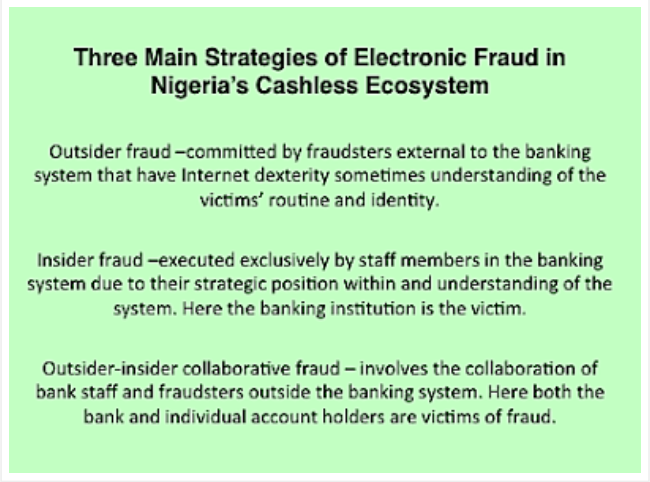
Sunday, November 20, 2016

Diverse Strategies of Banking Fraud in Nigeria

By IMTFI Fellows Oludayo Tade and Oluwatosin Adeniyi

A major snag since the introduction of Nigeria's cashless policy is pervasive electronic banking fraud (e-fraud). Although the policy was aimed at encouraging electronic transactions, reducing physical cash in the economy and thereby reducing the risk of cash related crimes, fostering transparency, curbing corruption/leakages and driving financial inclusion, the perpetration of fraud threatens the cashless ecosystem. The implications of rampant e-fraud are enormous, not only for the banked population adopting e-banking as a secure platform but also for the obstacles it poses to effectively capture the unbanked populace. Initial investigations show that with the prevalence of fraud and subscriber victimization, there is a growing fear of migrating to and using electronic banking, while those defrauded are altogether opting out of e-banking. The Nigeria Deposit Insurance Corporation (NDIC) annual report stated a total of 3,756 fraud cases in 2013 involving N21.79billion, which represented a 21 percent increase from 2012. Curiously, about half of the actual loss occurred within the first three months of 2013. Looking between these aggregate pictures, the NDIC 2013 report also offers an elaborate list of fourteen major fraud channels - automated teller machine (ATM) fraud being the leading source. In a climate of mounting complaints from e-banking customers/subscribers, we investigated the dimensions of e-fraud in Nigeria's cashless ecosystem. We collected data in Oyo, Ogun and Lagos States and employed qualitative methods of in-depth and key informant interviews with fraud victims, bank officials and fraud investigators at the Economic and Financial Crimes Commission (EFCC).



Opportunistic Kith and Kin

ATM fraud has continued unabated due to the breach of trust between account holders and fraudsters. Most ATM fraud was carried out by persons very close to the victim including spouses, boyfriends, and friends (Tade and Adeniyi, 2016). Often, online fraud is successful through selective identification and exploitation of victims' vulnerabilities by dexterous and savvy offenders. In a case reported to us at a new generation bank in Nigeria of a lady and her fiancée, the man had taken the lady's ATM card and made a withdrawal of about N300, 000. Getting the 'surprise debit alert', the lady lodged a complaint with the bank. The ATM custodian at the bank informed us that the lady threatened legal action against the bank. When the fraud alert was subject to internal

< Back to IMTFI home page

Posts by guest bloggers are those of the author and do not necessarily reflect the views of IMTFI.

scrutiny, it was found, through the Close Circuit Camera Television (CCTV) footage that it was actually her husband-to-be who made the withdrawal without her consent. According to the ATM custodian:

She was shocked seeing her man making the withdrawal. Her countenance changed and she felt sorry for raising her voice in the banking hall. She later left the banking hall to reconcile with her fiancée.

ATM withdrawals

In some instances, bank staff collaborates with fraudsters outside the bank. Outside fraudsters recruit people who have access and occupy sensitive positions within the bank such as sweepers and those in the Information Communication and Technology (ICT) unit. Not all participants are fully aware of their role or final purpose of their assignment. A fraud investigator we interviewed at the EFCC summarized a case as follows:

This fraud was huge. It involved the moving of about N400million ($2,010,050) naira from the account of the bank. It involved some bank staff in the ICT unit and those in the regular banking hall. They got a woman who sweeps the office of the branch manager and gave her a key-logger to insert in the computer to extract the necessary data they needed and security information. Through this, they were able to access the banks account and moved the money into about forty different accounts. They were strategic about their fraud. They waited for the day there was public holiday and then moved all the money and almost immediately withdrew from the different bank accounts. Before they could be stopped they had used more than three-quarter of the money to buy things online. It was the sweeper that eventually sold them out because as she claimed, she did not know that the things they gave her were to defraud the bank.

Un-credited Lodgment

Un-credited lodgment is another type of fraud perpetrated by bank staff using their knowledge of banking operations and technicalities. We found that the compromised bank staff in the cashier section would collect cash lodgment but would deliberately fail to credit the customer's account and later divert the money for personal business. This strategy was successful unless the account owner lodged a complaint for not receiving an alert regarding the payment he/she made. It should be noted that not all account holders subscribe to account transaction alerts that give them information about any transaction on their account. People often don't want any deductions to be made on their account for subscribing to this service. Fraudsters, therefore, prey on this loophole.

