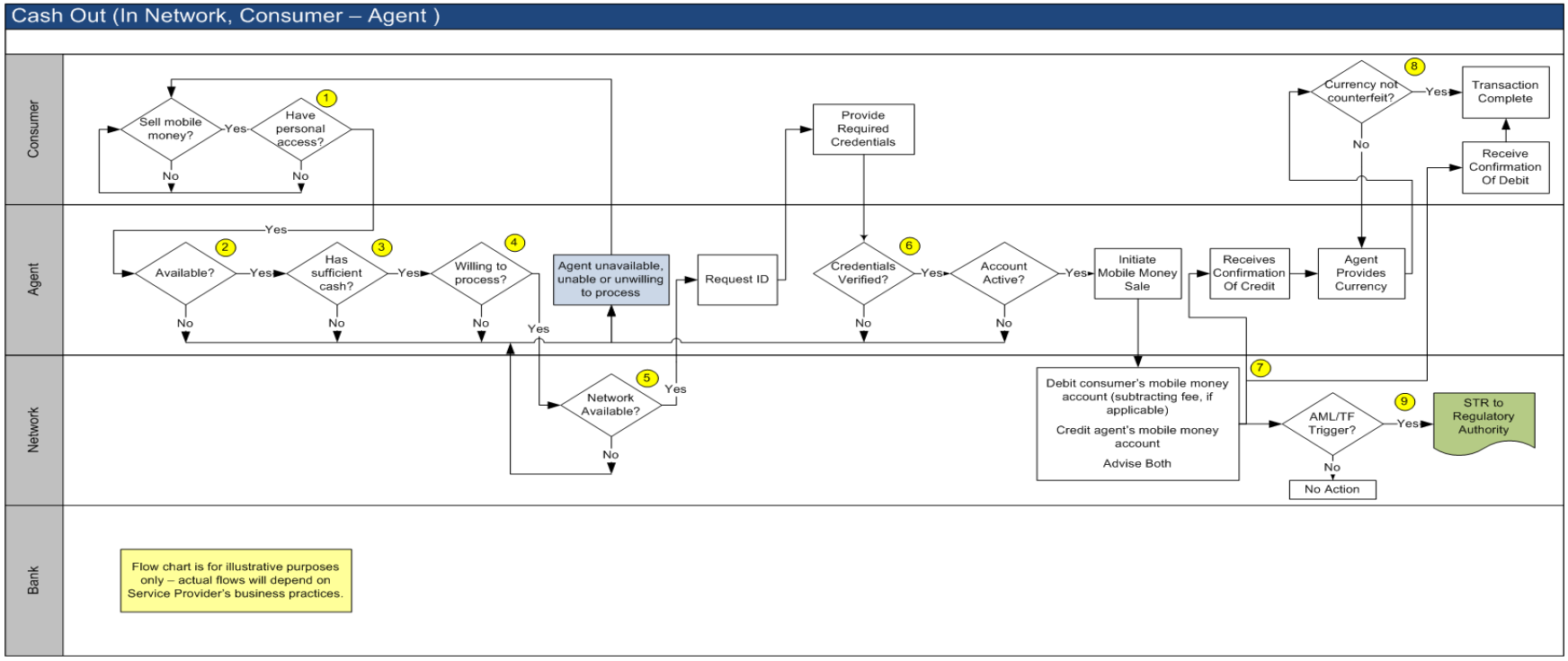
The Project Team Produced Several Representative Payment Transaction Flows Integrating the Risk Analysis



Comments

- *We conducted transaction flow mapping, highlighting where risks occur and how these differ depending on the service model*
- *Flow charts are representative, since each account provider will have its own business model*
- *Options found for each risk are not necessarily mutually exclusive, since more than one policy option may be appropriate*

