**ITUWebinars**

# Insights on Digital Financial Services during COVID-19 Webinar Series

*Episode #8: Handling of Digital Finance Crimes and Scams*

30 June 2020
15:00 - 16:30, CEST

Join us online!
http://itu.int/go/DFS-Webinar-08

# Handling of Digital Finance Crimes and Scams during COVID-19

## African Perspective

Mercy Buku LLM, LLB,CAMS, ACIB

.

# VULNERABILITY OF DIGITAL FINANCIAL SERVICES TO FRAUD

- Prevalence of mobile phones, wide acceptance of MMT, cashless service, speed, anonymity, and portability of mobile money
- Financial inclusion initiatives have led to a proliferation of new Digital/Mobile Financial products offered on mobile money platforms in partnership with other Financial service providers and corporate entities
- *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*

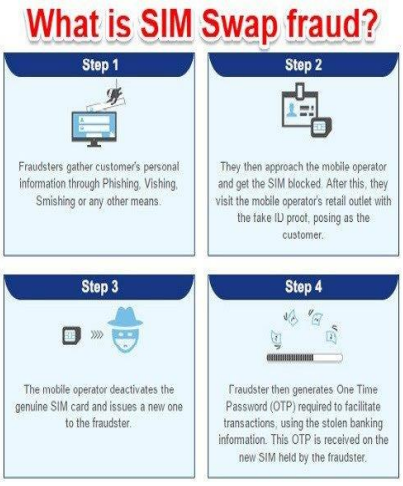
**These products provide opportunities for fraud, and other criminal activity**

***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***

# Common DFS 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

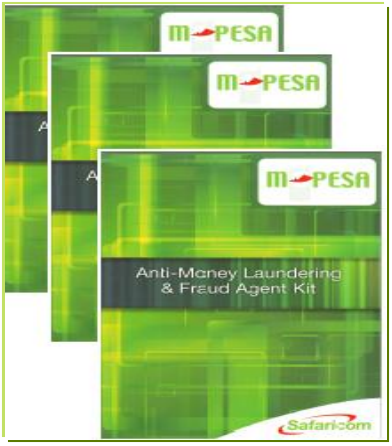


# Common DFS Frauds

## 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 DFS 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

# DFS Fraud Vulnerabilities During the Covid Era

Expected Resurgence of DFS Frauds due to :

- **Increased reliance on cashless/digital payments** arising from movement restrictions and government initiatives to promote cash less payments as a preventive measure for Covid
- **Incentives to use cashless payments, network services and data**; New products, online registration, reduced fees, tax reliefs, higher transaction and holding limits - have created opportunities for impersonation and other scams
- **System and Delivery Risk** - Increase in transactional volumes on mobile and online payment platforms may lead to system down times and impact service delivery including automated fraud monitoring,
- **Compliance Risks** - Staff working from home, challenges in compliance monitoring e.g for agents/branches in remote areas, no audit checks, KYC compliance violations, inadequate consumer protection measures
- **Economic Risk** : increased poverty levels due to business closures and redundancies arising from lock downs and other Covid measures

# DFS Frauds During the Covid Era

**Common Frauds include the following** :

**Consumer Impacting** : Identity Theft and Job application and promotional Scams, Hoax messages, Erroneous transfers, Impersonation Frauds, mobile banking frauds

**Agent Impacting** : OTC expected to reduce, however losses suffered from promotional scams and impersonation fraud may increase

**Provider Impacting** :

Internal Fraud and Digital Credit Fraud

# RECOMMENDED MITIGATORY MEASURES


1. **KYC/CDD**
   Enhanced due diligence measures due to move towards online registration and increased transactional volumes, data integrity

2. **Online, Media and Network Awareness Campaigns**
   Staff, Agents, third party partners, customers – on fraud trends

3. **Complaints Recourse Channels**
   Customer complaints and recourse measures e.g hotlines for fraud and other complaints ; invaluable data source for fraud trends

4. **Transaction Monitoring/ Screening**
   Automated Transaction Monitoring pegged to revised transaction limits (to detect suspicious activity) to include IMT and cross border transfers

5. **Agent Management**
   Risk based compliance monitoring, penalty structures for violations etc

6. **Risk Assessments**

   Product Risk Assessments covering New and existing products to identify new risks and recommend mitigatory controls

7. **Technical Controls**

   User access and PIN controls, controls on sim swaps and activation of new sims/mobile wallets, mobile banking controls, data privacy etc

8. **Investigations and Enforcement**

   Liaison with Law Enforcement agencies in Profiling, arrest and prosecution of fraud suspects

9. **Industry/Stakeholder Co-operation**

   Mutual sharing of SARS information, Benchmarking against industry best practice

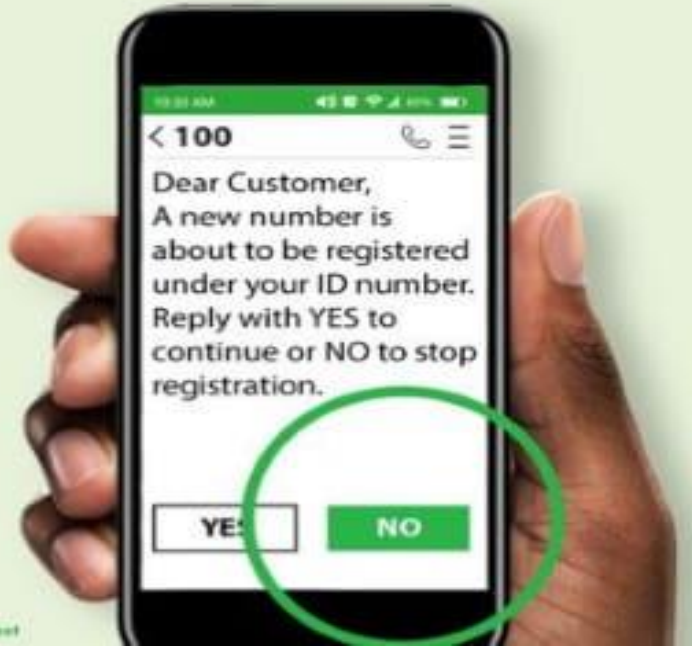
10. **Regulatory and Supervisory Measures**

    Consumer Protection, Risk Management, Compliance Supervision

# 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

# THANK YOU/ASANTE SANA