Mobile Money and Digital Payments Conference & Awards 27 July 2015 Meikles Hotel, Harare, Zimbabwe

Interrogating the Adequacy of Regulation Oversight & Deposit Protection Mechanisms in Telecoms Mobile Industry

Gift CHIROZVA
Business Operations Director
Deposit Protection Corporation

Discussion Outline

- Introduction
- Regulatory Oversight of Mobile Payments – An Evolving Landscape
- Protection of Mobile Banking Customers
- Developments in other Jurisdictions
- Deposit Protection Mobile Payments in Zimbabwe
- Conclusion

Mobile Money & Deposit Protection …

- The question of whether mobile money schemes qualify for deposit insurance is often met with mixed reactions.
- The argument is that since such funds are not in the strict legal sense 'deposits' as defined under the Banking Act
- The short answer is: Yes and No.
- We will return to this discussion later after putting the discussion into its proper context

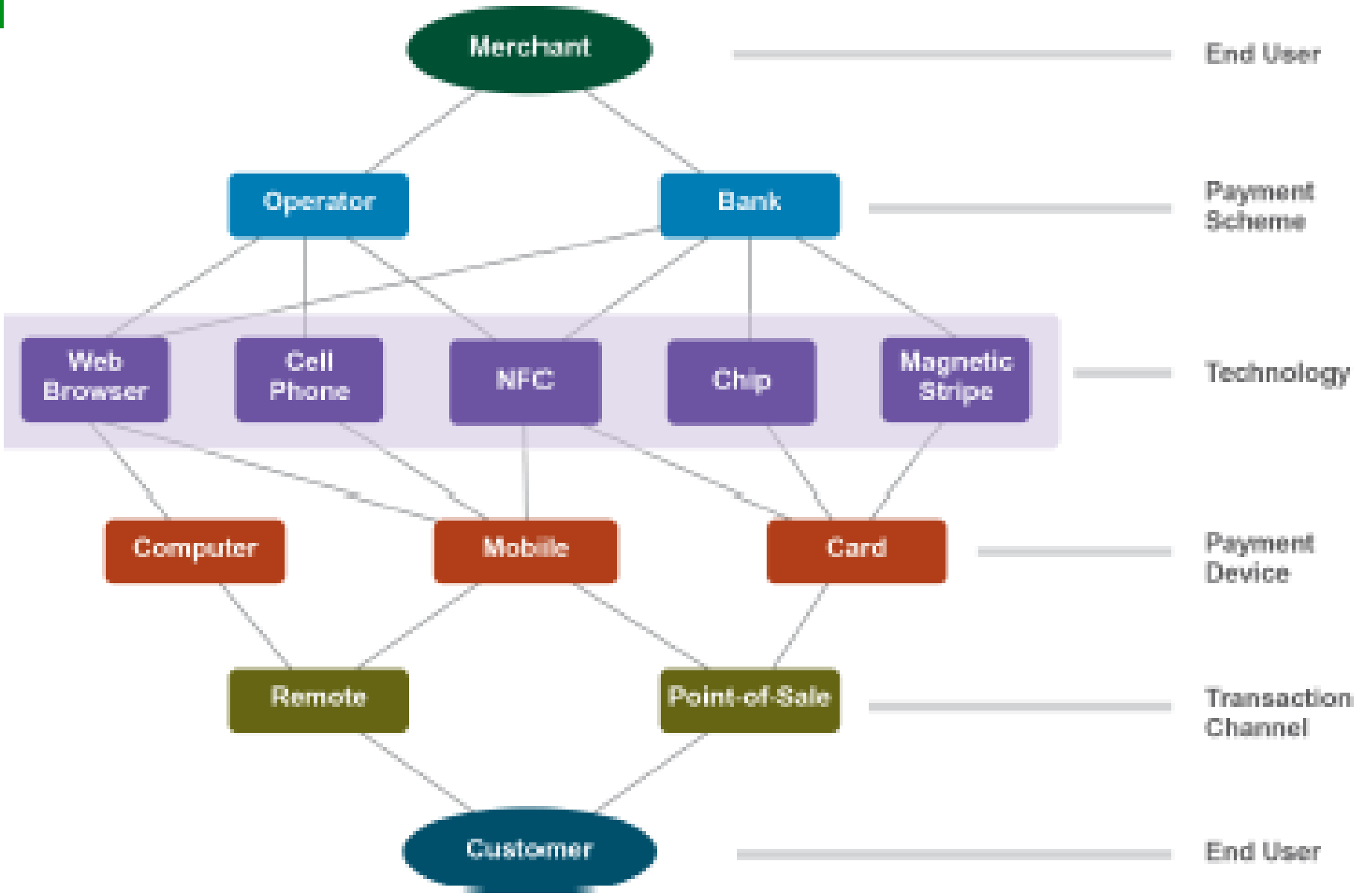
What is Mobile Money

