

Computer aided fraud and embezzlement: this is automated version of the good fashion manual fraud or embezzlement that has been going on for centuries by unscrupulous employees. Skilled data processing professionals usually perpetrate this type of computer fraud.

Time (or logic) Bomb or Trap Door: Convert instruments are written and inserted into a production programs or files, or cause application software, such as a payroll to or account receivable, or the whole system to crash. A time bomb is almost impossible to detect or prevent and it is almost impossible to catch the person who devise it because a clever programmer can write the instruments so that when the bomb erases the target program application or system, it destroys itself as well.

Scavenging: This is a method of obtaining data or information by searching trash cans of banks, data processing departments, this is called physical scavenging. There are also electronics scavenging that involves searching for residual data left in a computer.

Software piracy: It involves copying or theft of proprietary computer software and/or raw data or information. Moreover, if the criminal just copied the valuable software or sensitive data, it is almost impossible to detect the crime because the original software or data remains on the disk or in the computer.

CBN Report

According to CBN reports, year 2016 experienced a lot of innovation in the electronic payment space. New products and services, well driven by cutting edge technologies came to limelight which in turn led to an increase in the adoption of e-payment and transaction volume. For example, the ease of transacting with our mobile phones took a new dimension with the introduction of USSD. As we strive daily to improve our products and services, and also make electronic payment channels simpler to use, fraudsters are also not relenting in their efforts to take advantage.

The volume of fraud reported in 2016 compared to previous years attest to the fact that fraudsters do not grow weary. The more products and services that are rolled out without proper risk and impact analysis, the easier for the “bad guys” to perpetrate more fraud effortlessly. The determination and commitment of these unscrupulous elements cannot be underrated within the financial sector. The financial industry needs to ensure that more regulations and inter-industry collaboration are put in place to curb this trend.

Over the years, technology has played a vital role in the history of Nigeria’s financial space. From initiating funds transfer right from the comfort of our rooms, to paying utility bills without having to visit the service providers and uniquely identifying bank customers with biometrics, etc. Many cutting-edge products and services have been developed which in turn have changed the way we interact and transact. The ease, transparency and swiftness that technology brought to the financial ecosystem in Nigeria are noteworthy.

The directive by the Central Bank of Nigeria (CBN) for the establishment of industry fraud desks, sending of all electronic interbank transactions to the Central Anti-Fraud Solution

(HEIMDALL), introduction of biometrics to the ecosystem, and most importantly, our collaboration, have contributed to reducing fraud menace in Nigeria's financial space.

The Director, Consumer Protection Department, Central Bank of Nigeria (CBN) has said that electronic fraud losses in the banking system are projected to reach N6.1 trillion by 2021. He disclosed this at the workshop for Business Editors and Finance Correspondents, organised by Nigeria Deposit Insurance Corporation (NDIC) in Benin. According to him, the volume and value of e-transactions is projected to continue to increase nationally and globally.

The Director also said that the CBN, through its Consumer Protection Department (CPD), had resolved over 13,715 complaints which resulted in the refund of about N72.2 billion to customers by the commercial banks based on 25,043 cases of fraud in 2017. He said the amount represented a 28% increase if compared to 19,531 cases recorded in 2016. He disclosed that there was a 24% reduction in actual fraud loss value in 2017 with N1.63 billion as against the 2016 figures.

According to the Director, the statistics provided by the CBN shows there is a significant increase in the year-on-year volume and value of transactions across all payment channels in Nigeria. Consequently, 1.4 billion transactions with a value of N97.4 trillion were processed in 2017 as against 869 million transactions with a value of N69.1 trillion recorded in 2016. He said the increase of 59.7% and 40.9% were recorded in the volume and value of transactions in 2017.

