Banks and Asset Managers: Key to Fighting Fraud and Protecting Consumers

• JOHANNES COETZEE

NAMIBIA's FINANCIAL SECTOR sits on the frontline front line against fraud, and it must play an active, coordinated role.

Namibian regulators, the Bank of Namibia (BoN), Financial Intelligence Centre (FIC), and Namibia Financial Institutions Supervisory Authority (Namfisa) publish guidance, warn about fraudulent investment schemes, and operate reporting channels.

BoN maintains an 'illegal schemes' contact via the email, illegalschemes@bon.com.na, phone 061 283 5111, and regularly issues public warnings.

The FIC is the national Financial Intelligence Unit with statutory reporting channels for suspicious transaction/ activity reporting (STR/SAR) and publish typologies and annual reports that show fraud and money laundering trends.

Namibian authorities and international partners have recently put a spotlight on scam networks, e.g. Interpol action recovered assets and exposed scam rings operating in the region. Namibia was placed under Financial Action Task Force (FATF) increased monitoring (grey listing since February 2024).

This exemplified the urgency of robust anti-money laundering/anti-scam measures. Due to increased banking regulations accompanying grey listing, it complicated transfers and payments across the Namibia-South African border.

Actions banks, regulators and asset managers should take are discussed as follows.

1. Core roles of banks & asset managers

- Strong risk-based know your customer (KYC)/CDD: implement enhanced customer due diligence (CDD) for higher risk clients and for higher-value or unusual products; adopt simplified CDD only where legally appropriate. This helps block scammers from opening accounts or onboarding fake entities.
- Transaction monitoring tuned to local typologies: deploy rules and analytics to detect typical fraud patterns e.g. rapid withdrawals, multiple small deposits from different payers, sudden transfers to overseas accounts, layering behaviour, and integrate FIC typologies.
- Secure digital channels and authentication: enforce multi-factor authentication, device profiling, and tokenisation. Strong password rules, and in-app/card-not-present and account takeover fraud. Local banks already publish consumer guidance – scale and standardise those controls across institutions. However, often banks are not available 24 hours a day, especially not after hours for halting suspicious transactions.

2. Detect & report - faster handoffs to FIC & law enforcement

- Mandatory, timely STR/SAR to the FIC using the official electronic reporting platform. Build easy internal escalation paths for frontline staff to rapidly file good-quality STRs.
- Share anonymised typologies and indicators of compromise (IoCs) through industry fraud forums and with the FIC/BoN, while respecting data protection. Establish a secure information sharing mechanism, e.g., secure portal and regular taskforce. -The FIC and banks must be much more transparent in logging and reporting to industry fraud forums where the public is the most critical stakeholder.

3. Protect consumers - product safeguards and disclosure redress

- Plain-language disclosures at account opening and before investment product sale and allocating fees. Cooling-off periods, risk warnings about unsolicited offers, and examples of common frauds, e.g., phishing, vishing, and investment promises. Banks and regulators should standardise messages, so consumers receive consistent advice.
- Fraud-friendly product design: e.g. require two-person approval for high-value transfers, confirmations for beneficiary changes, and mandatory holds or verification for first-time external beneficiaries.
- Fast freeze and remediation policies: Publish and operate a rapid 'freeze' pathway to block suspected scam transactions and return funds when fraud is proven. e.g. as should have been implemented by banks and regulators over several years in which Fishrot and SME Bank money laundering have occurred. Offer clear complaint escalation and consumer ombudsman process and publish it. Banks in Namibia does have a Bbank Oombudsman. However, the low profile of the Oombudsman leaves much to be desired in executing this role.
- Basic bank account financial inclusion: Ensure safe, low-cost basic accounts with built-in protections for vulnerable consumers, e.g. the elderly and low literacy customers, building on existing basic account initiatives. Protection should include biometric information, e.g. iris and fingerprint recognition.

Johannes Coetzee

> "Namibian authorities and international partners have recently put a spotlight on scam networks, e.g. Interpol action recovered assets and exposed scam rings operating in the region.
>
> – Johannes Coetzee

4. Educate and empower the public - continuous, and targeted awareness

- Nationwide, multilingual education drives: Coordinate with BoN, FIC, Namfisa and large banks to run regular campaigns, e.g. radio, social media, SMS, and community outreach, which explain red flags, how banks communicate. e.g. banks will never ask passwords. Other include how to verify investment offers, and where to report uncertainties. BoN issues warnings and blog posts, and scale these to regular and targeted programmes. However, these regulators, have enormous potential to upscale their reporting and halt suspicious transactions of well-connected business people businesspeople and high-level politicians. re.g. deliberate oversights to prevent the corruption that occurred in the Government Institutions Pension Fund saga, Fishrot, SME Bank, Namib Desert Diamonds, and National Petroleum Corporation of Namibia.
- Targeted campaigns for at-risk groups: Sstudents, e.g. viral job fraud gangs, the elderly, e.g. romance and/or phone scams, and small businesses, e.g. invoice fraud. Use behaviourally informed messaging and real case examples for raising public awareness. Increasingly, financial institutions use passwords combined with one-time PINspins.
- Easy reporting channels and guidance: Publish FIC reporting steps, BoN hotlines and bank fraud hotlines – and create a single webpage or checklist for 'I think I have been scammed – do this now.'

5. Victim support – trust, reputation and social responsibility

- Resolute victim support teams: Provide immediate steps, e.g. freeze and change credentials, consult with law enforcement, and a case manager to guide victims through recovery and compliant processes.
- Financial relief policies: Restitution programmes for victims of scams and publish criteria to create public trust in support when scammed.
- Transparency and reporting on outcomes: Publish anonymised yearly scam loss figures and remedial outcomes to restore public trust and illustrate the financial sector's commitment.

6. Collaborate & public policy advocacy

- Formal partnerships between regulators and the Namibian Police,. Telecom Namibia and payment processors to share data, coordinate takedowns and close scam call centres and/ or phone numbers.
- Advocate for pragmatic law and regulation: Better civil mechanisms to freeze assets, improved cross-border cooperation, stronger sanctions for facilitators, and data sharing rules that balance privacy and prevention. Cross-border enforcement actions should demonstrate the value of coordinated actions. Interpol depends on diplomacy, which should be possible within the Southern African Development Community and the African Continental Free Trade Area Agreement countries. However, South Africa is a hub of illegal activities in which scammers participate in advance-free fraud, the '419 Nigerian fraud'.

To synthesise, within the context of profit margins of banks, and oversight duties of financial regulators, these institutions have tried but are underperforming in preventing fraud. The customer is at risk. It is time for change.

Johannes Coetzee is an associate professor in the Public Management Department: Governance and Management Sciences at the Namibia University of Science and Technology.