- Greenacre and Buckley (2014) following the Alliance for Financial Inclusion define 'mobile money' as a type of stored value instrument that
  - (i) is issued on receipt of funds;
  - (ii) consists of electronically recorded value stored on a device (such as a server, card, or mobile phone);
  - (iii) may be accepted as a means of payment by parties other than the issuer; and
  - (iv) is convertible back into cash.
- A customer deposits or 'cashes in' money with the Provider in exchange for e-money. The Provider stores the funds while the customer uses e-money to trade with other customers. Later, the customer 'cashes out' any remaining balance of e-money.

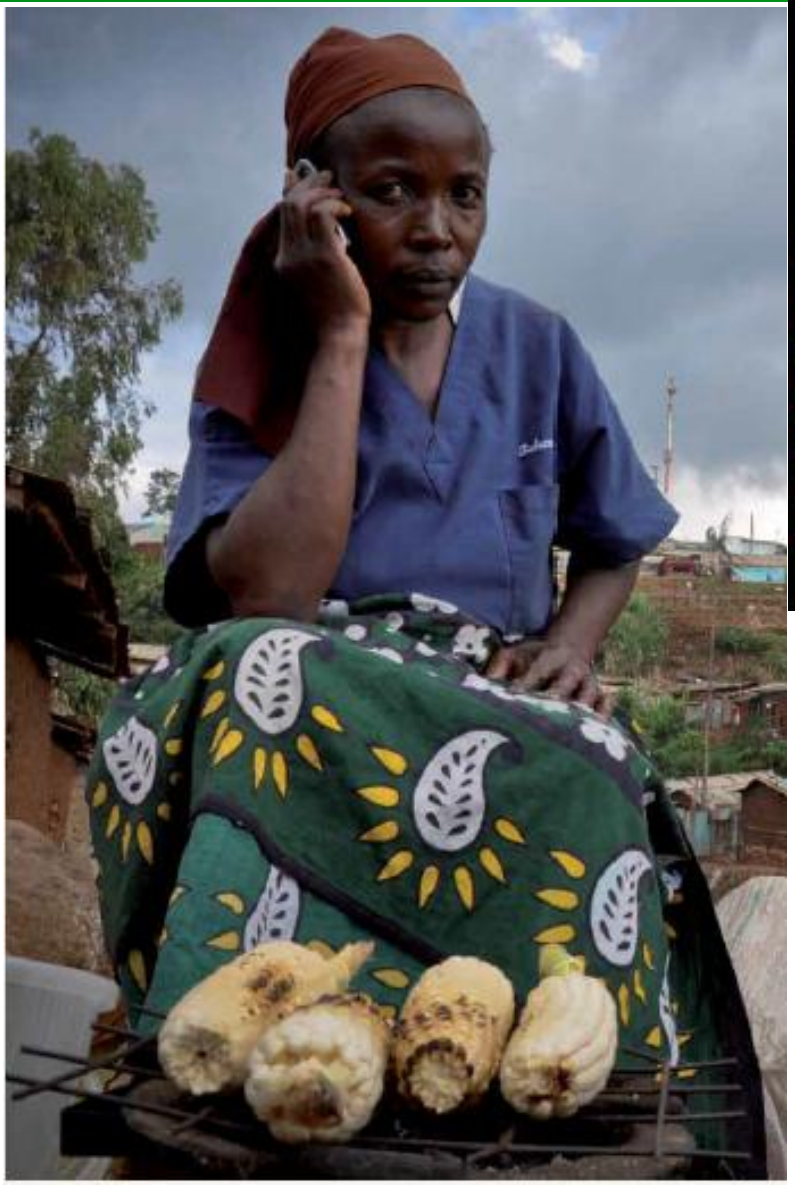
Types of mobile payment

- Mobile payments can be used for the following three types of transactions:
  - Mobile payment – (Paying for goods and services: shopping, paying bills, etc.)
  - Mobile remittance: Sending or receiving money - person-to-person; intra- or inter-national
  - Mobile banking (Withdrawals, transfers and other transactions on actual bank accounts)

