![USAID - From the American People logo]

September 16, 2011

Cloud Computing and Financial Services for The Poor:
Promise and Perils of a New Computing Paradigm

Bryan Barnett
Independent Consultant

Maria Stephens
USAID

Cloud Computing and Financial Services for The Poor:
Promise and Perils of a
New Computing Paradigm

Bryan Barnett, Ph.D.
bryan@4barnetts.com

Agenda

- Origins & Essential Characteristics

- Economic Drivers & Value Chains

- Microfinance and Mobile Payments

- Risks & Mitigation

Software-as-a-Service (SaaS)

▸ Applications offered & accessed over the Internet

▸ Free, subscription, or usage fee

▸ Application provider hosts software and data

▸ Examples
  ▸ Google Search, Ebay
  ▸ Quicken (Mint), NetSuite
  ▸ SalesForce
  ▸ Project Neon (architectural rendering)
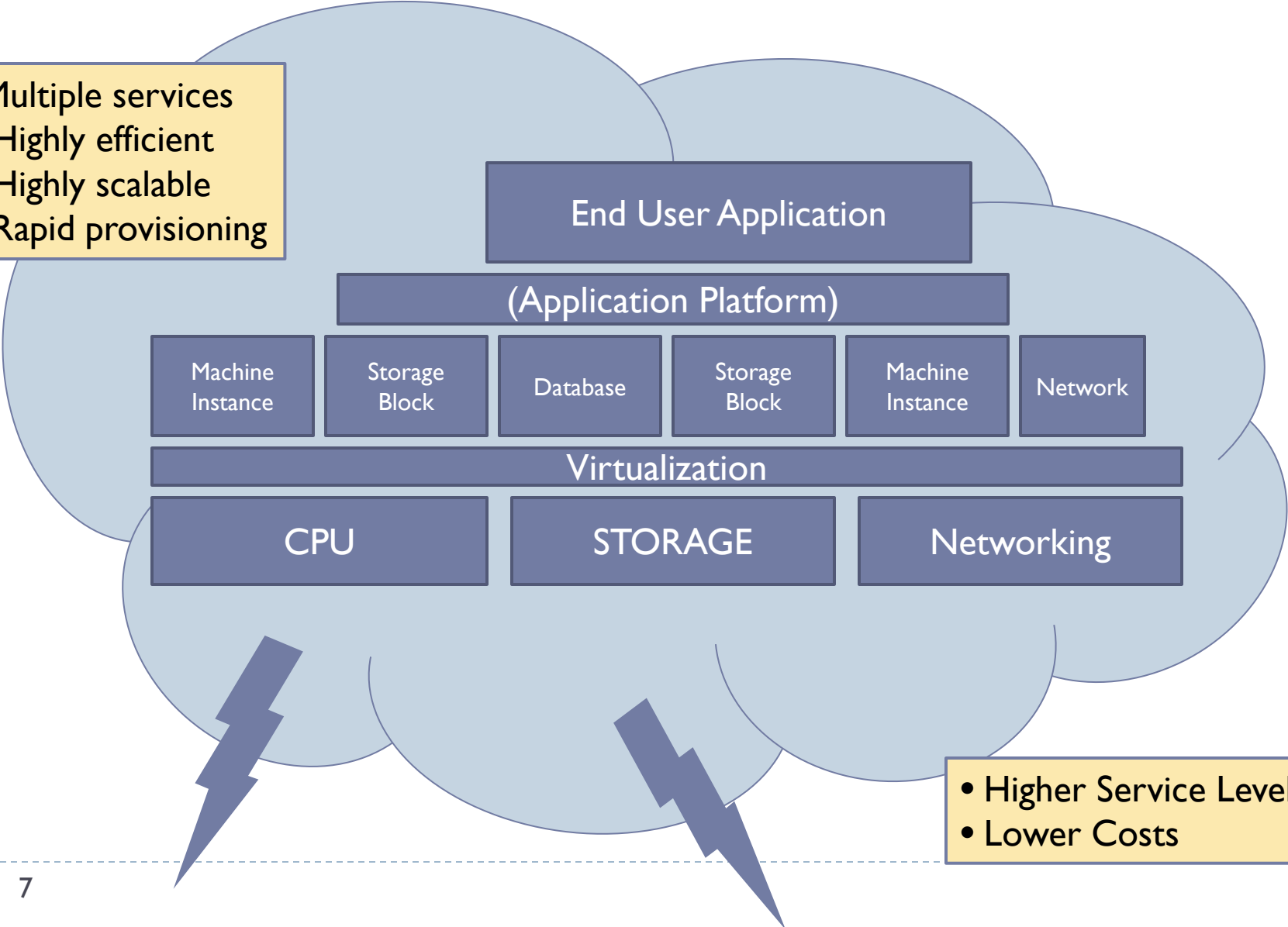
▸ Caveat: SaaS ≠ Cloud

