IMPROVING THE SECURITY OF SIGNALLING PROTOCOLS

DIGITAL FINANCIAL SERVICES RISKS AND VULNERABILITIES

Mercy Buku LLM, LLB,CAMS, ACIB

DFS CATEGORIES

There are 4 major categories of Digital Financial Services:

1. **Payments**: Electronic money, mobile financial services, crypto assets, remittance services;

2. **Asset management**: Internet banking, online brokers, robo advisors, crypto asset trading, personal financial management, mobile trading;

3. **Alternative finance**: Crowdfunding, peer-to-peer (P2P) lending, online balance sheet lending, invoice and supply chain finance, etc...; and

4. **Others**: Internet-based insurance services, etc...

COMMON SIGNALLING ATTACKS

- Signaling networks use various protocols such as SS7, SIP or Diameter, which are susceptible to a variety of fraudulent attacks
- Vulnerabilities in telecom networks allow hackers to read texts, listen to calls and track mobile phone users' locations and gain access to subscribers personal data to access and disrupt communication services

- Fraudsters can also gain access to mobile banking and DFS apps which use SMS authentication to intercept messages used by apps to identify users

Telecom vulnerabilities can be exploited through two attack surfaces :

- The SS7 signalling network and

- The cellular air interface (the radio frequency communication between the cell phone and the cellular network)

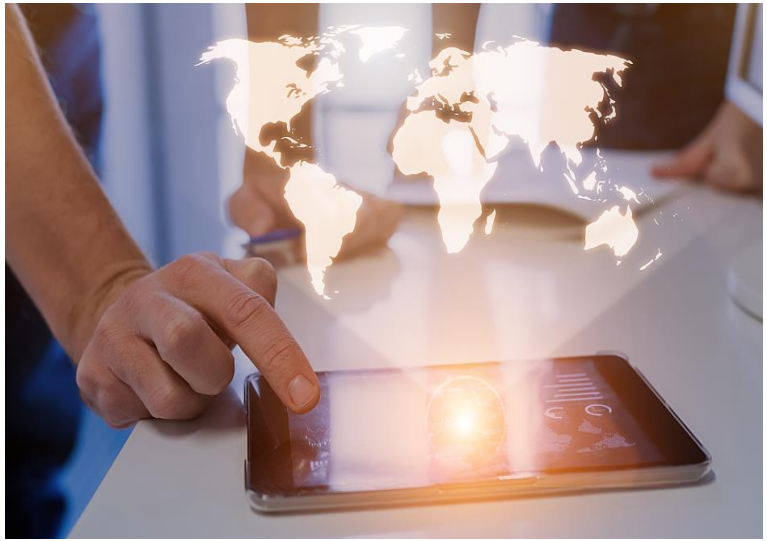
COMMON SIGNALLING ATTACKS

Common signalling attacks include :

- Telephone spam,
- Spoofing numbers (SS7 Spoofing)
- Location tracking
- Subscriber fraud
- Calls and message Interception,
- DoS, infiltration attacks,
- Routing attacks, etc.
- Two Factor Authentication Fraud (mobile banking frauds) – used to gain access to an online bank account through the interception of messages sent to customers with the OTP

Digital Financial Services Fraud on Mobile Networks

.



VULNERABILITY OF MOBILE FINANCIAL SERVICES TO FRAUD

Growth of digital financial services and more particularly mobile money, has been at the centre of financial inclusion initiatives in various countries, notably in Sub Saharan Africa and Southern Asia, due to:

- Lack of access to traditional financial services in these regions
- Prevalence of mobile phones, wide acceptance of MMT, cashless service, speed, anonymity, and portability of mobile money
- Proliferation of various financial services offered on mobile banking and other digital platforms:

➢ *Money Transfer including International Money –P2P, B2C,C2B,G2P*

➢ *Digital Payment Services – Bills and other payments, insurance, health, school fees, loan disbursements and repayments etc*

➢ *Mobile Banking – Bank to bank/mobile transfers, bill and other payments, digital savings and credit facilities, investments etc*

➢ *Airtime Management – Purchase of airtime for self and others*

These products provide opportunities for fraud, and other criminal activity

NB : These vulnerabilities have increased during the Covid era due to measures put in place by providers and regulators to encourage increased cashless payments as a means to prevent Covid

MOBILE FINANCIAL SERVICES – STATE OF THE INDUSTRY

Over 290 deployments of mobile money in 95 countries

Over 1 billion registered mobile money accounts transacting US$ 2 billion daily in 2019;

50 % of which are in Sub Saharan Africa and

31% in Southern and East Asia and the Pacific

GSMA-State-of-the-Industry-Report-on-Mobile-Money-2019

WHO ARE THE PROVIDERS?

