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

Maria Stephens
USAID/Senior Technical Advisor

Daryl Skoog
Opportunity International

Gino Picasso
GKN
AGENDA

- Introduction – Current Regulatory Outlook
- MFS and MMT 101 Mechanics
- Regulatory Context for MFI Uptake of MFS
- Mobile Financial Services Risk Matrix
- Back-office Capacity for MFI Uptake of MFS
- Outsourcing Options for MFIs
- Questions and Contact Information
Introduction: Current Regulatory Perceptions

- MFS comprise banking and telecom functions—Issue: “Is the stored value *money*?” or “Is the stored value (and associated payment capacity) a *service*?” Is the stored value a *deposit*? Who is primary regulatory—banking or telecom regulator?

- Development agenda -> unintended “benefit” of increasing public involvement in formal financial system; conversion of widely distributed consumer risk into concentrated systemic risk where value of funds *in transit* and *at rest (held in trust)* no longer insignificant.

- Lack of global standards -> proliferation of inconsistent operating environments and potential “weak points” in global financial system.

- Greater ability to identify and develop countermeasures for illicit and rent-seeking financial activities and increased security from “getting money off of the battlefield” are positive aspects; need to balance these with broader regulatory issues.
AGENDA

- Introduction – Current Regulatory Outlook

- MFS and MMT 101 Mechanics

- Regulatory Context for MFI Uptake of MFS

- Mobile Financial Services Risk Matrix

- Back-office Capacity for MFI Uptake of MFS

- Outsourcing Options for MFIs

- Questions and Contact Information
Mechanics of Mobile Money Transfers in MNO-led Model

- **Step 1**: An MNO retailer deposits real money funds into a pooled account held at the MNO partner bank.

- **Step 2**: The bank notifies the MNO of receipt of the funds and the MNO creates an equal amount of e-money which it then assigns to the merchant's mobile money account. The MNO retailer is now compensated for the funds it has surrendered to the bank.

- **Step 3**: Customers bring cash in to a retailer and exchange the case for an electronic or e-money equivalent, which the retailer transfers from his mobile money account (via SMS text message) to the customer's mobile phone. The customer is now compensated for the funds he has surrendered to the retailer (Zerzan 2010).
Mechanics of MMT in MNO-led model

The cash in the pooled bank account exactly matches the sum of all the e-money accounts in the system.

- The MNO opens an e-money (or “mobile money”) account for the retailer.
- An MNO retailer deposits funds into the pooled account at the MNO-partnered bank.
- The bank notifies the MNO and the MNO creates e-money, assigning it to the merchant’s mobile money account.

Customers bring cash to a retailer; the retailer takes the cash and transfers e-money from his mobile money account to the customer’s. The customer is now compensated.

(Slide courtesy of Andrew Zerzan)
Mobile Money Transactions “Live”

- Here are some examples of how MMT works, both in a MNO- and bank-led model environment: [http://www.youtube/watch?v=nEZ30K5dBWU](http://www.youtube/watch?v=nEZ30K5dBWU).

- The following three videos describe the MNO-led M-Pesa model found in Kenya.
  - [http://www.youtube.com/watch?v=Qj_UrRRkUyU&NR=1](http://www.youtube.com/watch?v=Qj_UrRRkUyU&NR=1)
  - [http://www.youtube.com/watch?v=h0Zq1cRRT1keature=relatded](http://www.youtube.com/watch?v=h0Zq1cRRT1keature=relatded)
  - [http://microlinks.kdid.org/library/g-cash-rbap-mabs-electronic-wallet](http://microlinks.kdid.org/library/g-cash-rbap-mabs-electronic-wallet). (This video shows the mechanics of the bank-led (USAID-supported) rural MABS MMT model in the Philippines.)
AGENDA

- Introduction – Current Regulatory Outlook
- MFS and MMT 101 Mechanics
- Regulatory Context for MFI Uptake of MFS
- Mobile Financial Services Risk Matrix
- Back-office Capacity for MFI Uptake of MFS
- Outsourcing Options
- Questions and Contact Information
Regulatory Context for MFI Uptake of MFS

- MFIs bear direct and contingent liabilities for any illicit funds flowing through their payments “pipes,” including within a third-party outsource construct: **Know Your Partners**

- Within a stable policy environment, there are potentially many development opportunities:
  - Lower transaction cost
  - More efficient remittance flows
  - More efficient payment solutions for government and others with large, disperse payrolls (e.g. agricultural out growers)
  - Lower cost operations structures for MFIs (mobile disbursal and payment-though harder for groups)
  - operations for voucher schemes

- Just as all politics are local, all regulations are local: **Know Your Regulations**

- Tech associated with MFS is fast-evolving and complex, as are CP issues re to MFS

- What is an MFIs comparative advantage in any MFS partnership construct?
Regulatory Issues Related to MFI Uptake of MFS/MMT

- Evidence of lack of capacity (human, technological, regulatory and enforcement) to monitor and supervise national MFS sectors, including client protection

- SaaS customers lack sophistication re the risks associated with reliance on cloud-based services provided by third parties

- Some governments have begun to exploit Internet and other technologies inherent within the MFS ecosystem as a way to repress dissent

- Risk- vs. rules-based legal systems may determine the extent to which MFS can be undertaken within various countries (French legal code vs. British common law).