Behind SaaS: a Brief History

Three Flavors of SaaS

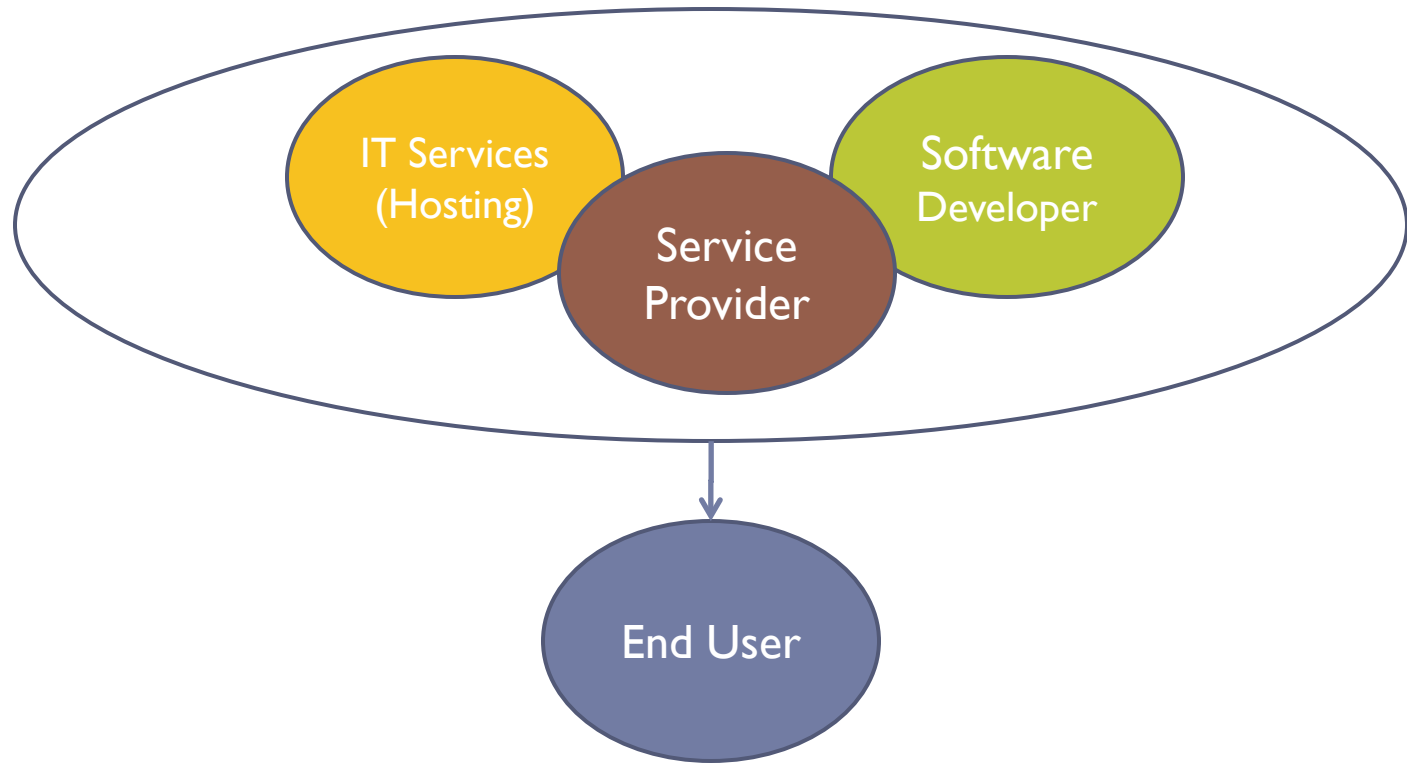|	On Premise	Co-Location	Public Cloud
Who owns & controls the data center facility?	End user	Independent data center operator	IT service provider
Who owns and controls machines within the data center?	End user	End users	IT service provider
How are computing resources within the data center allocated?	Dedicated or Pooled (private cloud)	Dedicated	Pooled

