Mobile Payments in Other Markets – Emerging Regulatory Frameworks

Ms. Maria Stephens, U.S. Agency for International Development, Washington, D.C.

Hyperlink to:
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

http://bizclir.com/galleries/publications/Mobile%20Financial%20Services%20Risk%20Matrix%20July%202010.pdf

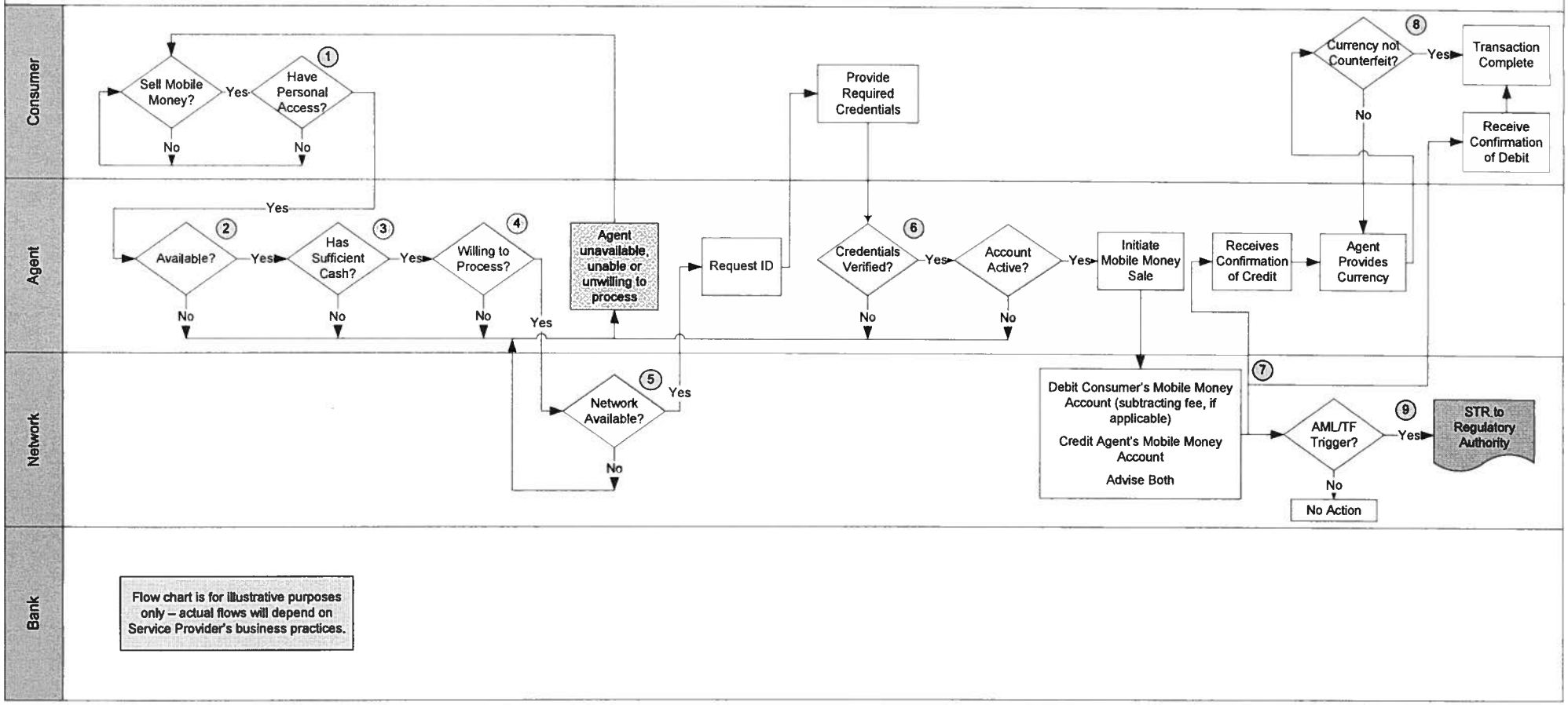
Hyperlink to:
Mobile Money Transfer Services: The Next Phase in the Evolution in Person-to-Person Payments, by Cynthia Merritt, Retail Payments Risk Forum White Paper, Federal Reserve Bank of Atlanta; August 2010

