Combating fraud in the age of digital payments

Strengthening Coordination and Collective Action Against DFS Fraud
Cyber Incident Response-A Central Bank Perspective

CENTRAL BANK OF LESOTHO

BANKA E KHOLO EA LESOTHO

Introduction and objective

- ✓ Digital financial services (DFS), especially mobile money, have played a central role in advancing financial inclusion in Lesotho.
- ✓ As of September 2025, registered mobile money users reached approximately 2.6 million.
- ✓ While mobile money has brought major benefits, it has also increased fraud and cyber risks. DFS fraud is now a system-wide concern which threatens financial stability.
- ✓ Today's presentation aims to share the insights on fraud and cyber crime trends and risks, and emphasize how cross-sector collaboration can strengthen the fight against fraud and cyber crime

DFS Growth & Risk Expansion

Real-time payments, savings and micro-loans expanded access

Innovation outpaces fraud controls

Weak coordination and consumer protection exploited by fraudsters

Observed Fraud and Cybercrime Trends

Commission Fraud: Current Trends and Controls

Commission fraud, including practices such as cash looping and transaction splitting, remains a common risk in DFS ecosystems.

TRENDS

- Commission fraud remains common in DFS ecosystems.
- Key examples include cash looping and transaction splitting.
- Often involves agents exploiting commission structures.

DATA TABLE (CENTERPIECE)

Q1 2025 Commission Fraud Mitigation Outcomes

Metric	Value
Attempted cases blocked	~99%
Losses prevented	M645,000+
Impact	Demonstrates effectiveness of controls

CONTROLS SECTION

Control 1: Rule-Based Monitoring

Implementation of rule-based monitoring systems to flag suspicious transaction patterns.

Control 2: Agent Training

Providing comprehensive and ongoing agent training to reduce fraud risk.

> **"Well-designed controls and continuous monitoring can significantly reduce commission fraud risk."**

Social Engineering – Domestic Market Trends

Reported trends indicate social engineering remains a significant threat in the domestic market.

Vishing (Voice Phishing)

Fraudsters call victims pretending to be DFS providers. Goal: steal PINs, OTPs, or personal details.

↓

- Vishing and smishins pretending to be DFS providers. Goal: steal PINs, OTPs, or personal details.
- Fraudulent SMS messages requesting OTP or PIN. Often disguised as urgent security alerts.

Smishing (SMS Phishing)

Fraudulent SMS messages requesting OTP or PIN. Often disguised as urgent security alerts.

Combined Attacks

Vishing + Smishing used together. Increases credibility and success rates.

Key Insight: "Vishing and smishing are the most prevalent and are often used together to increase credibility and success rates."

Payment Process Weaknesses Serve as a Driver for Fraud

Root Cause

Weak Processes

Some fraud incidents arise from weak or poorly aligned processes, rather than deliberate system breaches.

Fraud Examples

Examples of Process-Driven Fraud

- **Double withdrawals** Occurs when system controls and operational procedures are not fully aligned.
- **Misuse of group savings** (e.g., airtime/value-added service) where authorization is weak.

Control Measures

Needed Controls

- ✔ Strong internal controls
- ✔ Clear segregation of duties
- ✔ End-to-end process alignment

Fast Payment Systems: Emerging Fraud Risks

Fast payment systems, such as LeSwitch, have introduced new fraud risk dynamics.

New Fraud Risk Dynamics

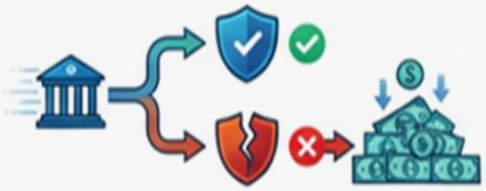
Fraudsters exploit speed and interoperability of fast payment platforms.

Common Fraud Patterns

- Rapid fund movement across providers
- Quick cash-out during off-peak or unusual hours

