Fraud in the Nigerian Financial Services

2nd Edition
Content

01 A realm of continuous innovation
03 Impact of COVID
04 Importance of data
05 Mitigating fraud risks: Customer education
06 Collective commitment to the industry
A realm of continuous innovation

Fraud. A common word, and a global phenomenon that seeks to take advantage of vulnerabilities in various systems in order to criminally achieve a financial gain. Nigerians have long been perceived to have perpetrated some of the most cunning and inventive scams, so much so that our reputation around the globe has been negatively impacted by this trend.

While this reputation predates the advent of electronic payments in Nigeria, it has continuously evolved to the extent that financial institutions and service providers alike are constantly on the lookout for odd behaviour to ensure that any potentially fraudulent behaviour is nipped in the bud.

It is no secret that Nigeria has some of the most advanced electronic payment capabilities in the world. Ironically, this stems from our own need to ensure transparency in payments, a feat that can only be achieved when there can be quick or near-instant feedback between the participating institutions.

However, the increase in transaction processing speed and available channels comes with an unavoidable side effect – more vectors for fraudulent transactions. This has been observed in many countries across the world. When the faster payments network was implemented in the United Kingdom, financial institutions saw as much as 300% increase in fraud. As adoption of Zelle was growing in the U.S, some institutions reported a 90% fraud rate on transactions.

Analysing the industry fraud data in Nigeria as at Q3 2019 and 2020 (January to September), similar growth trends can be easily observed. Growth in the use of electronic channels, specifically mobile devices, has also enticed fraudsters into focusing their efforts on these electronic channels.
While the channel distribution shows only a moderate shift of fraud attempts towards mobile and web channels year on year, analysing the total number of fraud attempts shows a more alarming narrative. The data shows that the total number of attempts as at Q3 (January to September) has grown by 186% from 2019 to 2020. Expectedly, fraud attempts via mobile channels saw a 330% increase YoY, while attempts via web and POS channels saw a 173% and 215% increase YoY. This trend is expected to continue as Nigeria further grows financial inclusion and customers become increasingly dependent on electronic channels for their day to day transactions.
Impact of COVID

The COVID-19 pandemic presented a new challenge for all. People, businesses, even governments all had to adapt to a "new normal". Industries have been radically disrupted in a way that has not been experienced for generations. Principal among the changes that had to be instituted was the requirement for contactless and remote interactions. This led to increased efforts from fraudsters in the area of social engineering.

Globally, there has been a marked increase in threat levels in the wake of the pandemic including a near-sevenfold increase in spear-phishing attacks. Customers and remote personnel are also being bombarded with attacks based on COVID-19-crisis themes that are taking advantage of delayed updates to email and web filters and using social engineering to prey on workforce concerns.

Meanwhile in Nigeria, the pre-COVID trend shows a substantial increase in reported fraud activity. However, a drop-off in the trend was observed post-COVID. This presents a welcome respite for institutions, as it provides a unique opportunity for additional security measures to be instituted before economic activities fully resume.

We are aware that criminals will always use ‘disruption to cause disruption’ and this pandemic has caused the greatest interference to human life and economic activity in more than a generation. Therefore this period presents an opportunity for financial institutions to counter expected new tactics from criminal elements. New potential points of vulnerability across platforms and new digital banking converts need to be proactively engaged to ensure resilience against fraud attacks.
Importance of data

Data remains, by far, the most important tool in the never-ending anti-fraud battle. Only by taking deep dives into the historical trends and activities can we effectively chart a course to the future we desire.

The role of data in accurate decision making cannot be overemphasized. The Industry Antifraud portal continues to allow financial institutions to report data on attempted and successful fraudulent transactions. This data allows us all to better understand the behaviours of fraudsters as well as the characteristics of the victims. This allows for more effective and targeted measures that will provide benefits to all players in the Nigerian financial services industry. Applying data analytics to noticed trends will enable proactive identification of suspicious activities and provide the ability to act quickly to frustrate fraudulent transactions.

On a global scale, fraudulent activities have resulted in losses amounting to about USD 42 Billion. Approximately 39% are perpetrated by external parties while 37% are perpetrated by internal parties.

Diving deeper into Nigerian industry data, the actual figures reported by the industry are quite striking. This year, about 91% of all fraud attempts as at September have resulted in a total loss, and more than NGN 5 Billion was lost as a result of fraud within the same period. This presents financial institutions with an opportunity to protect their investments as well as attract customers by offering increased antifraud protection and the ability to recover lost funds more easily.

Data Enhances Decision Making
Mitigating fraud risks: Customer education

Institutions need to keep in mind that as the threat of fraud looms over the industry, this field requires continuous innovation. As the fraudsters evolve, so must we. Ability to anticipate the action of the fraudsters is key.

Social engineering remains one of the principal ways in which fraudulent activities are attempted. Simply put, social engineering is a broad range of techniques that involve manipulating a victim into giving away sensitive information using psychological manipulation. Data from the industry antifraud portal data shows that ~56% of all reported fraud attempts were carried out using social engineering.

It stands to reason therefore, that institutions need to focus resources on user education. This includes both internal and external users. Recently, the world of social media was taken over by a storm based on the recent Twitter hack. This exploit was made possible due to the negligence of Twitter personnel coupled with the general unwariness of internet users.

Institutions need to be poised to promptly detect and block any such fraudulent activity from negatively impacting the customer’s perception of their platforms and products while also ensuring that customers are informed and perceptive enough to identify and reject any such offers.
Collective commitment to the industry

NIBSS role as the Nigerian central switch means that we process upwards of 10 million transactions on a daily basis. Statistically, even a 1% successful fraud rate would result in 100,000 successful fraudulent transactions daily. This would directly impact customer’s faith in the entire system and could significantly impact our financial inclusion drive as well as the CBN cashless policy. This remains the largest hurdle to overcome as it relates to fraud, as the inaction of a single institution in the financial value chain could potentially undermine the measures taken by all others and negatively impact the entire ecosystem.

The ever-increasing digital transformation of the Nigerian financial services landscape results in significant changes to the traditional risk landscape for institutions and the entire sector.

Dated risk assessments, policies, procedures and controls may result in knowledge gaps that could result in potential loopholes that can be easily exploited by malicious persons intent on fraud, data theft or other illegal activities. Institutions will need to invest in state-of-the-art antifraud solutions that take advantage of the latest advancements in AI to provide suitable protection against fraudulent activity.

The antifraud battle can only be won when organisations institute a well round strategy involving sensitization, investments in well-suited technologies, risk management, effective governance, and industry-wide collaboration with relevant stakeholders.
1. Bank Innovation – Preparing for real-time fraud

2. TransUnion Online Fraud Trends post COVID-19
https://www.channelnews.com/insights/transunion-online-fraud-trends-post-covid-19-

3. PwC Global Crime and Fraud Survey
https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-

https://www.helpnetsecurity.com/2020/05/25/covid-19-online-fraud/