http://www.frbatlanta.org/documents/rprf/rprf_resources/wp_0810.pdf

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									

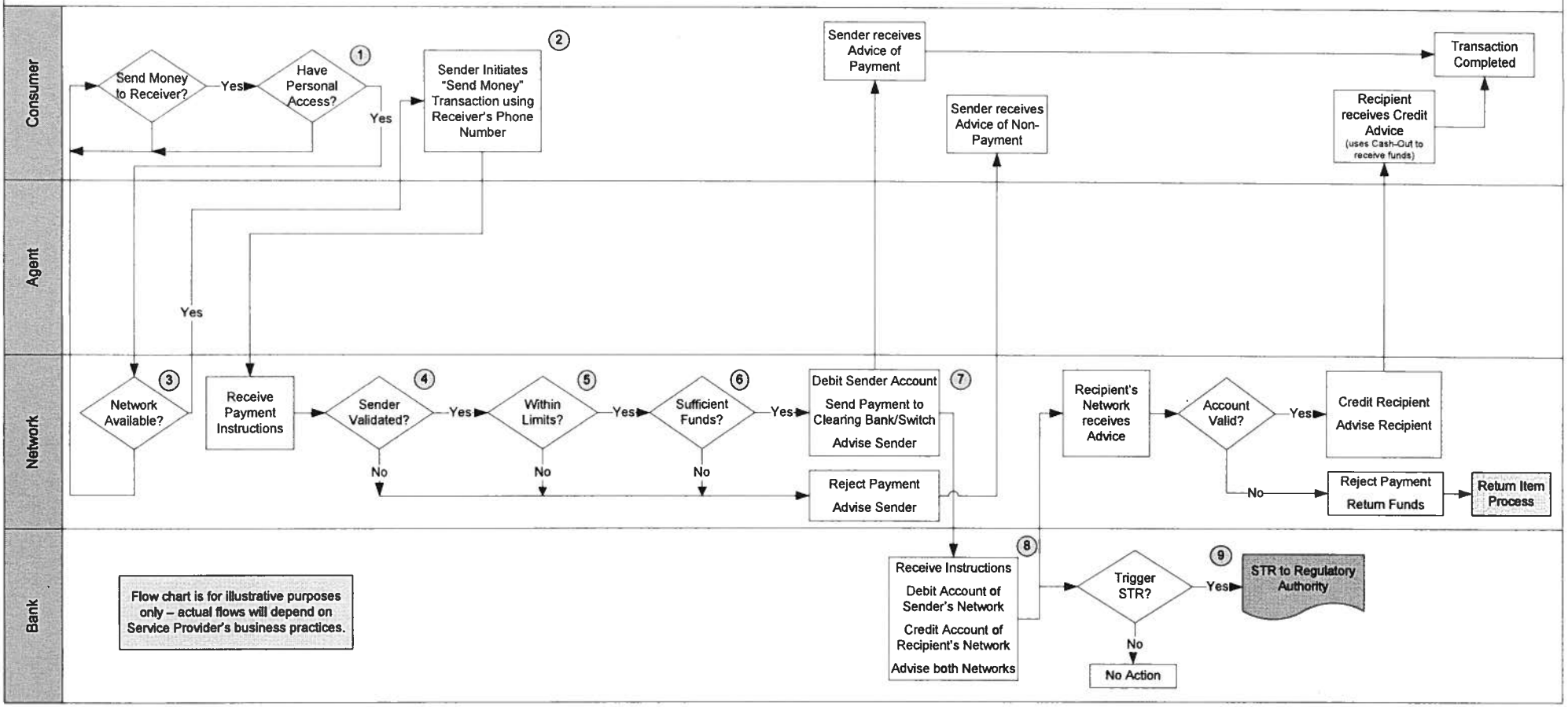
Cash Out – MNO Model



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.

