Mobile money fraud

9 October 2014

Presented by Stephen Omuga, CFE
Phone number 0721291705
Email address: soomuga@gmail.com

This is a mobile phone…

…and it's about to change our industry

agenda.

introduction to mobile payments | evolution of mobile money services | fraud schemes targeting each service| who then is at risk | ways to approach the mobile money problem| Q&A

Introduction to Mobile Payments

The Mobile financial services landscape encompasses the entire value stream of consumer offerings. Mobile payments and mobile banking remain the most popular in the consumer space

Mobile Financial Services Landscape

Mobile Payments			Mobile Banking	Mobile Marketing	Investing/ Personal Finance Management	Mobile Business	Mobile Add-Ons
•Physical POS purchases •Transit •Parking •Tolls •Vending •Coffee Shops •C2B Proximity Payments	•Remote purchase •Digital Content •Online Subscriptions •Mobile top-ups •C2B Remote Payments	•Money transfers •Remittances •Dividends •Person to Small Businesses •P2P Transfers	•Inquiries •Basic transactions •Account maintenance •Servicing •History •Loyalty currency	•Location based virtual coupons and promotions •Loyalty offers •Location specific advertising	•Transactions •Account maintenance •Servicing •History	•Wire transfers •Business transaction initiation and approval •Servicing	•Auto Loan Finder •Personal Banker
							

To differentiate between these two areas, we can broadly say that mobile banking is about "relationships and inquiry", while mobile payments is about "transacting and commerce"

	Mobile Banking	Mobile Payments
Definition	Utilizing a mobile device to access banking information and perform banking functions.	Utilizing a mobile device to conduct a point-of-sale payment.
Key functions	Balance inquires, schedule payments, transfer funds, view transaction history	SMS payments, NFC payments, reward cards, coupons, loyalty cards
Value Proposition	Offer consumers a self service channel to access their account information and interact with their bank on the go without having to call the bank directly or visit a branch.	Offer consumers the ability to pay using their mobile device. Includes the ability to store and use coupons, loyalty cards, rewards cards, etc. in addition to the ability to pay via credit card, all from their mobile device. The digital wallet as a replacement for a traditional wallet.

Evolution of mobile money services

2

Adobe Acrobat Document

Fraud schemes targeting each service

"People do not know how to act responsibly because if they did there wouldn't have been any need of law itself."
-Plato

Mobile money as a technology is good but not all its users are.

Schemes targeting consumer market (P2) - Trickery

- Employment schemes
- Promotion schemes (You have won, order while stocks last)
- New product schemes e.g. ATM withdrawal
- Sent money by mistake, please refund
- Funeral schemes where an imposter collects money on behalf of bereaved family.
- Issuing threats
- Phishing techniques with a view to steal identity
- etc .

Schemes targeting businesses

- Fake currency
- Fake systems upgrade disguising themselves as an MNO
- Saving contact as M-PESA or Airtel Money or YuCash or Iko Pesa
- Identity theft (SIM Swap
  - Online banking
  - Conventional banking services
- Tampering with the integration platforms between ERP and Mobile money services

Internal fraud schemes - SIM Swap fraud

- Getting a person's banking details – hacking, phishing, insider
- Clone SIM card
- Create beneficiary to transfer stolen money to
- Transfer and Withdraw the money
- Sometimes involves working with an insider from an MNO
- Sometimes involves hacking to obtain log in credentials of someone who can perform the SWAP.

Channel fraud schemes

- Strict KYC requirements to open bank accounts
- It is relatively easy to register a phone, mobile number and a mobile money account
- Fraudsters therefore target to steal from bank accounts but access the stolen money using a mobile money account
- Takes various forms – signing mobile money accounts using fake credentials, interfering in the m-banking interface

Who then is at risk?

Virtually everyone!

- Consumers
- Mobile money agents
- SACCOs
- Commercial banks
- Telecommunication companies
- Insurance companies
- Microfinance institutions
- NGOs
- Places of worship
- Educational institutions

Ways to approach to mobile money fraud

Consequences

- Incidences will increase and affect more customers
- Can result in subsequent intervention by the regulator
- Fraudsters will start targeting other banking products and channels or invent more elaborate financial crime schemes
- Some customers might refrain from using m-banking product and this might have an impact on the long term plans of the ban

Response

- Train staff so that they could identify customers who are at higher risk and provide adequate advise on risk mitigation (e.g. PIN generator versus static passwords, transaction limits, SMS alerts e.t.c)
- Raise awareness through sustained communication campaign warning customers about con schemes and other financial crime risks)
- Share experience and exchange information about the account mules within the industry and with other stakeholders (e.g. law enforcement)
- Current efforts clearly lack structure, coordination and consistency. Cooperation is key.
- Tight IT Security policy and management framework