1. Telcos/MNOS/Mobile Virtual Network Operators - licensed to provide MFS on their platforms/networks directly or in partnership with a bank

2. Banks, Insurance Cos, MFI's, Co-operatives, Forex Bureaux, Money Transfer Agents, PSP's NDCI's etc.. – offer DFS via internet, cards or through their own mobile apps/payment systems or on the various Telco MMT platforms

Common Mobile Financial Services Frauds

3 Categories

Consumer Affecting

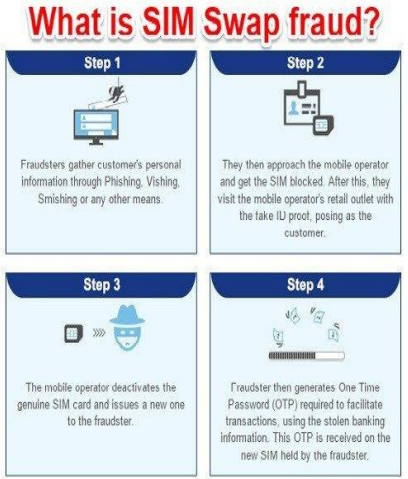
Agent

Provider Affecting

Common MFS Frauds

Consumer Affecting

- Identity Theft
- Impersonation Fraud
- Fraudulent SIM swaps through compromised PINS
- Loss from Erroneous Transfers
- Mobile banking frauds
- Agent defrauding the customer (OTC, Reversals, Fake Currency)
- Ponzi and other illegal investment schemes
- Social engineering – Phishing Scams/Con tricks such as Job application and promotional scams, fraudulent texts, extortion
- Digital Credit Fraud

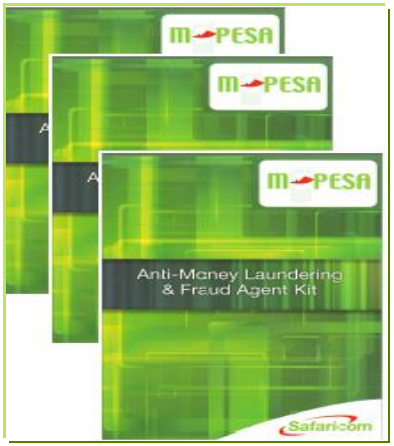


Common MFS Frauds

Agent Affecting

- Fake Currency Deposits
- Float loss from Impersonation Scams/ Unauthorized Use Compromising of PINS
- Customers defrauding agents e.g fraudulent reversals
- Agent Promotion scams promising bonus commission
- Pay bill Account Fraud e.g fake confirmation messages; fraudulent reversals

Common MFS Frauds



Provider

- Internal Fraud
- Mobile banking frauds
- Digital Credit Fraud
- Illegal use of mobile platforms for criminal activity e.g money laundering and terrorist financing

EMERGING RISKS- NEW PRODUCTS/SERVICES

- Digital Savings Accounts and Credit offered via digital channels
- Digital Insurance products paid for on DFS channels
- Money Remittance and Forex services on MMT platforms
- Debit Cards – Can be stolen and the funds transferred to bank accounts and mobile wallets via the internet
- Prepaid Cards and Gift Vouchers funded with criminal proceeds via mobile money
- Securities and Investment products paid for through mobile money and other DFS channels
- Digital Currency – universally transferrable on interoperable payment platforms including mobile payment platforms
- Mobile Network Risks

MOBILE NETWORKS AND ML/TF RISKS

➢Move away from use of mobile money platforms and traditional banking channels to remit the proceeds of terrorist financing

➢Increased use of informal channels such as *hawala,* and other informal money transfer agents by terrorists to transfer cash to finance their activities

➢ Use of mobile phones as the primary means of communication in the planning and execution of terrorist and other criminal acts,

