A Risk-Based Approach to Regulatory Policy and Mobile Financial Services

Federal Reserve Bank of Atlanta, Americas Center

Maria C. Stephens
Senior Technical Advisor
USAID/EGAT/PR/MD

Lisa C. Dawson
Lead Associate
Booz Allen Hamilton

Miami, Florida
May 4, 2011
Agenda

- Introduction – Current Regulatory Outlook
- USAID and Mobile Financial Services
- Mobile Financial Services Risk Matrix – Introduction
- Mobile Financial Services Risk Matrix – Operations
- Current Research and Relevance to USAID M-Money Initiatives
- Questions - Contact Information
Introduction: Current Regulatory Perceptions

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

- “Is the stored value money?” or “Is the stored value (and associated payment capability) a service?” Is the stored value a deposit?

- “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
Agenda

- Introduction – Current Regulatory Outlook
- USAID and Mobile Financial Services
- Mobile Financial Services Risk Matrix – Introduction
- Mobile Financial Services Risk Matrix – Operations
- Current Research and Relevance to USAID M-Money Initiatives
- Questions - Contact Information
Mobile Financial Services (MFS) and Development Opportunities

• Within a stable policy environment, there are potentially many development opportunities:
  
• Less expensive
  ✓ remittance flows
  ✓ payment solutions for government and others with large, disperse payrolls (e.g. agricultural outgrowers)
  ✓ operations structures for MFIs (mobile loan payment and disbursal—though harder for group loans)
  ✓ operations for voucher schemes

• Lower transaction costs for general economic activity, including domestic and international small scale trade

• Greater ability to identify and develop countermeasures for illicit and rent-seeking financial activities and increased security from getting money “off of the battlefield.”
Risk-based Focus Underpinning USAID’s MFS Involvement

USAID shares with other USG entities the responsibility to ensure both national and cross-border payments systems soundness alongside the expansive growth of the use of m-money:

- Unintended benefit of increasing public involvement in the formal financial system, including expansion of savings accounts in regulated financial institutions;
- Conversion of widely distributed consumer risk into a concentrated systemic risk where the value of the funds in transit and held in trustee accounts is no longer insignificant;
- Need to balance assurance of enabling environment conducive to innovation and economic growth alongside consumer protection;
- Lack of global standards → proliferation of inconsistent operating environments for account providers and, in some cases, limitations on range of services based on non risk-based factors.
Agenda

- Introduction – Current Regulatory Outlook
- USAID and Mobile Financial Services
  - Mobile Financial Services Risk Matrix – Introduction
  - Mobile Financial Services Risk Matrix – Operations
- Current Research and Relevance to USAID M-Money Initiatives
- Questions - Contact Information
USAID Project: Mobile Financial Services Risk Analysis

As part of G-20 Financial Inclusion Experts Group objective, USAID/EG identifies and develops the opportunities that the innovation of mobile payments presents for emerging markets. Specifically, USAID assists 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
- MD provided technical input to project and brought in FRB/Atlanta expertise to project
- EG’s two-year program partnered with experts from Booz Allen-Hamilton, in consultation with Kenya School of Monetary Studies and the Central Bank of Kenya
Initial project scope and analysis was Africa – centric

• Ongoing discussion with stakeholders indicates broad ranging applicability of the Matrix

• In many other countries, regulators balance the assurance of an enabling environment 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 limitations on the range of services provided based on factors other than the underlying risks
Agenda

- Introduction – Current Regulatory Outlook
- USAID and Mobile Financial Services
- Mobile Financial Services Risk Matrix – Introduction
  - Mobile Financial Services Risk Matrix – Operations
- Current Research and Relevance to USAID M-Money Initiatives
- Questions - Contact Information
The Matrix Identifies Risk Categorized by Stakeholder Group

Our team of experts, working in concert with USAID and the Kenya School of Monetary Studies, developed 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.
- An Appendix of detailed market examples inform policymakers.
## Mobile Financial Services – Operating Models