Pooled Resources Define the True Cloud

- Multiple services
- Highly efficient
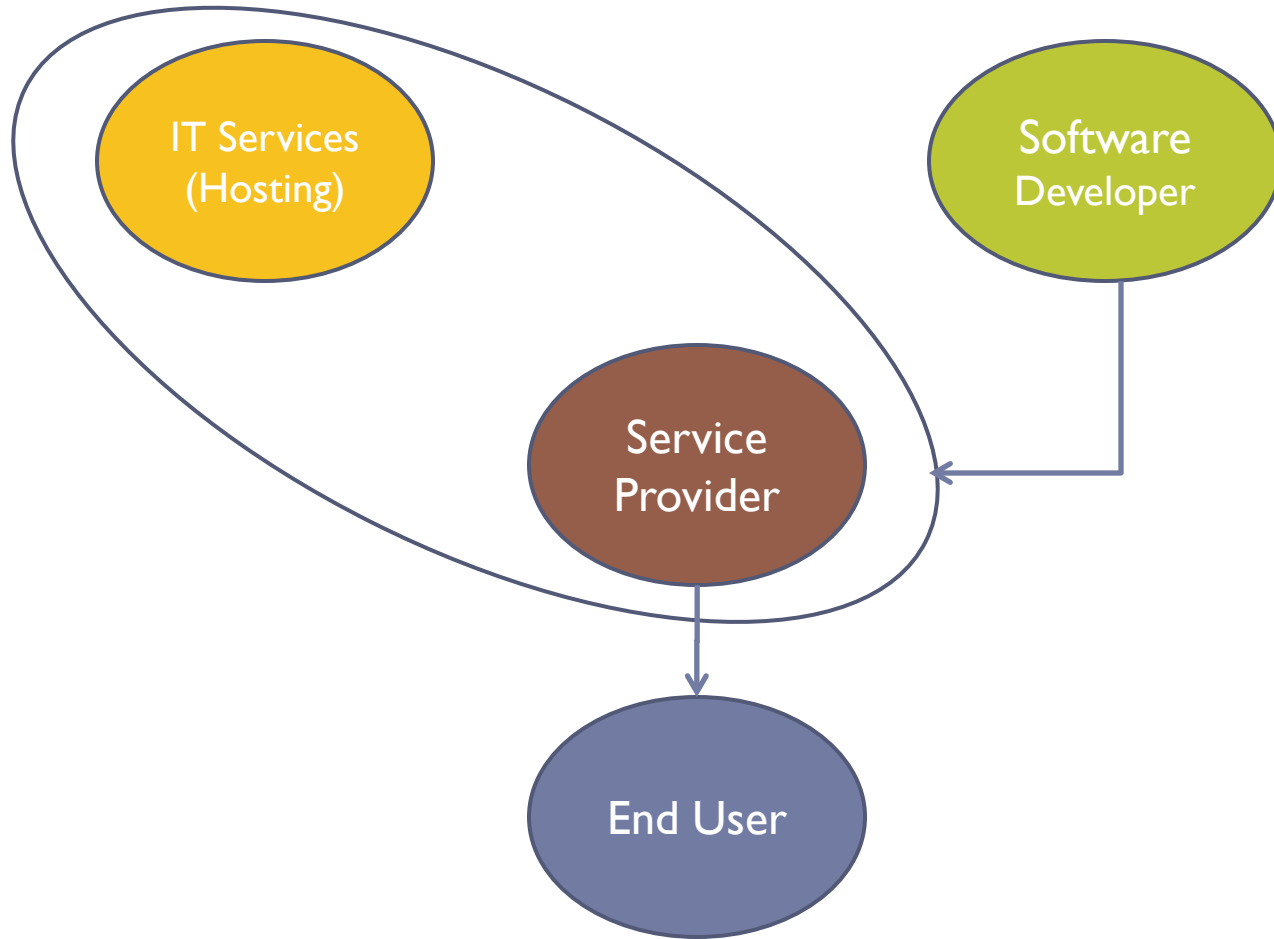- Highly scalable
- Rapid provisioning