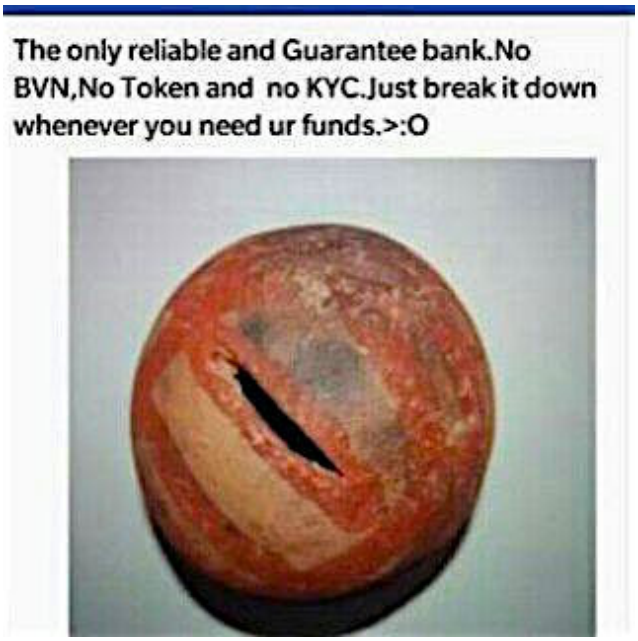
A PhD candidate who shared his victimization experience on un-credited lodgment stated:

I had a nasty experience with this electronic banking. I went to make a lodgment of N50,000 ($251.2) into my bank account and I went back home. Two days later I did not receive a deposit alert. I went to the Bank Manager to complain who asked me to come back. A lady cashier from the bank came to my house; apparently she traced the address through the Know Your Customer form I filled. She told me to come to the bank as I was the one who made mistake in the payment. I was angered by this and I told her what nonsense. She later told me she thought I was working with a businessman who benefits

from uncredited lodgment which he uses to do a business for about two weeks and then payback before the account of the lodger of the funds will be credited. Two hours she left my house, I got the credit alert.

This experience brings to the fore the issue of customer knowledge about banking operations and security features to help stop fraud. Those who do not subscribe to account alerts may have their monies un-credited and used for 'arranged' businesses by some compromised bank staff and their outsider accomplices.

Bank officials are also often associated with dormant account fraud (DAF). When an account has remained inactive for about 6-months, it is categorized as dormant until the account owner applies for its re-activation. In Nigeria, when a person dies it is difficult for dependents to access the bank accounts of their benefactors owing to many legal/institutional obstacles that can take months or even years to be resolved. Some family members are oblivious to the fact that the deceased even had a bank account. As a result, when the account holder dies, their funds become targets for bank official fraudsters, with insider knowledge, that then reactivate and withdraw money from the account.



'Kolo'- a trusted indigenous saving object being used to highlight fraud in the cashless ecosystem

Weak Governance Structure in the Cashless Ecosystem

We also found that weak governance structure is responsible for electronic fraud in Nigeria's cashless ecosystem. This weak governance is at the level of both banking institutions and regulating agencies. Our data indicated that there was poor supervision at the branch, regional and zonal levels of some banks where fraud, get perpetrated. A bank staff person stated:

There was a fund transfer fraud in which the best man we had for that job was involved in but rather than punishing him and sending the report to the regional head, the Branch manager decided to make it an in-house thing. They forced the man to fill a loan form where they were deducting the money he fraudulently made from customers account. They also moved him to another unit within the bank where he did not have direct access to money. The matter was resolved internally within the branch.

Such fraud neutralization strategies were adopted to cover the tracks of inefficient supervision, which kept compromised personnel within the banking system creating a weak governance and accountability structure. The Committee of Chief Compliance officers of Banks in Nigeria (CCCOBIN) at their meeting of October 29, 2015 also noted:

Banks in a bid to cut cost and increase profitability recruit contract staff and assign them to very sensitive areas of the Bank's operations and because these categories of employees are poorly remunerated they are susceptible to all sort of vices, including

fraud.

Due to increasingly neoliberal policies being adopted in banking operations, the majority of bank staff is not full-time but casualised and the NDIC's 2014 fraud report stated that contract/casual staff perpetrated 64% percent of frauds committed in banks.

The strategies used in perpetrating fraud, such as un-credited lodgment, fake job scam, ATM card swapping and compromise, fund transfer fraud, phishing emails/BVN fraud, and dormant account fraud among others, indicate that fraudsters are exploiting the loopholes of the cashless ecosystem. The results of this study point to the need for financial literacy education in Nigeria and improvements in the security infrastructure with a view to building confidence in the formal banking sector as well as e-banking. Furthermore, banking products/services should be designed with security features that take into consideration the peculiar characteristics and vulnerabilities of their customers.

All names of banks, institutions and participants are pseudonyms as they were assured of their anonymity when they agreed to participate in the research.

Reference
Oludayo Tade and Oluwatosin Adeniyi (2016), "On the limits of trust: characterising automated teller machine fraudsters in southwest Nigeria", Journal of Financial Crime, (2016) Vol. 23 Iss: 4.

Read more in Oludayo Tade and Oluwatosin Adeniyi's Final Report.

Posted by Mrinalini Tankha at 10:44 PM

Labels: ATMs, fraud, kinship, Nigeria

No comments:

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)