Participants in Mobile Payment Service



Source: Trites S., Gibney C., and Lévesque B. (2013)



Source: di Castri (2013)

Mobile Payments Technologies

Near Field Communications	Cloud Based	Image Based
Wireless protocol that allows for encrypted exchange of payment credentials and other data at close range.	Leverages mobile connection to the Internet to obtain credentials not stored on the mobile device.	Coded images similar to barcodes used to initiate payments. Credentials may be encrypted within image or stored in cloud.
Carrier Based	**Proximity Based**	**Mobile P2P**
Payments billed directly to mobile phone account. Merchants paid directly by mobile carrier, bypassing traditional payment networks.	Geolocation used to initiate payments. Merchant will identify active users within range and verify identity. Credential exchange is cloud-based.	Payment initiated on mobile device using recipient's email address, mobile phone number, or other identifier. Payment is via ACH, card networks, or intra-account transfer.

FDIC (2012) Supervisory Insights, p5

Regulatory Environment

- Mobile money involves a range of market players & cuts across various sectors including banking, payments systems, telecommunications, etc.
- A variety of market participants can be involved in mobile money including mobile network operators (MNOs), banks and micro-finance institutions (MFIs)
- Coordination between regulators; other government bodies; and industry players is essential
- Mobile money also touches on financial inclusion; competition; and consumer protection issues

Consumer protection issues

- **Lack of tangible proof of payments** (e.g. receipts for evidence in the case of a dispute)
- Calls for billing standards which facilitate tracking of transactions.
- **Unreliable mobile account crediting systems.** Need service standards to validate claims for investigations & compensation.
- **Lack of technology standard**. danger of limited interoperability.
- **No fully developed regulatory framework**
- **No independent ombudsman.** Due to the novelty of the phenomenon mobile payments seem to be a "no man's land" where the service provider would be both the judge and party

Consumer protection issues …

- **Lack of currency**. Mobile payments may lack the status of legal tender that is authorized, adopted and guaranteed by the government.
- At best mobile payments have to be backed by the issuer's promise to pay.
- **Dormant assets**. Contrary to other services such as bank accounts, the definition of when mobile money/assets become dormant needs to be determined.
- Although amounts, are relatively small on an individual basis, the aggregate amts cld be large.
- access codes are known only to the owner & cld be lost forever should the main owner pass away.

Profiling

- **Profiling** involves aggregating large amounts of consumer data and mining it to predict and shape consumer behavior in the m-payments ecosystem.
- Evidence in some jurisdictions indicates service providers are selling user data to third-parties who then target consumers with advertising based on demographic, behavioural & geographic informn.
- Profiling could reinforce the uneven playing field between corporations and consumers. Asymmetry can lead to significant consumer protection concerns when harmful products are marketed to vulnerable consumers, including children.
- May need to inform consumers of mobile profiling & their rights in order to increase transparency.

Supervision and Oversight of Mobile Money

- The supervision and oversight of mobile money banking (MB) providers, is emerging as a distinct area of inquiry among a global community of policymakers and regulators that have taken bold steps to enable access and usage of MB in their respective markets.

- The varying responsibilities of authorities involved in banking supervision, payments system and telecommunications regulation present several challenges in developing supervision and oversight procedures for MB and assuring successful deployments.

Mobile Payments Risks

Category	Risk	Challenge
BSA/AML	Failure to satisfy recordkeeping, screening and reporting requirements intended to detect financial crimes, deter illicit cross-border payments, and prevent terrorist financing.	Ensuring emerging mobile payments models developed (and sometimes managed by third-party service providers) satisfy BSA/AML/OFAC requirements.
Fraud	Failure to prevent or deter unauthorized transactions, the interception of confidential information, or other fraudulent activity.	Ensuring adequate security of account data and other sensitive information and providing methods of "turning off" access to mobile accounts in the event of loss or theft of mobile device. Educating consumers regarding the need to password-protect and otherwise secure their mobile devices.
Compliance	Failure to comply with applicable consumer protection laws, disclosure requirements, and supervisory guidance.	Developing ways to translate disclosure and response requirements to the mobile environment.