End User Application
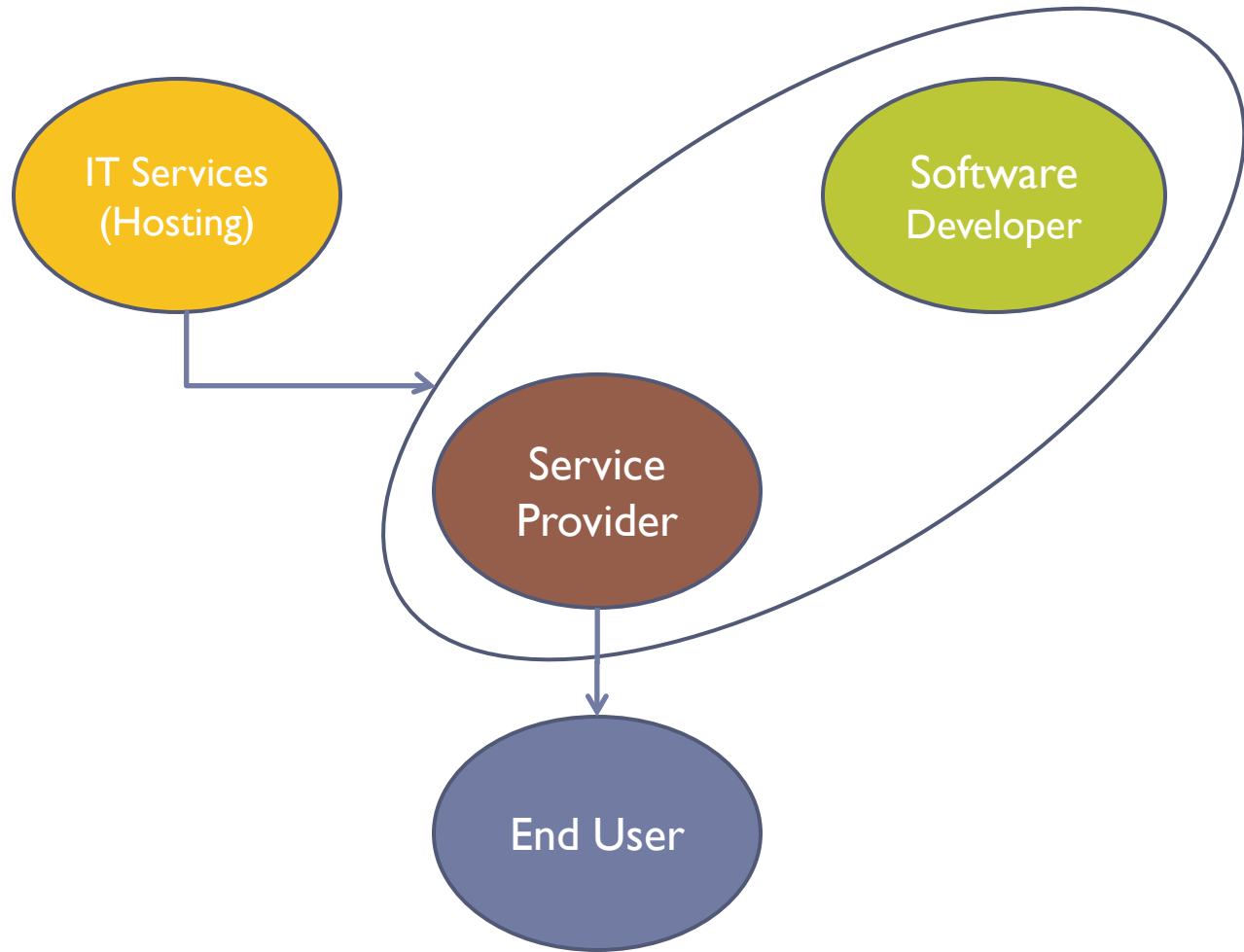
(Application Platform)

| Machine Instance | Storage Block | Database | Storage Block | Machine Instance | Network |