As reported by CBN, the number of recorded electronic fraud cases in the banking industry increased by 28 percent in year 2017, rising from 19,531 in 2016 to 25,043 resulting in a loss of N1.63 billion. The banking watchdog, however, noted that the number of actual losses declined by 24.0 percent relative to that of 2016 and the attempted fraud value also declined in 2017, falling to N4.03 billion from N4.37 billion in 2016. As contained in the CBN 2017 Annual report, the volume and value of electronic payments in 2017 rose by 60.0 and 39.7 percent to 1,478.5 million and N99,292.3 billion, respectively, compared with 941.8 million and N71,100.00 billion in 2016. The rise was attributed to increases consumer awareness and confidence in e-payment channels.

Methodology

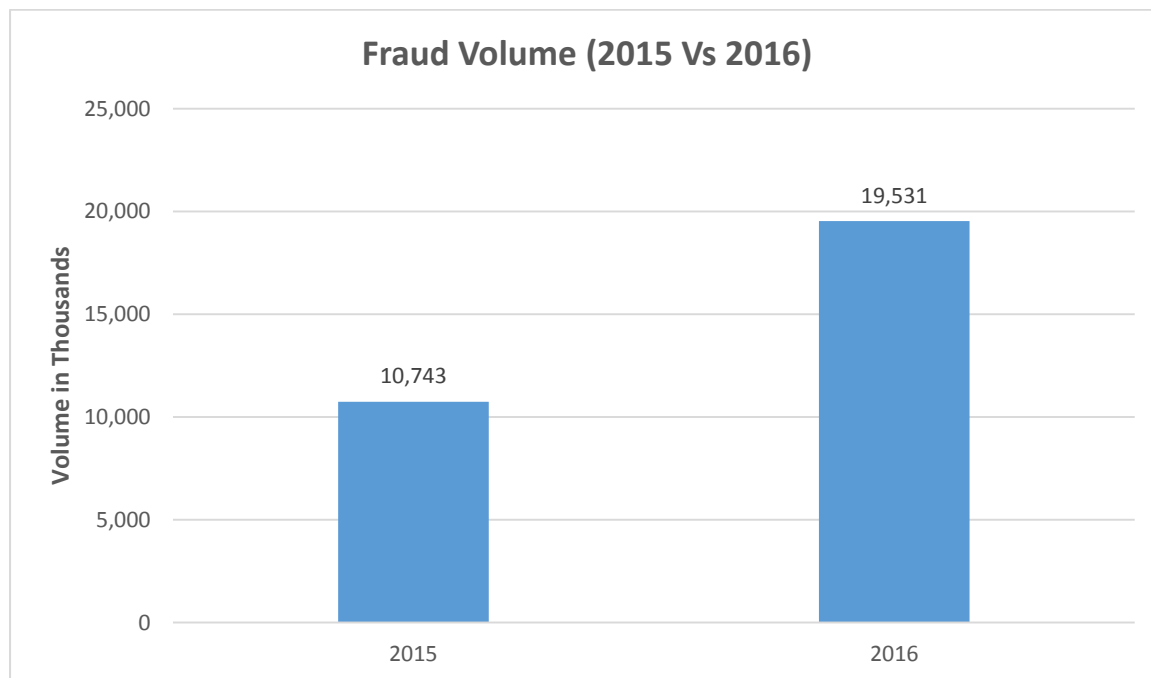
This study adopted case study research design of data collection, which was based on the use of secondary. The documentary data collection includes the number of e-banking products utilized, fraud volume, attempted fraud value and actual loss value in Nigeria for year 2016 which was compared with year 2015 figures. These were extracted from CBN: Nigeria Electronic Fraud Forum (NeFF) Annual Report, 2016 and the data were presented in tables and bar charts.

Results

The figure below shows that 19,531 fraud cases were reported for Deposit Money Banks in 2016 as against 10,743 in year 2015. Although, there was 82% increase in reported fraud cases as compared with 2015, we also witnessed marginal reduction in attempted fraud value

and actual loss is N 4,368,437,371.64 and N 2,196, 509, 038.78 respectively. Also, there was a decrease of 2.65% in actual loss due to fraud in 2016 when compared with 2015.