FDIC (2012) Supervisory Insights, p7

Mobile Payments Risks …

Credit/Liquidity	Possible loss from a failure to collect on a credit obligation or otherwise meet a payments-related contractual commitment.	Managing mobile payments credit risk linked to underlying payment type (e.g., credit/debit card, ACH credits/debits, prepaid, EFT, etc.).
Operations/IT	Failure to protect confidential financial information or applications.	Ensuring mobile payments solutions satisfy requirements to safeguard customer information (e.g., Gramm-Leach-Bliley Act) and that such products are developed/configured in a secure manner.
Reputation	Negative consumer experience may reflect poorly on the bank or discourage the use of mobile payments.	Selecting and actively managing mobile payments technology partners and ensuring customer satisfaction with new products.
Vendor Management	Third party may fail to meet expectations, perform poorly, or suffer bankruptcy.	Ongoing due diligence of partner relationships with entrepreneurial companies that may be unfamiliar with operating in regulated environment.

FDIC (2012) Supervisory Insights, p7

Main Risks

- There are three main risks facing e-money customers, each of which relates to the Provider or its agents: insolvency, illiquidity & operational risk.

Insolvency

- As with a bank, there is a risk that the Provider may become insolvent & use customers' funds to repay debts that it owes to other parties if customers' funds are not held under a trust.
- The problem may be exacerbated if the Provider uses customers' funds as collateral to obtain loans from third parties.
- In a bank prudential regulations aim to reduce the riskiness of banks & ensure the safety of deposits

Illiquidity

- A Provider should provide only as much e-money as exists in the e-money system or 'float', held by customers, agents, and itself.
- In other words there should be a 1:1 relationship between e-money and customers' funds.
- If this is broken this may mean that when a customer seeks to cash in its remaining e-money, the Provider cannot return all of it.