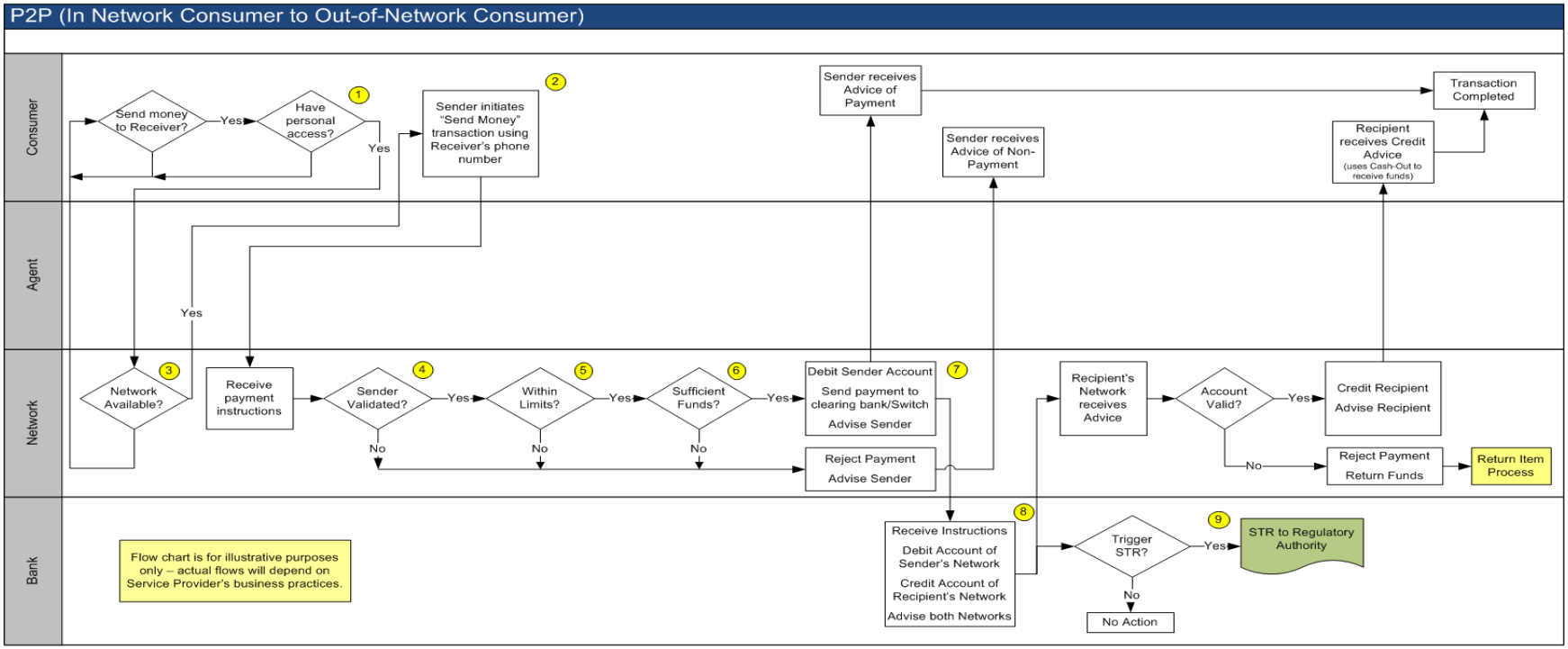
Cash-Out (Consumer – Agent)



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. 1.9/4.4/4.7/5.2/5.3 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.
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.