Year	Fraud Volume	Attempted Fraud Value (N)	Actual Loss Value (N)
2015	10,743	4,374,512,776.64	2,256,312,660.00
2016	19, 531	4,368,437,371.64	2,196,509,038.78

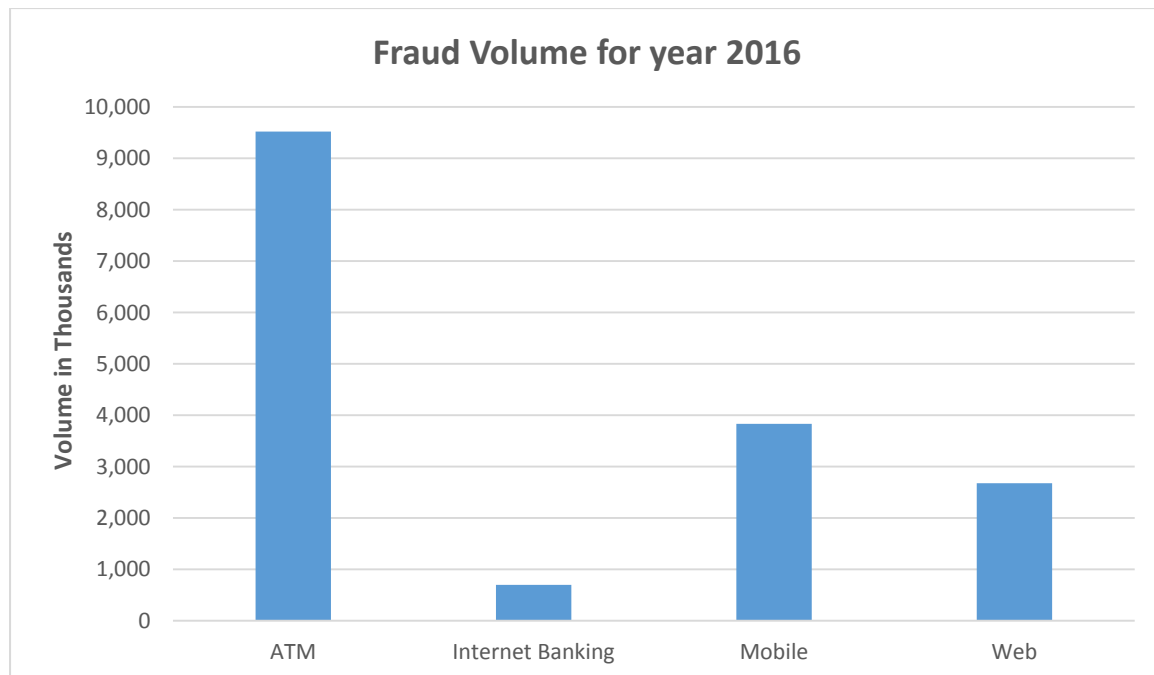


Fraud per channel

Exploring reported fraud events in the year 2016 and categorizing them according to channels, fraud perpetrated through the Automated Teller Machine (ATM) recorded the highest volume of fraud followed by Mobile. This is analogous to several emerging products and services riding on these channels which fraudsters are taking advantage of, especially mobile channel. The third most used channel to perpetrate fraud is Web.

Channel	Fraud Volume	Actual Loss Value (N)
Across Counter	325	511,072,861.29
ATM	9,522	464,514,684.27
Cheque	12	4,558,897.75
E-commerce	520	132,252,118.32
Internet Banking	698	320,665,957.87
Kiosk	3	10,198,000.00
Mobile	3,832	235,170,720.40
POS	1,658	243,321,812.67
Web	2,677	83,776,994.11
Others	284	190,976,992.10

Following the fact that we are concern with the bank electronic fraud in Nigeria, the diagram below only considered the following channels: ATM, Internet banking, Mobile and Web.