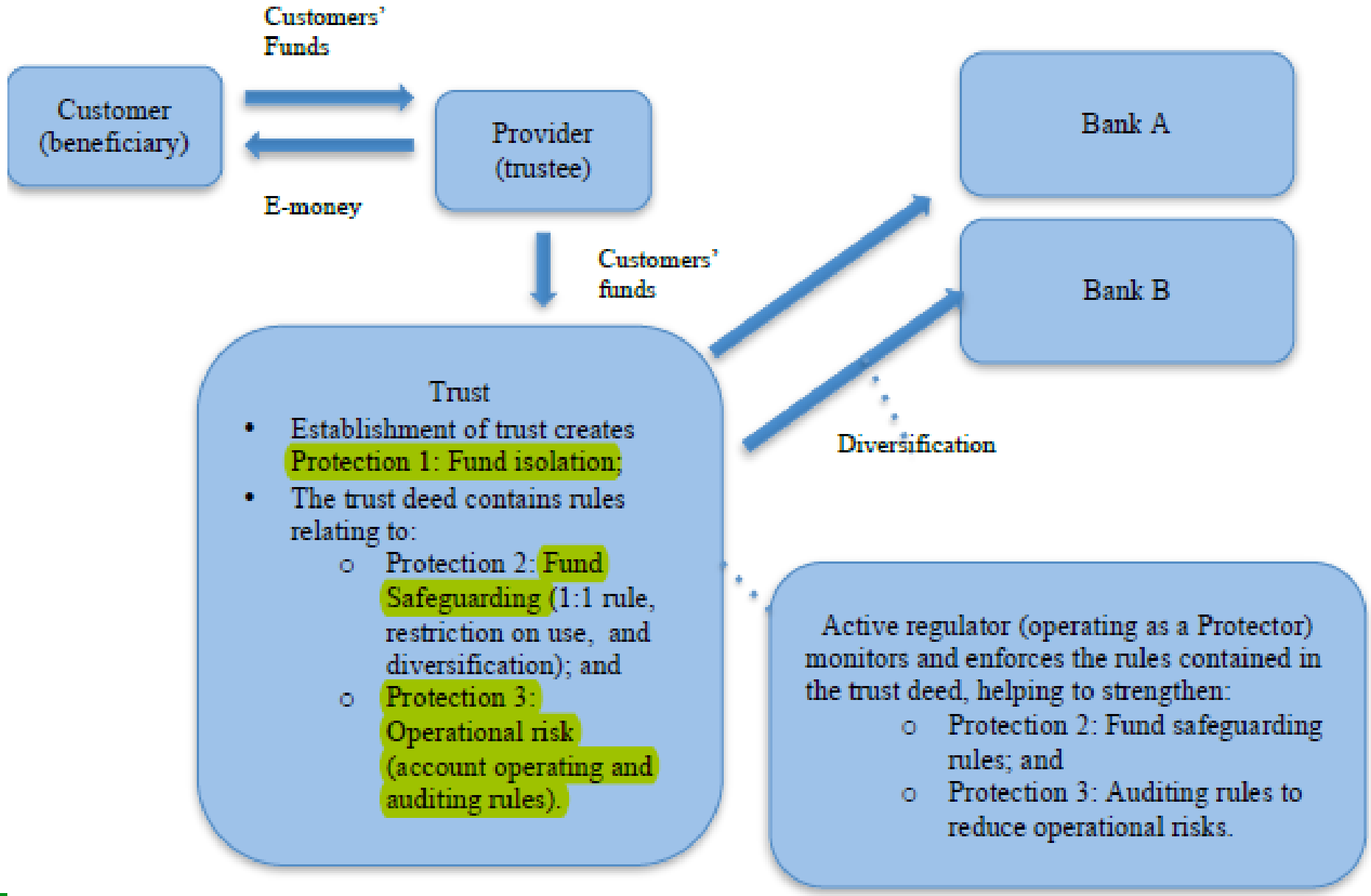
Operational Risk

Operational risk arises due to the Provider's internal activities, such as fraud, theft, misuse, negligence, or poor administration.

Transaction stage: Customer performs cash-in/out transactions, payments and transfers			
Vulnerability	Threats	Risks	Regulatory Implications
• Low-income/ indigenous population with limited access to information or low levels of literacy/ numeracy (e.g. Terms and Conditions) • Shared mobile phone usage within the family or community • Transactions facilitated by agents or others • Customer interface is overly complex and not intuitive	• Inaccurate/uninformed decisions • Potential for fraud	• Erroneous transactions • Vulnerability to fraud • Loss of trust	• Disclosure of information • Accessible information • Consumer education • Improvements in business processes that reduce the risks (e.g. contact/address book appears to facilitate transaction or the receiver's name appears before the person confirms the transaction, to reduce transactions sent to an unintended third party)

Alliance for Financial Inclusion [AFI] (2014, P6)

Use of Trusts for Protection



FUND ISOLATION (FI)

- Customer funds are normally stored in the name of the Provider in one or several bank accounts implying that the Provider is the legal owner of the funds.
- FI rules seek to address this anomaly of loss of customer funds that arises due to classification of ownership of funds.
- Providers are required to create trust accounts in a bank where they store customer funds and beneficiaries will be the e-money customers.
- In Afghanistan Providers are required to deposit 100% of customers funds in a trusteeship account.
- For customers to retain ownership a trust has to be declared over the funds and held in a separate bank account.
- Creditors or third parties cannot claim these funds during insolvency if the Provider becomes insolvent.

FUND SAFEGUARDING (FS)

- FS rules are designed to minimize the loss of agents or customer funds & illiquidity risk. They require Providers to maintain a ratio of 1:1 between e-money and float.
- Providers are prohibited from using the funds to finance business expenses, use funds as collateral, extend credit, but only to repay customers wanting to cash out
- The Provider can keep cash balances in a bank account as a 100% reserve requirement or invest in liquid government securities e.g. in Philippines.
- Holding the funds in a bank as deposits may result in the funds diminishing if the bank becomes insolvent.
- To mitigate this risk, Providers are encouraged to diversify via multiple accounts e.g.Safaricom& EcoCash
- FS can be implemented using trust laws providing for trustee duties; restrictions on use of funds; & rendering deposits in a trust account segregated from property of the Provider in event of the latter's insolvency.

REDUCING OPERATIONAL RISK

- There are several operational risks in mobile money e.g. misappropriation, negligence & mismgt of assets
- Theft of funds most common risk: (e.g. MTN Uganda $3.5m from a suspense a/c in 2012). Proper records rq
- There is need for auditing (the Provider should audit agents a/cs) and active monitoring to enforce terms on behalf of clients (Regulator given powers as Protector).
- This means that the Regulator will be given authority to oversee the actions of the trustee as the Protector.
- In other jurisdictions Protectors have powers to remove or appoint trustees, review the administration of the trust, settle disputes etc.
- Trust legislation may indicate whether the Protector is a fiduciary or not. If thus empowered, a Protector has a fiduciary relationship with the beneficiaries.