<table>
<thead>
<tr>
<th>Operating Model</th>
<th>Observations</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank</td>
<td>Primarily an additive model linked to an existing transactional account (e.g., debit card)</td>
<td><img src="image" alt="NMB" /> <img src="image" alt="EQUITY" /> <img src="image" alt="easypay" /></td>
</tr>
<tr>
<td>Mobile Network Operator (MNO)</td>
<td>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.</td>
<td><img src="image" alt="MPESA" /> <img src="image" alt="Zap" /> <img src="image" alt="Pesa Mkrokeni" /></td>
</tr>
<tr>
<td>Hybrid Model</td>
<td>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.</td>
<td><img src="image" alt="M-KESHO" /> <img src="image" alt="EQUITY" /> <img src="image" alt="Safaricom" /></td>
</tr>
</tbody>
</table>
Model Identification

Countries of Models Identified

Research Observations

- Extension of credit to agents by non-bank actors to meet liquidity needs of the agents;
- Group ownership of individual accounts;
- Issues of beneficial ownership and access to credit;
- Cross border value transfers
Mobile Financial Services – Risk Definitions

• **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

• **Reputational:** 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 mobile financial services (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
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

*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.
Example of laundering counterfeit currency via MFS

Fraudster with counterfeit currency

Purchases minutes from Mobile Network Operator (MNO) Agent using counterfeit currency

Transfer minutes to fraudsters mobile phone via the mobile carrier system

Fraudsters receives the amount and cashed out clean money or utilizes minutes

MNO Agent
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 be 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.
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.
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 – In Network, Consumer – MNO Agent

1. Consumer
   - Sell mobile money?
   - Have personal access?

2. Agent
   - Available?
   - Has sufficient cash?

3. willingness to process?
   - Agent available, enable or unwilling to process?

4. Request ID
   - Credentials verified?

5. Network Available?

6. Bank

Flow chart is for illustrative purposes only – actual flows will depend on Service Provider’s business practices.

Risk Legend

1. Customer cannot access cash from mobile money account due to lack of personal access.
2. Agent unable to process transaction due to lack of agent availability.
3. Customer cannot access cash from mobile money account due to lack of sufficient cash.
4. Agent unwilling to process transaction due to lack of willingness.
5. Network unavailable.

Mobile Financial Services Risk Matrix
P2P In Network to Out-of-Network Consumer - No Acct

P2P (In Network Consumer to Out-of-Network Consumer – No Account)

1. Consumer

1. Send money to Receiver? Yes

2. Have personal access? Yes

2. Send initiates "Send Money" transaction using Receiver's phone number

3. Sender Receives Advice of Non-Payment

4. Transaction Completed

5. Recipient uses Payment Code to cash out through Agent or purchase goods

6. Use Payment Code to transfer stored value to own account against cash and/or sale of goods

7. Trigger STR?

8. Yes STR to Regulatory Authority

9. No No Action

Agent

1. Network Available?

2. Receive payment instructions

3. Sender Validated?

4. Yes

5. Within Limits?

6. Yes

7. Sufficient Funds?

8. Yes

9. Yes

10. Receiver Phone Valid?

11. Yes

12. No

13. No

14. No

15. No

16. No

17. No

18. No

19. No

20. No

21. No

22. No

23. No

24. No

25. No

26. No

Network

1. Yes

2. No

3. No

4. No

5. No

6. No

7. No

8. No

9. No

10. No

11. No

12. No

13. No

14. No

15. No

16. No

17. No

18. No

19. No

20. No

21. No

22. No

23. No

24. No

25. No

26. No

Bank

Flow chart is for illustrative purposes only. Actual flows will depend on Service Provider’s business practices.

Risk Legend

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Mobile Financial Services Risk Matrix

USAID: From the American People

Booz | Allen | Hamilton

6/4/2010
P2P (In Network Consumer to Out-of-Network Consumer – No Account)

Flow chart is for illustrative purposes only — actual flows will depend on Service Provider’s business practices.