Summary of Findings

1. There is a significant relationship between e-banking practices in Nigeria and the rate of increase in the insecurity of banking transactions.
2. The practice of e-banking in Nigeria is significantly increased the volume of banking transactions.
3. The e-banking has tremendously improved the services of banks to their customers.
4. The e-banking operation has made the banking payment transactions easy and reduced the congestions in the banking all.

Effects of electronic fraud in Nigeria

Electronic fraud is fast becoming a potent threat to the Nigerian banking industry. There is an upsurge of e-fraud despite the many efforts to check cybercrime in the country. Undoubtedly, frauds lead to loss of money which belongs to either the bank or customers. This loss results in a decline of productive resources available to the bank. Adewunmi (1996), identified the under listed effects of bank frauds and forgeries:

- a. It destroys the bank's reputation
- b. It discourages banking habit among the banking public.
- c. The bank ceases to meet up with staff welfare.
- d. The trust and understanding among staff is reduced.
- e. The bank will lack the ability to compete favourably with its competitors.
- f. Fraud reduces bank's profitability.
- g. It places emotional and psychological burdens on the fraud victims.
- h. Others include: Increased operating expenses, reduced operational efficiency, damage to credibility, public criticisms, endangered bank's plans and strategies, bank's

liquidation, a decrease in foreign direct investments (FDI) and foreign investors, depletion of shareholders' funds and banks' capital base, and bad national image.

Prevention and control of electronic fraud in Nigeria

Although the incidence of fraud is neither limited to the banking industry nor peculiar to Nigeria economy, however, the high rate of fraud within the banking industry, calls for urgent attention with a view to finding solutions. Frauds in its effect reduces organizational assets and increases its liabilities. With regards to banking industry, it may engender crises of confidence among the banking public, impede the going concern status of the bank and ultimately lead to bank failure. It has become necessary to review and strengthen existing rules and enact new laws to stem the problem. Recommended solutions are:

1. **Issued of operating guidelines:** With the rapid growth in users and wider coverage of mobile phone networks, mobile banking is increasingly coming up as a significant delivery channel for extending banking services to customers. Putting the onus on banks, the Central Bank of Nigeria (CBN) should issue operative guidelines to regulate this channel, suggesting reporting of suspicious transactions to its financial intelligence unit.
2. **Deploying advanced tools and technology:** Owing to the heavy reliance on telecom operators for its services, the prevention and detection of frauds in mobile banking have become even more complex. To keep a check on frauds, banks need to incorporate a greater level of scrutiny, by deploying advanced tools and technology capable of protecting the customers against unethical activities.
3. **Deep learnings:** Internet payment companies providing alternatives to traditional money transfer methods are using deep learning, a new approach to machine learning and artificial intelligence that is good at identifying complex patterns and characteristics of cybercrime and online fraud.
4. **Internal Audit function:** This function is being altered to include fraud risk management in its scope. The changed technological landscape requires the old ways of Internal auditing to give way to new, technologically equipped audit functions. Annual audit planning may no longer be fully effective and flexible audit plans are the need of the hour, as fraud risk assessments require extensive use of forensic and data analytics solutions.
5. **Automated analysis tools:** Today, the industry is increasingly aware of the need for automated analysis tools that identify and report fraud attempts in a timely manner. Solution providers are providing real-time transaction screening, third-party screening as well as compliance solutions.
6. **CCTV Camera:** The management of the bank should install the Close Circuit Television (CCTV) camera at all the ATM locations and strategic positions within the banking hall.
7. **Networking and routine checks:** To prevent computer and ICT fraud, better networking and routine check of money transfer and transactions would frustrate the fraudsters.

8. **Effective control:** An effective control is the most potent antidote against fraud. Human supervision of ICT high waves can bring incidence of ICT manipulation to the barest minimum.
9. **High level ICT consciousness:** ICT should be subjected to a high level of security consciousness to guard against improper use, that is, posting and diversion.
10. **Regular rotation of bank staff:** The management of the bank should ensure regular rotation of duties and staff to prevent an individual from staying too long on a computer system or in a department. Also, there should be inter-branch and intra-bank regular rotation of bank staff.
11. **Relevant laws:** The National Assembly should propose relevant bills that can curb the electronic frauds in Nigeria. For example:
 - Cyber security and Information Protection Bill.
 - Electronic Transactions Protection Bill.
 - Computer Security and Protection Bill.