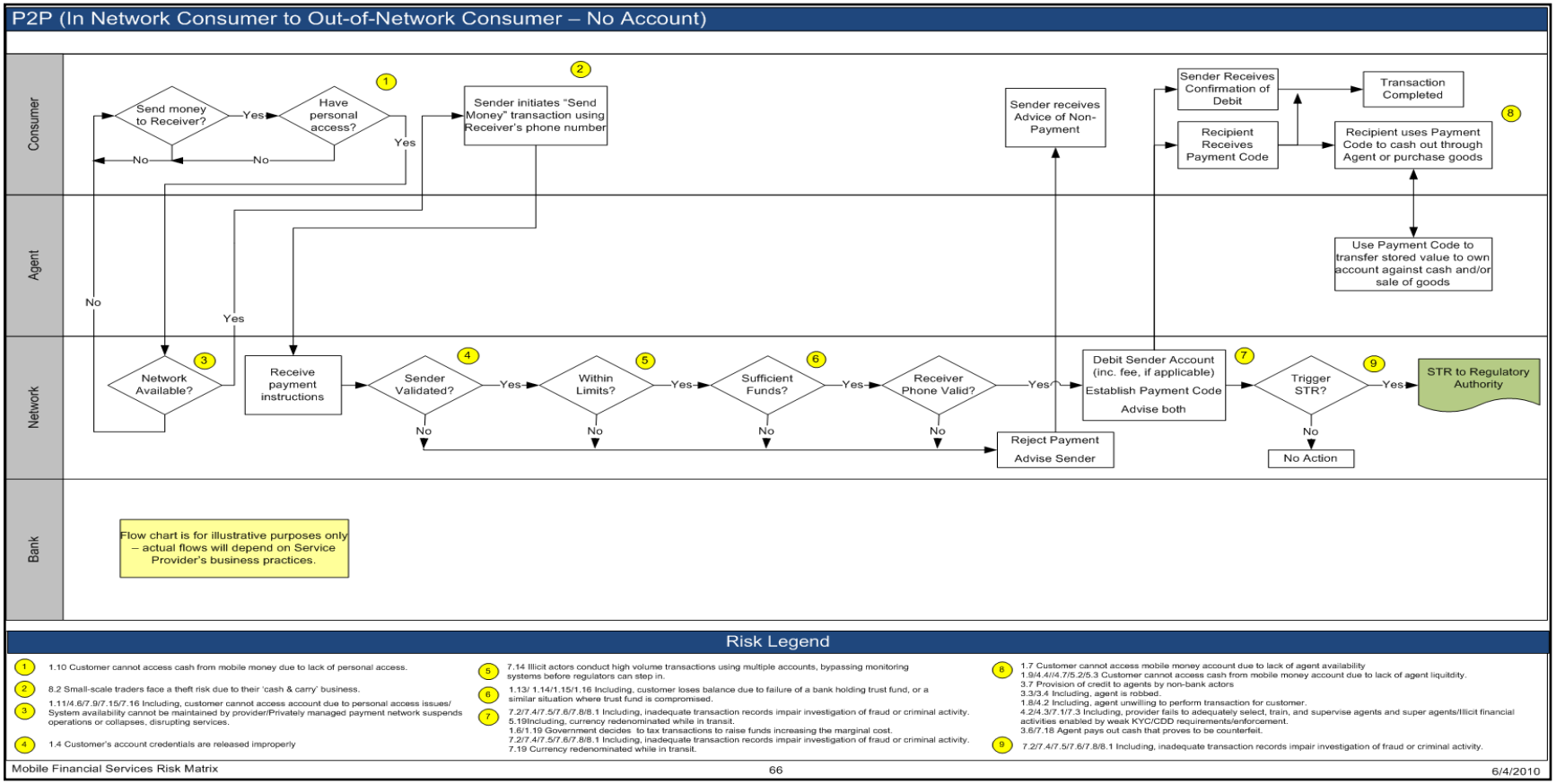
P2P (In Network Consumer to Out-of-Network Consumer)



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 (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.

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.

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.

Appendix - continued

- **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).

Appendix - continued

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…
- **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 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.
- **Pakistan:** 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. …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.

Table of Contents

Policy and Regulatory Considerations

- Economic development impact of supporting MMT services
- Creating a safe environment to encourage sustained client uptake (focus on application of HACCP model)
- Defining appropriate roles for donors in supporting MMT services infrastructure development
- Establishing client protection principles and standards for MMT services

Focus on Creating a Safe Environment in Which to Encourage Sustained Client Uptake

- Hazard Analysis and Critical Control Point (HACCP) system is a management system focused on prevention of problems in order to assure the production of food products that are safe to consume.

- A similar risk-based approach should be developed to assure that MMT services, particularly within a cross-border context, are safe to undertake.

Application of HACCP Principles to MMT Services

- Principle 1: Conduct a hazard analysis.
- Principle 2: Determine the critical control points (CCPs).
- Principle 3: Establish critical limits.
- Principle 4: Establish monitoring procedures.
- Principle 5: Establish corrective actions.
- Principle 6: Establish verification procedures.
- Principle 7: Establish record-keeping and documentation procedures.

- A complete HACCP analysis assumes that a pre-established set of standards exists against which analysis can be made. Such standards do not currently exist within the MMT services industry.

From *HACCP: A Systematic Approach to Food Safety. A Comprehensive Manual for Developing and Implementing a Hazard Analysis and Critical Control Point Plan. (NFPA, 1999)*

Table of Contents

Summary (with recommendations)

- Previous financial crises provide valuable lessons related to risk that can be applied to nascent MMT services sector.
- MNOs need to be monitored as if they are an actual component of the financial and banking system.
- No actor within the MMT services ecosystem should be permitted to grow “too big to fail.”
- Develop risk-based standards and guidelines similar to HACCP approach.
- Support proactive interaction between MNO, regulators, and other actors within MMT services ecosystem.

Question to Ponder…

- "Because financial markets do not tend towards equilibrium they cannot be left to their own devices. Periodic crises bring forth regulatory reforms. That is how central banking and the regulation of financial markets have evolved." (Soros 2009)

- If mobile financial technology services are borderless, how will they function within this context?

Thank You

Maria C. Stephens

Senior Technical Advisor

U.S. Agency for International Development

Office 202-219-0257

mstephens@afr-sd.org

Lisa C. Dawson

Associate - Booz | Allen | Hamilton

Center for Financial Intelligence

Office 703-377-8837

Dawson_Lisa@BAH.com