SIX

COMBATING FINANCIAL CRIME

Effective anti-money laundering systems protect the integrity of the financial system, which is crucial to economic and social development. The banking system plays a central role in collecting and moving funds. Banks detect and report suspicious financial transactions, which is vital in preventing fraud, corruption and money flows to criminal syndicates and terrorist organisations. Cybersecurity is a growing concern.
Standard Bank has robust controls to protect system integrity and the security of our clients' funds.

PREVENTING FINANCIAL CRIMES

Our role as a trusted partner depends on the reliability of our services and our clients' confidence in our ability to protect and grow their assets. In 2017, Global Finance Magazine named Standard Bank as the Safest Bank in Africa in its annual ranking of the World's Safest Banks. We were also named Safest Bank by Country in Kenya and South Africa.

"I'm proud I was able to protect my bank from reputational damage."
– FraudStop winner 2017: Sibongile Dube, team leader of personal markets, Vanderbijlpark, Standard Bank South Africa

Preventing and mitigating fraud

In South Africa, we're introducing fingerprint verification to strengthen the security of our authentication process and better protect customers from impersonation fraud. We've partnered with the Department of Home Affairs to improve the accuracy of our client records. When a new customer opens an account with us, we copy and store their fingerprint, and check it against the Department's population register for authentication.

Our employees are our first line of defence in identifying, reporting and exposing suspected fraud. FraudStop is an ongoing campaign within the bank, to raise awareness and to reward employees who successfully prevent financial crime by reporting fraud. In 2017, Sibongile Dube won the R1 million prize for her quick thinking and immediate action that protected a customer from fraud.

Avoiding debit order fraud

Debit order fraud has become a significant concern in South Africa, leading to disputes between clients and banks. The South African Reserve Bank instructed the Payments Association of South Africa and South African banks to address this issue. The result is DebiCheck, a controlled debit order system intended to ensure fair management of debit orders and customer security.

Protecting our clients and business partners' assets and data is a priority for us. This is an industry-wide and societal issue, and collaboration is crucial. We actively contribute to SABRIC forums for collaboration between banks on combating cybercrime.

– Graham Blain, Head of IT governance, Standard Bank Group

Fighting cybercrime

2017 saw a continued focus on improving cybersecurity capabilities.

THE GLOBAL CHALLENGE

- Increasing cybercrime incidents
- Sophistication of attacks.

Cybercrime includes:

- cyberfraud
- data theft
- extortion (ransomware)
- malicious business disruption.

The escalation in the scale and sophistication of cybercrime is amplified by:

- growing digitisation of businesses
- ageing and vulnerable IT systems.

OUR SOLUTION

- Extensive focus on cyber risk at every level of the organisation
- Investing in enhanced security capabilities.

THE IMPACT

In 2017, we **mitigated** several attempted attacks, without any impact on our operations or customers.

Many of these incidents were **prevented** as a direct result of the advanced cyber defence capabilities introduced in 2016 and 2017.

Cyber regulation is evolving worldwide. Most banking regulators will probably issue cyber regulations in 2018. The South African Reserve Bank (SARB) issued guidelines to banks for developing resilient systems that can recover quickly in the event of a cyber incident. In 2017, Kenya's Central Bank has also issued similar guidelines.

The banking sector and the relevant authorities are collaborating well. We regularly send security tips to our clients, and contribute to the growing of awareness on cybercrime topics.

The international shortage of cybersecurity skills is well documented. We have employed eight graduates who will be guided through specialised training towards becoming cybercrime specialists.

The number of phishing sites targeting Standard Bank clients reduced significantly in 2017, as did the number of online banking fraud incidents reported. We believe this was largely due to implementing new prevention and detection controls.

The Cybercrime and Cybersecurity Bill

During 2017, the Department of Justice (DoJ) led the drafting of the Cybercrime and Cybersecurity Bill. Standard Bank worked closely with industry bodies, particularly the Banking Association of South Africa and the South African Banking Risk Information Centre, to provide feedback on drafts, towards helping ensure that the legislative objectives are fulfilled, while minimising unintended impacts.

Following constructive engagements between the DoJ and various stakeholders, including the banking sector, we are confident that the Bill aligns well with the current realities of cybersecurity, and will be useful in preventing cyber-related crime.

Money laundering, terrorist financing, illicit financial flows

We're piloting an enhanced compliance management and monitoring capability using an integrated data analytics capability. The bank is automating parts of the high traffic processing operations for anti-money laundering controls. This will enable real-time data analytic problem-solving capability during 2018. Our Money Laundering Surveillance Unit has established a dedicated team to track adverse information linked to Standard Bank clients. This team will identify risks introduced to the bank by clients and respond quickly to analyse and address these, as necessary.