➢MNOs and users of mobile network platforms will still be at risk

HENCE : Need for appropriate controls to safeguard the integrity of subscriber data and ensure that mobile networks are not being used to facilitate terrorist and other criminal activity

CASE STUDY 1: Uganda's banks plunged into chaos by a mobile money fraud hack

- Security breach involving Pegasus Technologies, mainly affected bank to mobile wallet transfers
- At least $3.2 million is estimated to have been stolen in this latest incident with some reports quoting a much higher figure. The hackers used around 2,000 mobile SIM cards to gain access to the mobile money payment system and transfer millions of dollars via banks to various mobile wallets
- MTN Uganda and Airtel Uganda, suspended mobile money service transactions between their networks, indefinitely. Stanbic Bank Uganda, and Bank of Africa also suspended transactions between the banks and the mobile phone companies.

- ***Possible cause : Upgrade of MTN System on October 6th 2020 during which the period, data, voice and mobile money services were interrupted.***

CASE STUDY 2: Congolese regulator warns mobile users against a 'missed call scam'

- The Electronic Communications and Postal Regulatory Agency (ARPCE) in the Republic of Congo has recorded an upsurge in fraud involving missed calls in the country.
- “For the past few months, a form of telephone fraud has been rampant in Congo, the Wangiri, also known as missed call fraud, ‘’ the ARPCE said.
- Wangiri is a Japanese term meaning “ring and cut”. (Feb 2018)

https://www.africanews.com/2018/02/08/congolese-regulator-warns-mobile-users-against-a-missed-call-scam//

Impact of MFS Fraud from a Business Perspective

- More specifically MFS Fraud and other criminal activity :
- Diminishes consumer **trust** in MFS
- Hampers **bottom line** of MFS providers
- Hampers **growth of value added services** on digital transactional platforms
- May lead to **account inactivity** and prevalence of **OTC** transactions
- May lead to significant **consumer harm** and losses **SMALL AMOUNTS, BIG IMPACT!**

RECOMMENDED MITIGATORY MEASURES

INTERNAL CONTROLS

Fraud Risk Mitigation and Best Practises for Digital Financial Services – Mobile Networks

INTERNAL PROVIDER CONTROLS

DFS RISK MANAGEMENT STRUCTURE

A prudent DFS Risk Management Structure will comprise of the following key areas of assurance:

- Money Laundering Reporting/Risk and Compliance Office (Statutory Requirement)
- Ethics and Compliance Risk Management (Fraud Management and Prevention, Compliance with processes, Staff Ethics)
- Enterprise Risk Management – Business Continuity Plans, Information Security etc.
- Revenue and Product Assurance (Telcos)
- Internal Audit and Information Security Audit (this should be a separate division)

DFS RISK MANAGEMENT PROGRAM

TECHNICAL CONTROLS

1. Transaction Monitoring/ Screening

- Real time Automated Transaction Monitoring pegged to transaction limits for financial transactions
- Fraud monitoring systems that apply artificial intelligence (AI) and machine learning (ML), combined with pre-packaged rule sets – *(Data must be valid, up-to-date industry data including roaming partners, number ranges, contact details and other intelligence regarding sources of attacks)*
- Sanction screening against international watch lists (AML/CFT)
- Use of appropriate link analysis tools to analyze subscriber data including locational details, call and financial transaction patterns- *(used to detect hoax calls and texts, corruption and fraud, terrorist activity, hate messages, kidnapping etc)*

