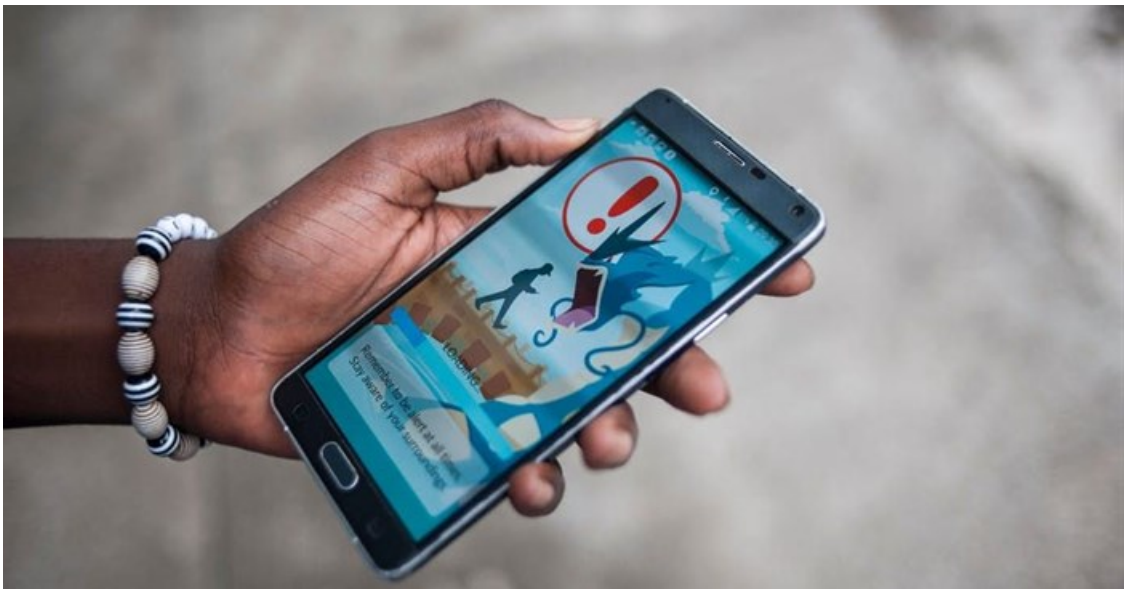
BIZCOMMUNITY

Electronic banking fraud in Nigeria: how it's done, and what can be done to stop it

By Oludayo Tade

24 Jun 2020

Six years ago, a cashless policy became fully operational in Nigeria. The aim was to encourage electronic transactions with a view to reducing the amount of physical cash in the economy. The logic was that this would minimise the risk of cash-related crimes.



A warning sign advising users to be aware of their surroundings while playing a video game. Stefan Heunis/AFP via Getty Images

But a major downside of the policy has been pervasive electronic banking fraud (e-fraud). Although the cashless banking system was designed to foster transparency, curb corruption and drive financial inclusion, it's threatened by the growing perpetration of fraud.

About N15.5 billion was lost to bank fraud in 2018. About 60% of the fraud was perpetrated online owing to available internet-based and tech-rated banking services.

Our research investigated dimensions of electronic fraud in Nigeria. We found three: internal fraud carried out by banking staff; external fraud carried out by ordinary Nigerians; and collaboration between fraudsters and banking staff.

We found that inefficient supervision, non-performance of oversight by regional heads of banks, and poor follow-up on

customers' addresses (Know Your Customer) accounted for the fraud that took place.

Our study provides the banking industry, banking public and investors with critical pointers on how to reduce fraud.

Different types

Our study involved collecting data as well as conducting interviews with 30 people. These included victims of bank fraud, bank customers who did not subscribe to the cashless policy and fraud detectives at the Economic and Financial Crimes Commission (EFCC).

These were the common patterns we uncovered.

Insider fraud: By insider, we mean those working with banks or those in a relationship with account holders. Here, the fraud was exclusively executed by members of staff in the banking system who exploited the strategic position they held in the system and their grasp of how it works. Banking institutions and customers were their victims

An example we came across during our research was the case of a N90m ($452,261) fraud perpetrated by an account officer of a major eatery in Lagos State. The job of this account officer was to collect the eatery's takings and deposit them at the bank. A fraud detective told us that: "As the account officer he would collect money on a daily basis and was expected to credit the company's account. However, he would collect money on Monday and lodge it and collect on Tuesday and not lodge it. He was missing one day out. He did this continuously until he was able to rake in N90m. At this time, when the eatery management raised the alarm on their account, he ran away and could not be found. We however used his sister to arrest him. We were only able to recover N8m from him. He had used part of the money to organise his wedding, had a baby and almost completed a four-bedroom bungalow at another area in Lagos."

Bank fraud is often successful because many Nigerians don't subscribe to transaction alerts. The eatery management trusted their account officer but did not know that he was dishonest.

Outsider fraud: These perpetrators were external to the banking system. They thrived on their internet skills and sometimes on their understanding of the victims' routine and identity.

An example we came across was the fraudulent use of bank verification numbers (BVN). These were made compulsory by the Central Bank of Nigeria in 2014. All bank account holders had to undertake biometric registration. The intention was to ensure security and check fraud.

But fraudsters have found a way to cheat the system by sending bank customers false emails asking for their bank verification details. As one victim explained to us: "I needed to make some transactions and I headed for my bank. I had called my account officer ahead of time. On getting to the bank, I connected my computer and got a mail from a supposed same bank. I was asked to click on a link and supply my BVN details for update of my account or face service suspension on the account. I just clicked the link and supplied my details and behold, N1m debit alert came on my phone within five minutes! I was shocked and devastated but before we could do anything they had withdrawn everything."

Collaborative fraud: This involved collaboration between bank staff and fraudsters outside the banking system. Banks and individual account holders were the victims. For example, bank staff could provide account details of customers to the collaborating fraudster.

Governance gaps

Despite this weak governance architecture, which is still not fraud proof, bank executives reported having in place mechanisms which had limited the incidence of fraud. One was sending out information to customers who subscribed to electronic alerts. Through this, banks contact and send anti-fraud messages to their customers.

Owing to reputational risk, banks try to refrain from public prosecution of erring staff. We found that banks adopted shaming as a mechanism for instilling discipline within their organisations while attempting to ease out “bad eggs” through flagging of their images on computers and across the banking industry.

There is a need to check fraud through customer awareness and financial literacy education.

While fraudsters continue to design new ways of working on customers’ vulnerabilities, Nigerian banks need to use the Cybercrime Act to prosecute offenders as a way to boost confidence in the banking sector and deter fraud in the future.

ABOUT THE AUTHOR

Oludayo Tade, researcher in criminology, victimology, electronic frauds and cybercrime, *University of Ibadan*