- Lack of a coordinated global approach toward MFS could expose “weak points” through which illicit funds can flow from the informal economies to the formal economies (and vice versa)
Regulatory Issues Related to MFI Uptake of MFS/MMT

• An increasing number of emerging mobile phone-based payment systems rely upon outsourced Internet-based services for IT infrastructure maintaining accounts.

• The growing prevalence of such solutions introduces risks brought on by Internet or data center interruption; data access compromise; and/or business failure.

• Limited awareness that SaaS providers are often themselves outsourcing; limited warranties in contracts with Saas providers, in particular liability for data loss or service interruptions (ex: Amazon’s 4/2011 platform crash)

• No clear plans for unwinding claims of mobile money account holders if service provider who operates the system were to be dissolved or forced into bankruptcy.

• SLAs typically don’t identify these risk points, leaving parties to contracts (including donors) exposed to tech-based risks that may not be resolvable across jurisdictions
AGENDA

- Introduction – Current Regulatory Outlook
- MFS and MMT 101 Mechanics
- Regulatory Context for MFI Uptake of MFS
- Mobile Financial Services Risk Matrix
- Back-office Capacity for MFI Uptake of MFS
- Outsourcing Options
- Questions and Contact Information
Project Motivation


- During the assessment, the opportunity for financial inclusion that mobile financial services opened was highlighted; however, the lack of regulatory infrastructure and competition was noted as a concern for long-term viability.

- A recommendation was made to promote four goals:
  - Limit systemic risk
  - Increase competition
  - Promote interoperability across providers
  - Promote interoperability across borders

- The 1st step was to be a white paper that considered the risks associated with MFS, looking not only at Kenya but other markets with different experiences.
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
A core team of BAH and USAID technical experts worked 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.

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" /></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="Equity" />, <img src="image" alt="Safaricom" /></td>
</tr>
</tbody>
</table>
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

See a global map of MFS deployments at:
http://www.wirelessintelligence.com/mobile-money
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 effect.

- **Contingent liability**: US companies/persons must comply with OFAC standards, and are liable for any actions undertaken within any outsourcing context.
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.
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

1. Fraudster with counterfeit currency
2. Purchases minutes from Mobile Network Operator (MNO) Agent using counterfeit currency
3. Transfer minutes to fraudsters mobile phone via the mobile carrier system
4. Fraudsters receive the amount and cashed out clean money or utilizes minutes

(Slide courtesy of Lisa Dawson, BAH)
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.*
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.
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. *
Cloud-based Platform Services Ecosystem
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 suggests various policy options and associated implications to help guide policymakers (these are not exhaustive).

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.

Given the variances in risk, and capacity, across countries, we do not put forth a recommendation.
We developed transaction flows, highlighting where the 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

**Cash Out (In Network, Consumer – Agent)**

**Consumer**
- **Have personal access?**
  - Yes
  - No

**Agent**
- **Available?**
  - Yes
  - No

**Network**
- **Network Available?**
  - Yes
  - 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 account due to lack of personal access.
2. Customer cannot access cash from mobile money account due to lack of agent availability.
3. Customer cannot access cash from mobile money account due to lack of agent liquidity in mobile money.
4. Customer cannot access cash from mobile money due to lack of service viability.
5. Customer cannot access cash from mobile money due to lack of service viability.
6. Customer cannot access cash from mobile money due to lack of service viability.
7. Customer cannot access cash from mobile money due to lack of service viability.
8. Customer cannot access cash from mobile money due to lack of service viability.
9. Customer cannot access cash from mobile money due to lack of service viability.
10. Customer cannot access cash from mobile money due to lack of service viability.
11. Customer cannot access cash from mobile money due to lack of service viability.
12. Customer cannot access cash from mobile money due to lack of service viability.
13. Customer cannot access cash from mobile money due to lack of service viability.
14. Customer cannot access cash from mobile money due to lack of service viability.
15. Customer cannot access cash from mobile money due to lack of service viability.
16. Customer cannot access cash from mobile money due to lack of service viability.
17. Customer cannot access cash from mobile money due to lack of service viability.
18. Customer cannot access cash from mobile money due to lack of service viability.
P2P In Network to Out-of-Network Consumer - No Acct

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

1. **Consumer**
   - **Sender initiates “Send Money” transaction using Receiver’s phone number**
   - **Sender receives Advice of Non-Payment**
   - **Transaction Completed**

2. **Agent**
   - **Recipient receives Payment Code to cash out through Agent or purchase goods**

3. **Network**
   - **Use Payment Code to transfer stored value to own account against cash and/or sale of goods**

4. **Bank**
   - **Network Available?**
   - **Send money to Receiver?**
   - **Have personal access?**

   - **Sender validated?**
   - **Within Limits?**
   - **Sufficient Funds?**
   - **Receiver validates?**
   - **Reject Payment Advise Sender**

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

**Risk Legend**

1. **1-3** Customer cannot access cash from mobile money due to lack of personal access.
2. **4-6** Small-scale mobile money is a threat due to their "cash & carry" business.
3. **7-9** Mobile money transactions are not regulated by existing financial laws.
4. **10** Mobile money clients may be vulnerable to fraud.