Virtualization

| CPU | STORAGE | Networking |

- Higher Service Levels
- Lower Costs

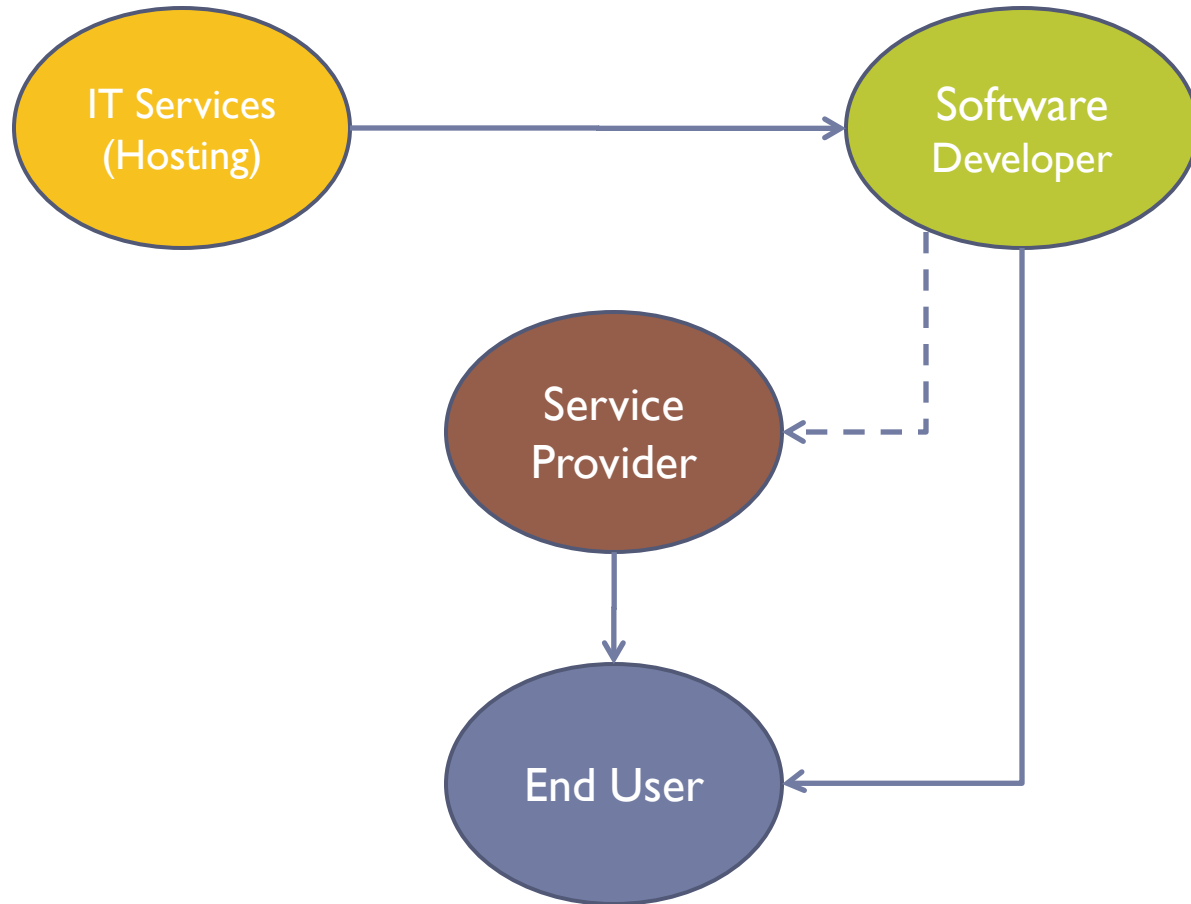# New Value Chains

New Value Chains