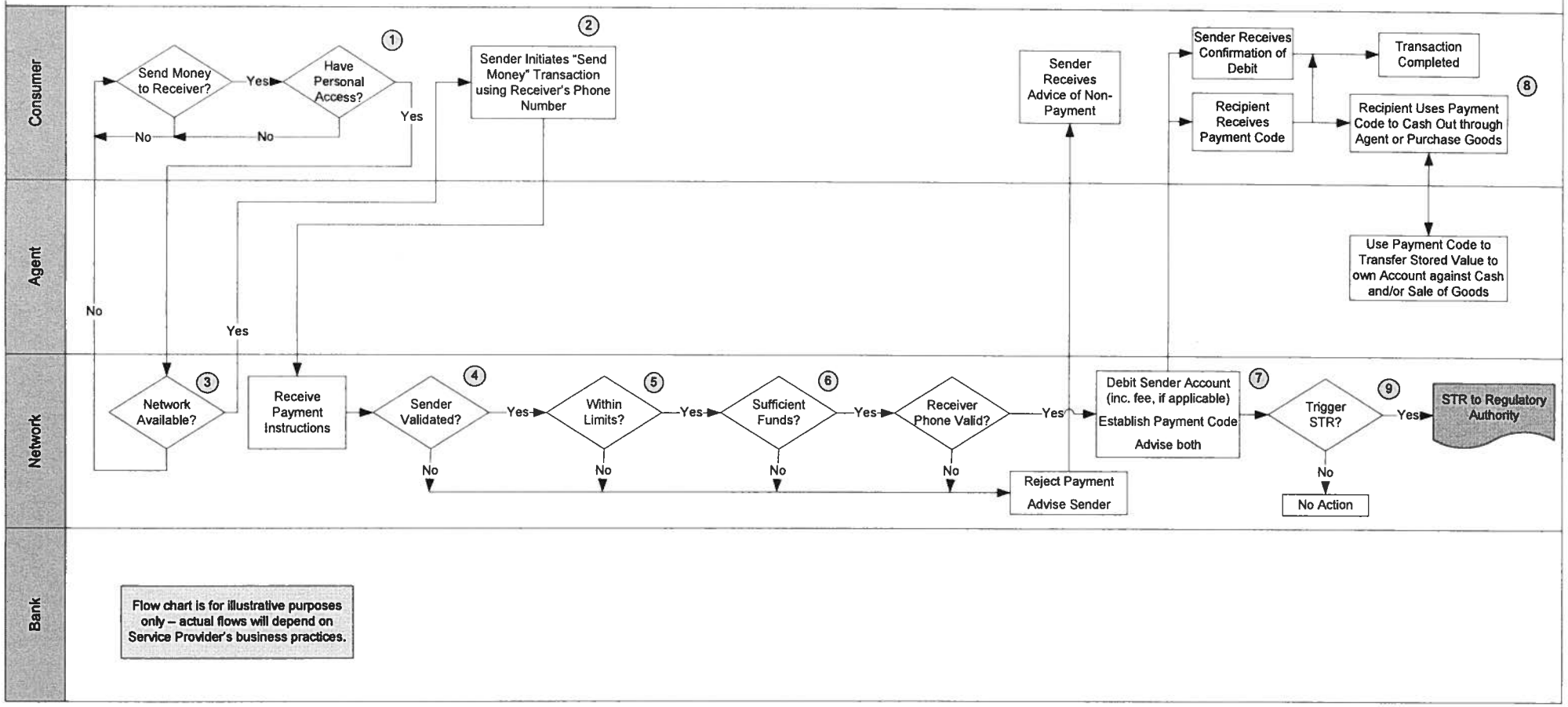
P2P – MNO Model, In Network Consumer to Out-of-Network Consumer



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.

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