**Risk Legend**
1. 10: Customer cannot access cash from mobile money account due to lack of personal access.
2. 2.3: Small-scale traders face theft risk due to their ‘cash & carry’ business.
3. 1.14: $75/77/157/16 including, customer cannot access account due to personal access issues.
4. System scalability cannot be maintained by providers without managed payment network services operations or collapses, disrupting services.
5. 1.4: Customer’s account credentials are released improperly.
6. 7.14: Implement options such as transactions using multiple accounts, bypassing money transfer service before regulations on step-in.
7. 1.13: 1.14/1.15/16 including, customer loses balance due to failure of a bank holding trust fund or a similar instrument where trust fund is compromised.
8. 1.21: 4/7/78/16 inclusive, inadequate transaction records impair investigation of fraud or criminal activity.
9. 1.26: 4/7/78/16 inclusive, inadequate transaction records impair investigation of fraud or criminal activity.
10. 1.27: 7/17/17/18/19 inclusive, inadequate transaction records impair investigation of fraud or criminal activity.
11. 1.28: 7/17/17/18/19 inclusive, inadequate transaction records impair investigation of fraud or criminal activity.
12. 2.7: Provision of credit to agents by non-bank entities.
13. 2.9: 417/418/78/79 inclusive, inadequately-determined agent’s account number.
14. 6.1: 4/7/78/16 inclusive, agent unable to perform transactions for customer.
15. 7.28: 7/1/78/16 inclusive, provider fails to adequately vetted, and super-sede agents and super agents to cut financial network services operations.
16. 7.29: 7/1/78/16 inclusive, inadequate transaction records impair investigation of fraud or criminal activity.
17. 2.37: 7/1/78/16/17 inclusive, inadequate transaction records impair investigation of fraud or criminal activity.

Mobile Financial Services Risk Matrix

Booz | Allen | Hamilton

66

6/4/2010
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:

<table>
<thead>
<tr>
<th>Options</th>
<th>Implications</th>
</tr>
</thead>
</table>
| 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 – Policy Narratives Expand Matrix Options

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:

- **Recommendation 29:** Compliance by financial institutions - 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.”

- **Recommendation 30:** Countries, as well, should both provide their competent authorities involved in Anti Money Laundering (AML) and Combating the Financing of Terrorism (CFT) with sufficient “financial, human, and technical resources”

- **Recommendation 31:** Countries should ensure that “policy makers, the FIU, law enforcement and supervisors” can effectively and efficiently develop and implement AML and CFT policies
Appendix – Market Examples of MFS Implementation

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 Laundering 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.
Agenda

- Introduction – Current Regulatory Outlook
- USAID and Mobile Financial Services
- Mobile Financial Services Risk Matrix – Introduction
- Mobile Financial Services Risk Matrix – Operations
- Current Research and Relevance to USAID M-Money Initiatives
- Questions - Contact Information
Current Research & Relevance to USAID Programming

- “Creating A Living Document” out of the risk matrix
- Cloud computing risk research: Service Level Agreements
- Developing industry MFS norms, standards, guidelines
- Internal controls & risk mitigation: Cloud computing, stress tests
- Consumer Financial Protection initiatives
- Policy papers, collaboration and subject matter expertise
How will USAID partner effectively with State (Citibank, Cisco), partner country regulators (Haiti, DRC), and US regulatory authorities (FRB, FDIC, Treasury, OCC, CFPB) to take advantage of these opportunities together?
Agenda

- Introduction – Current Regulatory Outlook
- USAID and Mobile Financial Services
- Mobile Financial Services Risk Matrix – Introduction
- Mobile Financial Services Risk Matrix – Operations
- Current Research and Relevance to USAID M-Money Initiatives
- Questions - Contact Information
Thank You

MATRIX:

Maria C. Stephens
Senior Technical Adviser-U.S. Agency for International Development
Bureau for Economic Growth, Agriculture and Trade
Office: (202) 712-1426
mstephens@usaid.gov

Lisa C. Dawson
Lead Associate - Booz Allen Hamilton
Financial Intelligence Center of Excellence
Office: +1 703-377-8837
Dawson Lisa@BAH.com