New Value Chains

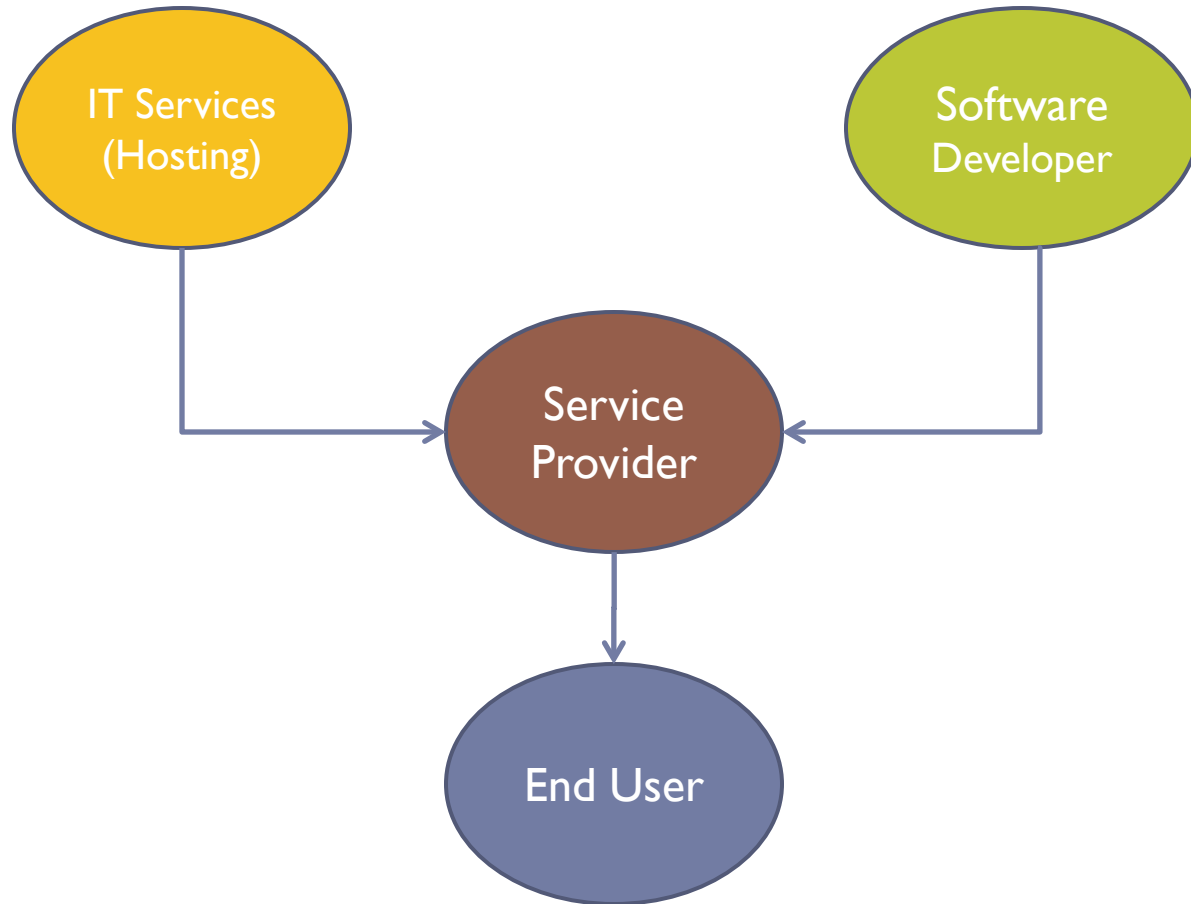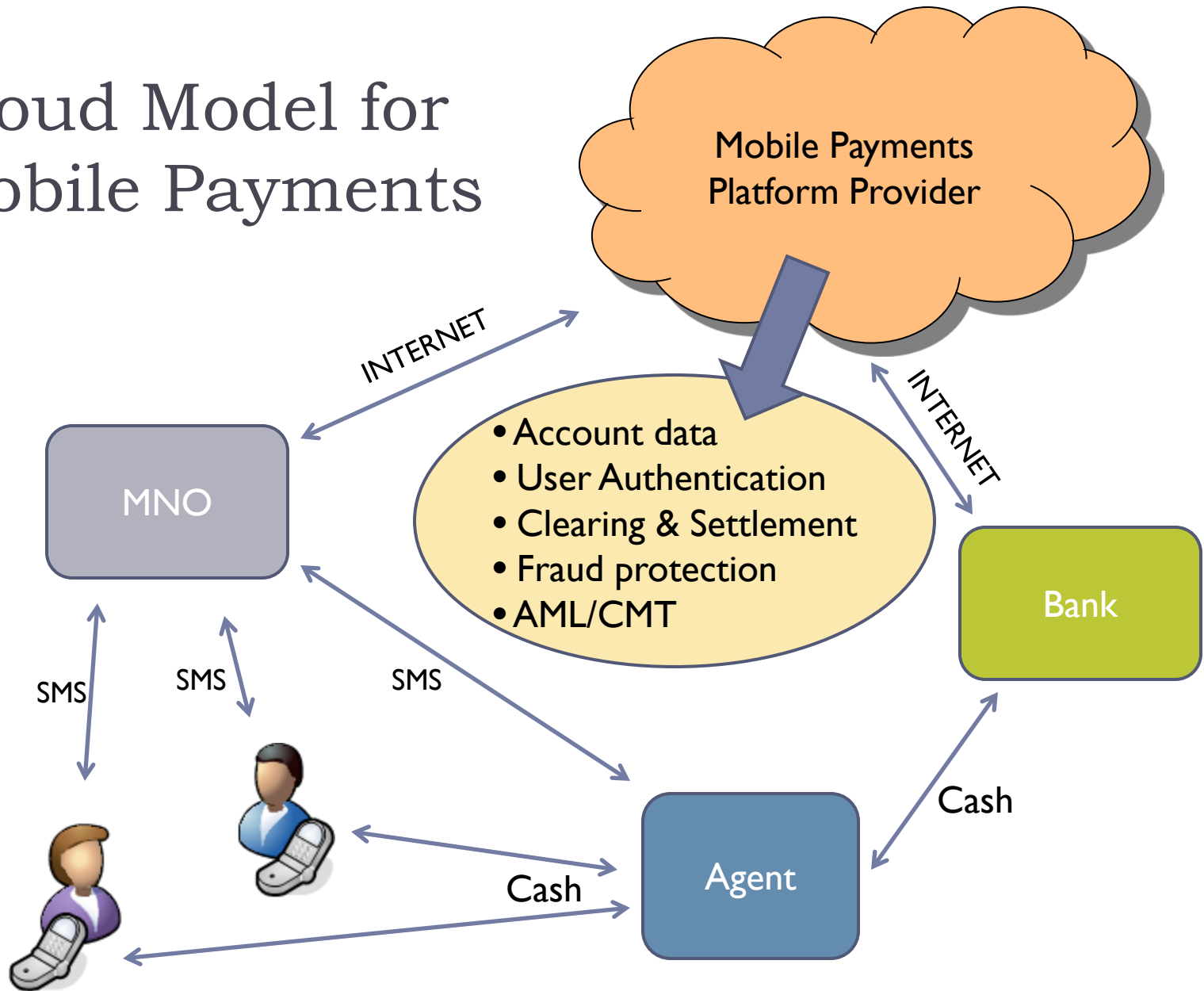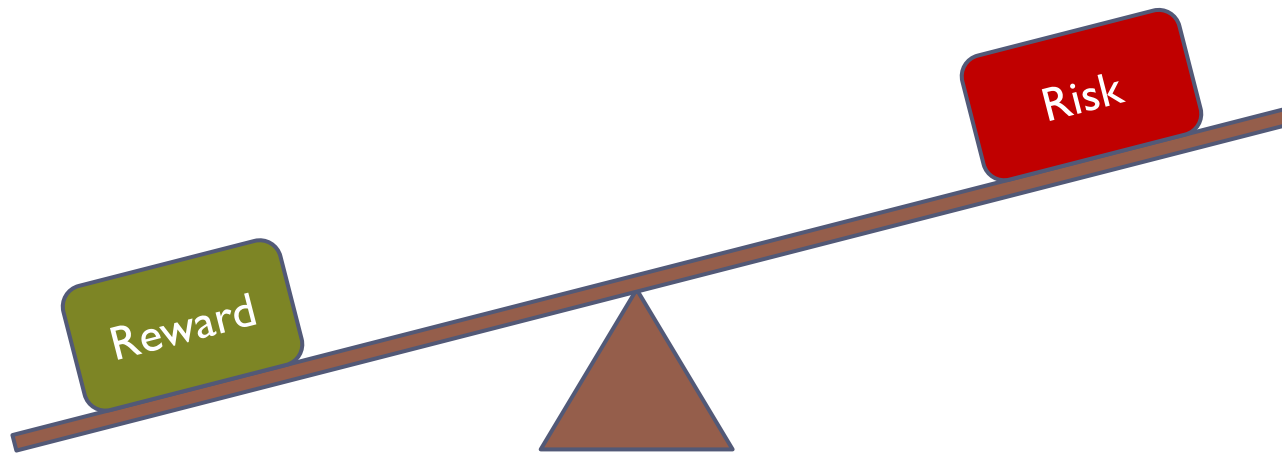# New Value Chains