Conclusion and Recommendation

In view of the fact that the security problem may have seen to be a crucial issue in the practice of e-banking in Nigeria but that could not imply that the operational efficiency of e-banking is impaired. This is because the core banking operations of accepting deposits, granting credit facilities and facilitating cash withdrawal have empirically proved to have improved with the introduction of e-banking in Nigeria. Woherem (2000) opined that only banks that overhaul the whole of their payment and delivery system and apply ICT to their operations are likely to survive and prosper in the new millennium. Therefore, it can be concluded that e-banking introduction in Nigeria had aid to enhance Nigerian banking operations vis-a-vis banks employees' productivity cum general performance. Consequent upon this, the researcher recommended the following:

- a. Government through CBN should provide adequate security measures towards the various e-banking products in Nigeria.
- b. Banks should regularly train their workers who in turn will educate their customers on e-banking system and its products.
- c. The CBN should organize seminars, workshops, symposia and public lectures to bank customers and general public on the application of information and technology cum e-banking system.
- d. Banks should in addition to the storage of information in the computer, maintain the manual filing of all the relevant documentary evidence of information in their financial statement in order to avoid loss of audit trail, with an understanding that e-banking in Nigeria is an "add process" and not an "or process".
- e. The banking industry should review the existing BVN framework with the introduction of BVN Watchlist in the framework.

REFERENCES

- Adegunmi, W. (1996). Fraud in banks. Nigerian institute of bankers, Land mark Publication, Lagos.
- Adeyemi Adesanya-Daniel (November, 2018). CBN Journal on “Central bank: Electronic Fraud will hit N6.1 trillion by 2021”.
- Aluko-Olokun (1990). Nigeria Banks and Computer.
- Central Bank of Nigeria (2017) Annual report Page 38.
- Chike, O. (2018). “Banks loss N1.63 BN to E-fraud”. Nigeria Communications week Journal. August 18.
- Dogarawa, A. B. (2005). The impact of E-banking on consumer satisfaction. Department of Accounting, Ahmadu Bello University, Zaria.
- Ekwueme, C. M., Egbunike, P. A., & Amara, O. “An Empirical assessment of the Operational efficiency of electronic banking: Evidence of Nigerian banks”. Review of Public Administration and Management paper. Vol.1 No. 2 Page 108-133.
- Folami, O. M. (2000). Crime in the Banking Sector. M.Sc. thesis, Department of Sociology, OAU.
- Irechukwu, G. (2000). “Enhancing the performance of banking operations through appropriate Information Technology”. Information Technology in Nigeria Banking Industry, Ibadan, Spectrum Books.
- Journal of Forensic Accounting and Fraud Investigation (JFAFI) ISSN 2659-1138 (Print): ISSN 2659-1146 (Online) volume 4. Issue 1, January-March, 2019. P. 49.
- Nwankwo, G. O. (2005). Bank management, principles and practice.
- Okpala, K. E. & Enwefa, C. (2017). War against corruption in Nigerian public sector: An analysis of stakeholders’ role. FUNAI journal of Accounting, Business and Finance, 1 (1), Page 204-218.
- PWC India publication (June 2015). Current Fraud trends in the Financial Sector.
- Salawu, R. O. & Salawu, M. K. (2007). The emergence of internet banking in Nigeria.
- The Nigeria Electronic Fraud Forum (NeFF) Annual Report (2016). A changing

payments Ecosystem: The Security challenge.

Tughgba A. (2017). Katsina-Ala Multidisciplinary Journal. The challenges of Information and Communication Technology in the Nigerian Banking Industry in the 21st Century: The way out.

© GSJ