



Closing the Implementation Gap on DFS Fraud and Cybercrime

From Policy Intent to Supervisory Practice



The Implementation Gap

The Real Challenge

- DFS fraud evolves faster than supervisory routines
- It requires collective action
- This is not a skills deficit; it's a hard operating environment
- The gap is operationalising policy into practice continuously



Emerging Fraud Typologies

What is Changing?



Social Engineering and
Authorised Scams



Agent/Insider-assisted
Fraud



Data-enabled Identity
Exploitation



Cross-border/
Platform Spillovers

Information Exchange Mechanisms

What Works?

- Standard data formats and typologies and common definitions
- Incident reporting thresholds and timelines
- Shared indicators (complaints, anomalies)
- Cross-sector exchange (finance, telecom, data protection, law enforcement)
- Cross-border and regional exchange
- Industry engagement

Shift from reporting of incidents to forward-looking information sharing

Coordinated Response

Sequence, Not Slogans



Practical Lessons

The Supervisor Playbook

- Market monitoring as the backbone
- Outcome-based supervision
- Standardise reporting before dashboards
- Cross-sector and cross-border coordination
- Continuous evolution and learning, not once-off training





+27 (0) 21 201 7299

info@digitalfrontiers.org

www.digitalfrontiers.org



Alliance of Digital Finance
and Fintech Associations

+27 (0) 78 754 3785

Sarah@alliancedfa.org

www.alliancedfa.org