New Value Chains

Cloud Model for Mobile Payments

Mobile Payments Platform Provider

INTERNET

INTERNET

MNO

- Account data
- User Authentication
- Clearing & Settlement
- Fraud protection
- AML/CMT

Bank

SMS

SMS

SMS

Cash

Cash

Cash

Agent

Rewards have Risks

Key Cloud Risks (a personal assessment)
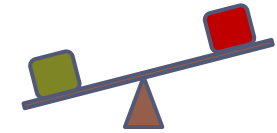
Risk	How Likely to Occur	Potential Impact
Internet Interruption	Increased latency due to traffic volume is common, especially in developing countries. Internet access subject to political control in some countries.	Services degraded but no data loss. Potential loss of customer support due to inconvenience, leading in turn to business failure.
Data Center Stability and Security	Low to moderate risk depending on quality and location of data center operations. Where local governments require local hosting in developing countries, risks are higher.	Potential for extended service interruption and data loss if storage not geographically dispersed.
Unauthorized access to data	Unlikely apart from spear-phishing attacks because can be encrypted and many services use some form of two-factor authentication for users.	Undetected compromise of privacy and theft of data very likely. Potential legal, public relations and regulatory impact.
Business failure or transfer of control	Moderate to high risk in the case where service providers are start-up enterprises with limited track record and thin capitalization.	Customer suffers immediate loss of access to software and data resulting in total inability to continue business operations.

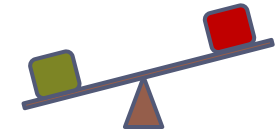# Risk Mitigation (for SaaS customers)
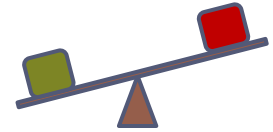
- ▶ Due diligence
  - ▶ Financial position?
  - ▶ Tenure in business?
  - ▶ Staff
    - ▶ Number?
    - ▶ Experience?
    - ▶ Roles?
  - ▶ Origins of Software?
  - ▶ Hosting & data center operations?
    - ▶ Independent audit of internal controls (SAS 70 and others)
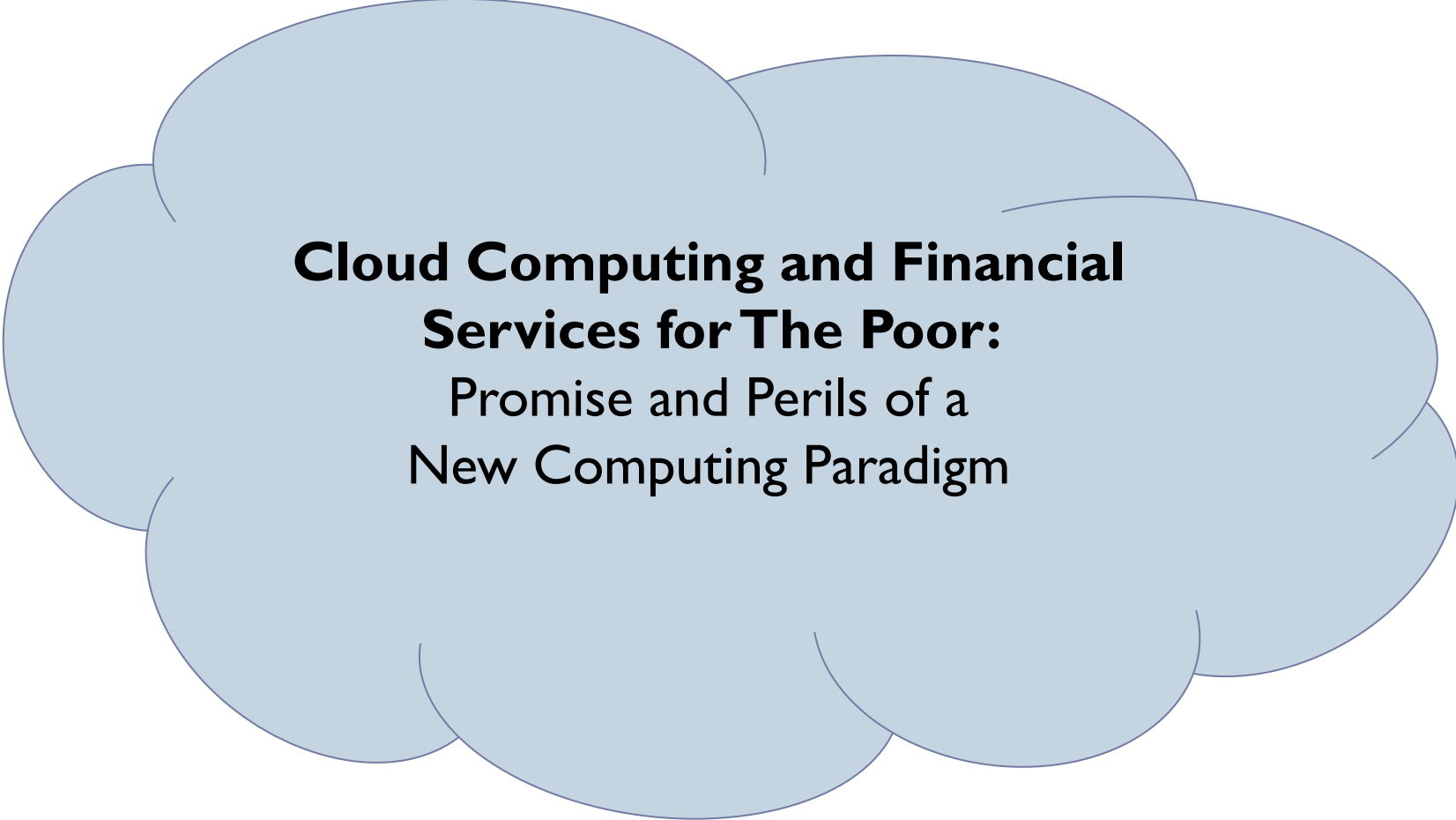
Risk Mitigation (for SaaS customers)