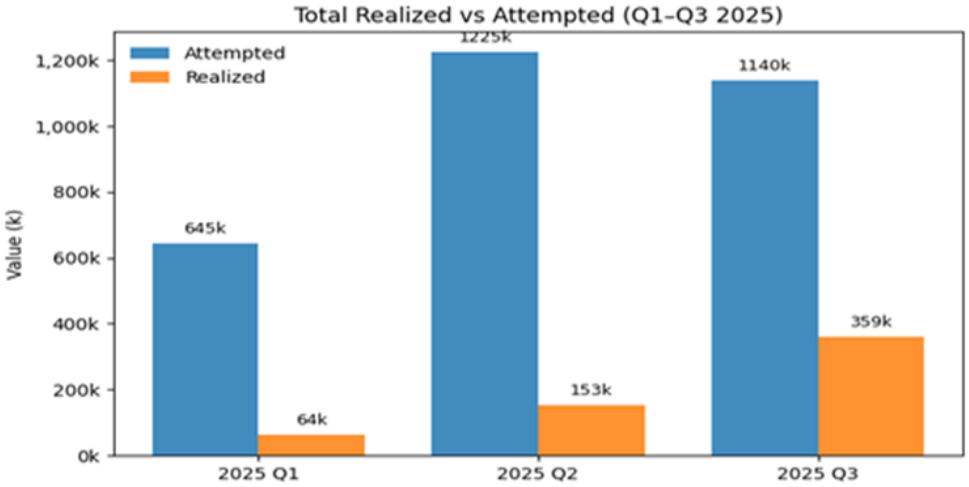
Amplified Risk Without Controls

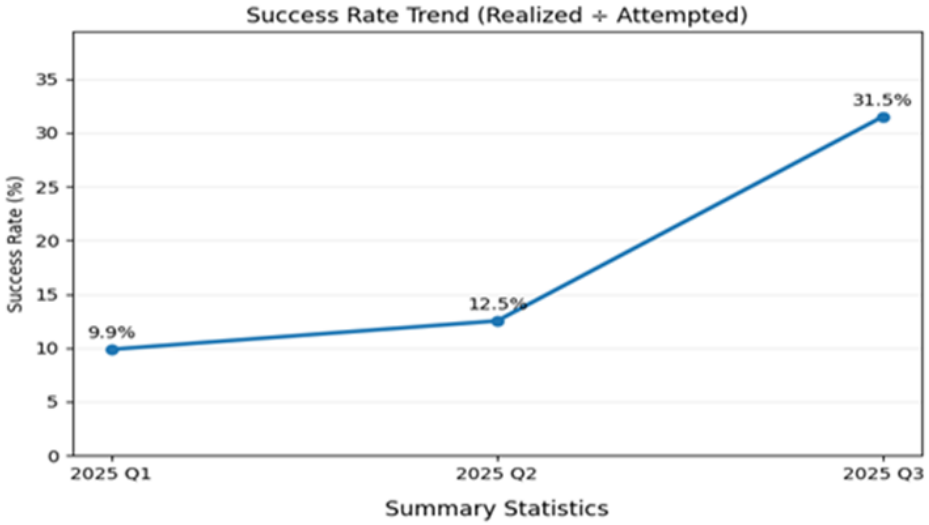
Without real-time DFS fraud monitoring and coordinated inter-provider response, the speed of fast payment systems can amplify fraud risk.

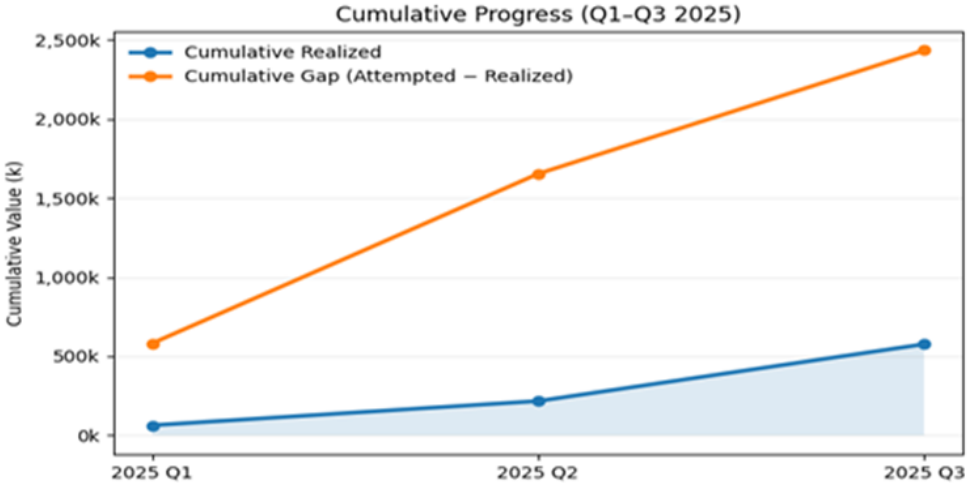


"Speed and interoperability are benefits only when paired with real-time monitoring and coordinated responses."

Quantified DFS Fraud and Cybercrime





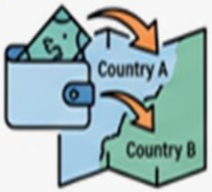


Total Attempted	3,010k
Total Realized	576k
Overall Success Rate	19.14%
Total Gap	2,434k

Regional & Cross-Border Dimension

DFS fraud is not confined to national borders; it is increasingly regional.

2 Fraud typologies in Lesotho mirror SADC trends



Cross-border wallet abuse

Exploitation of interoperable and fast payment systems

3 Shared risk patterns require regional coordination

4 What is needed

Stronger cooperation among central banks

Collaboration with regional cybersecurity & CERT teams

Harmonized supervisory & regulatory approaches

Priority Actions

- Formal DFS fraud coordination structures


Central Bank Initiatives
DFS Security Lab (CBL, LCA, ITU)
DFS Security Guidelines
Cyber & Information Risk Guidelines
Fraud Reporting Templates
ALERT!

Conclusion & Way Forward

- ✓ DFS Fraud and cyber crime is now a systemic risk, cross-sector, and regional risk, extending beyond individual institutions.
- ✓ DFS users are exposed to significant financial losses, particularly from consumer-targeted fraud.
- ✓ Fragmented and institution-specific responses are insufficient to address the evolving threat landscape.
- ✓ Stronger coordination and information sharing among providers, regulators, and regional partners are essential to: Maintain trust in DFS ecosystems, Enhance consumer protection, and Safeguard financial stability.

Thank you

CENTRAL BANK OF LESOTHO

BANKA E KHOLO EA LESOTHO