**Mobile Financial Services Risk Matrix**

66

6/4/2010
Appendix – Policy Table Expands Matrix Implications

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 upon 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 “authorized 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 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.
AGENDA

- Introduction – Current Regulatory Outlook
- MFS and MMT 101 Mechanics
- Regulatory Context for MFI Uptake of MFS
- Mobile Financial Services Risk Matrix
- Back-office Capacity for MFI Uptake of MFS
- Outsourcing Options
- Questions and Contact Information
Why go Mobile?

What are your Reasons?

- Better/more efficient Service?
- Better profits?
- Safety/Access of funds?
- Relevance in the Marketplace?
- Scalability?
- Competitive Advantage/first mover?
Policy Considerations

Business Policy

- Who Owns the customer problems?
- Is the MNO providing a channel or product?
- When does the business day end?

Agent network, Build or Join?

What Services will be provided?

How should the customer be educated and enticed?
Technology Platform

Portfolio System Capabilities

Electronic Interconnect with External Systems?
- Manual or electronic transactions
- Reconciliations
- Audit trails

7 x 24 Business transaction handling?
Enterprise Customer DB or Branch level?
Close of Business Handling?
Customer Education

Customer Preparedness

- Who do they trust?
- What other ways do they interact with you?
- How will product be introduced?
- What are the customer incentives to change?
- How will customers learn how to interact?
- When things go wrong, then what?
AGENDA

- Introduction – Current Regulatory Outlook
- MFS and MMT 101 Mechanics
- Regulatory Context for MFI Uptake of MFS
- Mobile Financial Services Risk Matrix
- Back-office Capacity for MFI Uptake of MFS
- Outsourcing Options
- Questions and Contact Information
Canales de Acceso a Productos Bancarios

PRODUCTOS

- CUENTAS CORrientes
- CREDITOS
- CUENTAS BASICAS
- CUENTAS CELULARES
- MONEDERO ELECTRONICO
- TARJETA REGALO

MEDIOS DE ACCESO

- TELLER
- ATM
- INTERNET
- POS/TARJETA
- MOVIL (PAC y otros)
The Problem

The Poor Need And Use Financial Services

Inaccessible

Cumbersome

Dangerous

Inconvenient

Payments done at bank
Agente Corresponsal
Observation

Goods and Cash Find their Way to Almost Every Community
Solution: Leverage what exists

GKN leverages mom and pop shops to perform cash-in/cash-out service, aka, Correspondent Agent Banking

KasNet Processes Electronic Transactions

Capture
Agentes KasNet
KasMovi

Transmit
Transmission Network

Process
Globokas Switch

Financial Institutions, Insurance Companies
Gov’t & NGO’s
Other Enterprises

Agent Converts Cash to/from E-Cash

Customer Account
Institutional Account
KasNet Agent Account
Agent Banking as an outsourced service to Banks, MFIs, *Telcos*, Enterprises, Government Agencies

Shared platform (i.e., multibank) to ensure lowest cost, widest availability

Lower barriers to entry

Focus and specialization
Compelling Value Proposition
$3-5  Vs. <$1

**Economic Drivers**

### Consumer
- Transport: $2
- Time: 1-3 hrs
- Transaction fee: $0.25

### Bank
- Teller Transaction Cost: $1-2.50
- Collection fee: $0.25
- Less: Chargeback: $.40

### GKN
$0.25-1.00 All In

Source: GKN estimates based on average drive time and cost of transportation
GKN’s Solution

Our Services Make It Possible To Serve the Poor Well, Economically

Accessible

Easy

Safe

Convenient

Branch in village

Pay at local store

mobile banking
Correspondent Banking Agents Handled 10% of All Banking Transactions in Peru in 2009
Agents are quick to sign up
Small % of agents equipped to be a “teller”
Agent commitment dependent on “skin in the game”
Agents can be ‘evangelizers’
Communities differ widely
People from the community drive success
Need Is Nearly Universal

- Only one bank with more than 100,000 customers enough to get started
- Per country break-even achievable with only 65K active customers
- Platform easily replicable – no need for significant investment until first customer signed
Visit Microlinks to access resources from USAID’s Mobile Financial Services Seminar Series

Join the upcoming Speakers Corner online discussion on November 29 – December 1
“Mobile Financial Services: Balancing Regulatory Risks and Financial Inclusion Opportunities”
Thank You

MATRIX:


Maria Stephens
USAID/Senior Technical Advisor

Daryl Skoog
Opportunity International

Gino Picasso
GKN