- ## Contracts (a/k/a Service Level Agreement)
  - ### Is it complete?
    - Ownership & access to data?
    - Data retention, eDiscovery
    - Fees & Charges
    - Liability and warranties?
    - Insurance?
    - Data center audit?
    - Regulatory compliance?
  - ### Is it enforceable?
    - Choice of forum?
    - Cost of enforcement?
    - Governing law?

- Service offerings in microfinance and mobile financial services will migrate to the cloud.

- The economic and operational advantages are compelling and the risks are very manageable.

- But know what you are buying.

Mobile data communication options

SIM – based application	A small application is loaded into the SIM card on the phone which presents a menu to the user. GSM only. Uses encrypted SMS
Structured SMS	Requires no special application on the phone. Not secure. Uses direct connection from mobile money platform to SMS gateway.
USSD (Unstructured Supplementary Service Data)	No special application required. GSM only. Uses continuous open channel for two-way communication so is more responsive than SMS. Requires no application on SIM.
Java J2ME	Java applications can generate either internet data communications or SMS messages, but Java not supported on all phones (especially low-cost feature phones).
Mobile Internet	Independent of MNO, communication direct with mobile money platform, but not widely available in developing countries.

Cloud Computing and Financial Services for The Poor:
Promise and Perils of a
New Computing Paradigm

Maria Stephens, USAID
mstephens@usaid.gov

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 any expansive growth of the use of m-money, the latter of which has resulted in→

•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 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.

Mobile Financial Services – Operating Models

Operating Model	Observations	Examples
Bank	**Primarily an additive model linked to an existing transactional account (e.g., debit card)**	
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.**	
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.**	**Banko**

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

Representative Payment Transaction Flows Integrate Risk Analysis

Cash in (In Network, Consumer – Agent)

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 – In Network, Consumer – MNO Agent

Cash Out (In Network, Consumer – Agent)

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

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 to Out-of-Network Consumer - No Acct

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

Consumer

- Send money to Receiver? — Yes → Have personal access? ①
  - No / No
  - Yes → Sender initiates "Send Money" transaction using Receiver's phone number ②
- Sender receives Advice of Non-Payment
- Sender Receives Confirmation of Debit → Transaction Completed ⑧
- Recipient Receives Payment Code → Recipient uses Payment Code to cash out through Agent or purchase goods

Agent

- No
- Yes
- Use Payment Code to transfer stored value to own account against cash and/or sale of goods

Network

- Network Available? ③ → Receive payment instructions → Sender Validated? ④ — Yes → Within Limits? ⑤ — Yes → Sufficient Funds? ⑥ — Yes → Receiver Phone Valid? — Yes → Debit Sender Account (inc. fee, if applicable) / Establish Payment Code / Advise both ⑦ → Trigger STR? ⑨ — Yes → STR to Regulatory Authority
  - No / No / No / No → Reject Payment / Advise Sender
  - No → No Action

Bank

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

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.

Bryan Barnett

bryan@4barnetts.com

Maria Stephens

mstephens@usaid.gov

September 16, 2011

microlinks
Mobile Financial Services

THANK YOU!

Please visit microlinks.kdid.org/events
for seminar presentations and papers