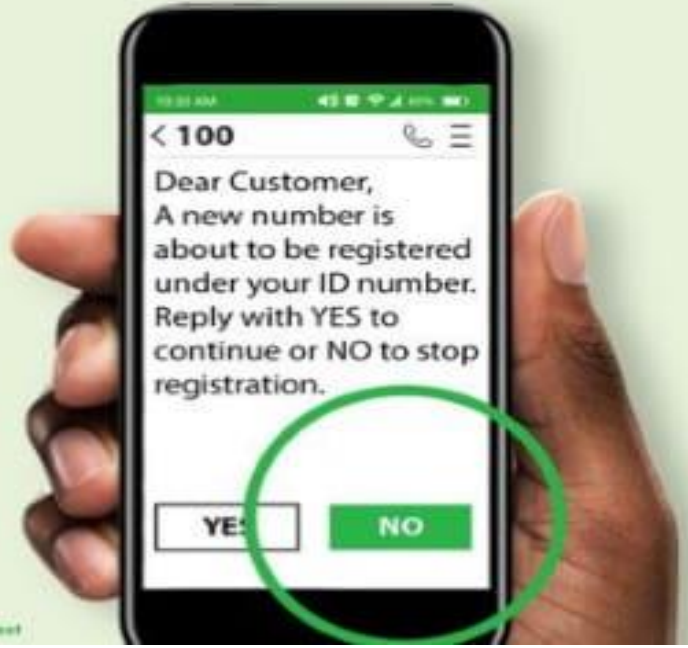
2. Systemic Controls

- Restriction of access rights,
- Electronic/biometric registration to curb errors,
- Information security and system audit checks,
- PIN controls – for financial transactions, SIM swaps etc.
- System prompts to prevent sim swaps, erroneous transfers, etc., lead time for operationalizing of sim swaps, mobile banking registrations

TUWAANIKE

EXTRA SECURITY FOR YOU

If someone tries to register a line using your National ID, you'll receive an SMS alert from 100. Simply reply with a 'NO' if it's not you.



Simple • Transparent • Honest

Common Suspicious Transactions/Red Flags on Mobile Networks

1. Frequent agent deposits and low/no commission transfers to multiple numbers
2. Multiple customer and agent registrations (sim and mobile wallet)
3. Same day deposits by the same person in different locations
4. Customers depositing to third party accounts (Direct Deposits)
5. Customers failing registration validation checks
6. Customers failing sanctions screening checks
7. Immediate withdrawals after deposit (through Agents/ATMs)
8. Customers carrying out Multiple high value/high volume transactions with no apparent economic rationale

Common Suspicious Transactions/Red Flags on Mobile Networks

9. Multiple attempts of failed transactions or password resets
10. Immediate Transfer of funds after registration/deposit
11. Frequent sim swaps/change of authorization mandates
12. Frequent texts/calls from blacklisted sites known to have terrorist or fraudulent activity
13. Frequent calls/texts/money transfers between known fraud/terrorist suspects and their associates
14. Frequent agent transaction reversals
15. Suspicious activity reports from agents and customers

DFS RISK MANAGEMENT PROGRAM

Regulatory and Procedural Controls (Compliance and Consumer Protection)

1. KYC/CDD (Know Your Customer)

- KYC Registration and Ongoing CDD checks on customers, agents and business partners
- electronic biometric registration and identity verification and data integrity, Risk based Tiered KYC based on transactional volumes restrictions on multiple registrations, account suspensions etc.,

2. Training and Awareness (Know Your Procedures)

- Online, Media and Network Awareness Campaigns on Fraud
- Staff, Agents, third party partners

3. Complaints Recourse Channels

- Specialized desks/hotlines with trained staff for common complaint types: Reversals, lost SIM/PIN, new products
- Dedicated agent hotline
- Training of agents on complaints handling and fraud detection
- Remedial action to resolve complaints e.g. fraud management tools

DFS RISK MANAGEMENT PROGRAM

4. Product Risk Assessments (Know your Products)

- Covering New and existing products to identify risks and recommend mitigatory controls on an ongoing and Annual basis

5. Agent Management (Know Your Agents)

- Banks and Telcos – Onboarding KYC, risk based compliance monitoring, penalty structures,

6. Compliance Monitoring/Risk Management (Know your Procedures)

- Internal Compliance monitoring and Spot checks on Agents and Retail shops to confirm compliance with onboarding and transactional procedures (.g Mystery shopping)
- External Compliance Surveys by professional contractors to test compliance with set parameters remedial action to address compliance gaps

DFS RISK MANAGEMENT PROGRAM

7. Investigations and Enforcement

- Status of action on SARS Reports
- Blocking/Freezing of suspect accounts
- Liaison with Law Enforcement agencies in Profiling, arrest and prosecution of suspects

8. Reporting

- Internal SARS Reporting processes and Complaints Recourse
- Periodic Regulatory and management reporting on ML/Fraud Trends
- SARS reporting to relevant FIU