Responsibilities of the Financial Regulator

- Regulators must be aware of and keep pace with developments in ICT and continually build the competencies to better understand and properly regulate the industry to ensure at minimum that:
- A risk-based approach to consumer protection that & allows for innovation & financial inclusion.
- Providers are licensed under clear rules to protect consumer funds from misappropriation by the MFSP insolvency, fraud or any operational risk.
- level playing field that promotes competition to boost efficiency and increase consumer choice.
- There are appropriate standards for disclosure of information; data privacy; profiling; confidentiality and complaints handling channels.

Malawi

- In Malawi, RBM is the lead regulator for mobile money and it is now focused on developing and formalizing the overarching regulatory framework for the mobile money sector.
- Mobile money providers are required to use a trust deed with a declaration of trust.
- In Malawi, customer funds are not generally considered to be deposits and so are not covered by depositor protection provisions or deposit insurance.
- Regulatory requirements focus on fund isolation, fund safekeeping and operational risk management.

Kenya

- The Kenyan Deposit Insurance has proposed a principle called "Derived Protection Model" to extend deposit insurance to group of depositors, envisaged as those holding 'MPESA' and other accounts of a similar nature.
- Third party beneficiary/s of monies held under the trust account operated for and on their behalf are entitled to be compensated to limited amounts as provided in their law.
- This is on condition that the MNO has identified itself to be a trustee, acting in a fiduciary capacity, for and on behalf of certain identifiable beneficiaries provided that it meets particular requirements required as per the law and practice.

Nigeria

- In June 2014, the NDIC indicated that it is considering extending the deposit insurance coverage to mobile banking subscribers.
- Alternatively, if a bank fails, the insured mobile account can be transferred to another sound bank.
- The NDIC framework for extending deposit insurance to individual customers of mobile payment service is being deliberated on.

Laws and Regulations That Apply to Mobile Payments Transactions in the USA

Law or regulation description	Coverage	Applicability to mobile Payments	Key Obligations/Other Information
FDIC and National Credit Union Administration Protects funds of depositors in insured depository institutions and of members of insured credit unions in the event of failure of the institution.	Applies to "deposits" and "accounts" as defined in laws and regulations of the FDIC and National Credit Union Administration. These include savings accounts and checking accounts at banks and share accounts and share draft accounts at credit unions.	If the funds underlying a mobile payment are deposited in an account covered by deposit insurance or share insurance, the owner of the funds will receive deposit or share insurance coverage for those funds up to the applicable limit.	Deposit insurance or share insurance does **not guarantee that a consumer's funds will be protected in the event of a bankruptcy or insolvency of a nonbank entity in the mobile payment chain.**

Source: FDIC (2012) Supervisory Insights

Mobile Money & Deposit Protection

- Lets now focus on the question deposit insurance and mobile money.
- In Zimbabwe, S13 DPC regulations currently provide cover to trust accounts provided there was appropriate disclosure of the trust account; each trustee's & beneficiary's name, address & ID #; each beneficiary's % interest in in the trust account.
- If a trustee fails to comply with the requirements, each beneficiary's interest is not be deemed to be a separate deposit and shall not be separately insured.
- The DPC is currently engaging other key stakeholders including RBZ & CCZ to dev. an appropriate framework.
- Globally research is still ongoing on development of a protection framework for users of mobile banking products & the International Association of Deposit Insurers (IADI) is also currently seized with the matter.

References

- Alliance for Financial Inclusion [AFI] (2014), "Consumer Protection in Mobile Financial Services", Guideline Note No.13
- di Castri S. (2013) "Mobile Money: Enabling regulatory solutions" , GSMA — Mobile Money for the Unbanked
- Federal Deposit Insurance Corporation [FDIC] (2012) Supervisory Insights, Winter, Vol. 9, Issue 2
- Greenacre J and Buckley R. P. (2014), "Using Trusts To Protect Mobile Money Customers." Singapore Journal of Legal Studies
- Khiaonarong T. (2014) "Oversight Issues in Mobile Payments", International Monetary Fund IMF Working Paper WP/14/123
- OECD (2014), "Consumer Policy Guidance on Mobile and Online Payments", OECD Digital Economy Papers, No. 236, OECD Publishing.
- Simpson R (2014),"Mobile Payments and Consumer Protection Policy Briefing", Consumers International
- Trites S., Gibney C., and Lévesque B. (2013), "Mobile Payments and Consumer Protection in Canada", Research Division, Financial Consumer Agency of Canada
- United Nations Conference on Trade and Development [UNCTAD] (2012) "Mobile Money for Business Development in the East African Community: A Comparative Study of Existing Platforms & Regulations"

- **Thank You for Your Attention**