9. Industry/Stakeholder Co-operation

- Mutual sharing of SARS information
- Benchmarking against industry best practice
- Common MM Association/Forums to address stakeholder challenges and engage regulators on stakeholder matters

ITU - SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Technical report on SS7 vulnerabilities and mitigation measures for digital financial services transactions

Proposed the following mitigatory strategies for detecting and mitigating signaling attacks:

- Social engineering attacks with MT-USSD – via location checks and verification of the IMEI and IMSI of the hone and use of 2 way secure OTP
- Detect Interception of MO-USSD transactions via locational and IMEI checks
- Detection of unauthorized SIM card swap via IMEI checks
- Internal rules on SIM swaps by MNOs/MVNOs including SMS notifications to the subscriber seeking confirmation to SIM SWAP, 2-4 hour holding time, verification measures including queries as to last transaction etc;
- Detection and prevention of mobile banking fraud by Linking bank 2FA systems used by banks/PSPs to SIM/phone number databases to enable real time verification on SIM Swaps and new mc banking/payment accounts

ITU - SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Technical report on SS7 vulnerabilities and mitigation measures for digital financial services transactions

- Mitigating SIM card recycle risks – by monitoring dormant DFS accounts for signs of unusual activity upon which the account should be blocked.
- Embedding spoof identifier within the user's phone for authentication of communications between the DFS provider and the user's phone to authenticate the user and phone.
-
- Regulation requiring the putting in place of policies and procedures for the mitigation of SS7 and related attacks e.g on SIM swaps.
- Regulatory rules on SIM swaps, including: standardization of sim swap rules, identification of subscriber including an affidavit, and passport photo, verification of proxies
- Regulatory coordination between regulators so as to assign specific and joint roles and responsibilities.

- GSMA have made similar recommendations in their Report on SS7 Vulnerability – 2018 and https://www.gsma.com/security/resources/fs-21-interconnect-signalling-security-recommendations-v6-0/

CHALLENGES

Reporting Institutions/Providers

- In-effective /Inadequate Risk Management structures e.g. no MLRO
- Ineffective /Inadequate Risk management Policies and Procedures
- Need for customised AML Awareness and Training programmes
- High cost of infrastructure (Monitoring and watchlist Screening systems)
- Lack of management support /misaligned business strategies (business expediency vs controls)
- Compliance Violations e.g - Failure to Report Suspicious Activity

Regulators

- Slow pace of operationalizing legislative reforms – (*National Risk Assessments still outstanding, RIS and Stakeholders not on board)*
- Lack of Capacity, Training, and infrastructural support; impacts on effectiveness and fulfilment of statutory duties e.g. inspections, compliance monitoring etc.
- Dual regulations for some RI's (e.g. telcos)
- Pending crucial legislation e.g. Consumer Protection, Cybercrime and Electronic Payment Laws, Sector Specific Legislation
- Inadequate penalties for non compliance

CHALLENGES

ENISA survey in the EU and the Security Infrastructure and Trust workstream survey by the ITU

- Only 25% of Mobile operators reviewed have addressed the issue of SS7 telecom vulnerabilities
- Implementation rate was very low (below 10%) Have implemented mainly SMS home routing and filtering on signalling nodes.
- Lack of awareness of mitigation strategies by both telecom regulators and telecom operators
- Cost implications and the lack of regulation - 75% of the surveyed operators in the EU replied that cost is the inhibiting factor in implementation, and the lack of regulation mandating it

KEY TAKEAWAYS

1. Speed of Delivery of Electronic payments may give rise to non traditional banking risks associated with Fraud, Money Laundering and Terrorist Financing

2. Regulators must ensure that providers have effective compliance programmes in place to detect and prevent criminal activity on their networks.

3. Need to have the necessary legislation in place, coupled with appropriate regulatory regimes to enforce it; including appropriate training programme for all stakeholders.

4. Need to ensure that providers have effective Transaction Monitoring and Screening systems - the cost of such systems can be shared through multi-licensing arrangements – Regulators should play a co-ordinating role towards this end

5. Supervisors and institutions must assess relevant DFS risks and design appropriate and proportional measures to address risks, taking into account individual risk profiles


DON'T
Be
A
VICTIM
Mobile Money fraud


DON’T BE
CONNED!

THANK YOU/ASANTE SANA