Advances In Multidisciplinary & Scientific Research
A Multidisciplinary & Interdisciplinary Journal

Vol. 2 No. 3, September 2016

Statistical Monitoring (SM) of Electronic Fraud Occurring in Nigerian Banks

Braimah, O.J
1Department of Statistics
University of Ilorin
Ilorin, Kwara State, Nigeria
E-mail: ojbraimah2012@gmail.com
Phone: +2347036708840

Okonkwo, I.A
Department of Industrial Mathematics
University of Benin
Benin City, Edo State, Nigeria

ABSTRACT

For some time now, consumers have come to depend on electronic banking to conveniently meet their banking needs. But in recent time there have been a proliferation of electronic banking frauds in the country and across the globe. Monitoring the risk associated with this fraud as well as diminishing its impact is an important issue that face financial institutions as fraud techniques have become more advanced with increased occurrences. The ATM is only one of many Electronic Funds Transfer (EFT) devices that are vulnerable to fraud attacks. This paper includes other fraudulent channels; i.e Point of Sale (POS), Web, Across Counter, Internet Banking, Mobile Banking and Cheques. This paper carried out a quality (fraudulent) monitoring analysis using the fraud actual loss amount in Nigeria in the year 2013 and 2014 as extracted from the 2014 Nigeria Electronic Fraud Forum (NEFF) Bulletin. Standard Cumulative Sum (CUSUM) technique was adopted to monitor the e-fraud rate in Nigeria for the two years; the fraudulent rate was in statistical control, though on increasing trend. Recommendations were made based in order to curb this menace.

Keywords: Point of Sale (POS), Web, Across Counter, Internet Banking, Mobile, Cheque, CUSUM control Chart, Upper control Limits, Out of control.

Aims Research Journal Reference Format:
Braimah, O.J & Okonkwo, I.A. (2016): Statistical Monitoring (SM) of Electronic Fraud Occurring in Nigerian Banks. Advances in Multidisciplinary Research Journal. Vol. 2. No. 3, Pp 93-104

1. INTRODUCTION

Banking in Nigeria is becoming totally dependent on Information Technology initiatives. The huge work force that would have been required in today's massive volume of financial transactions (if handled manually) has been taken care of by utilization of computer systems. Any Bank that aspires to survive the current hyper-competitive and highly dynamic business environment must devise effective ways of engaging resourceful electronic devices to support her service delivery. This gave rise to the landmark migration from the traditional ways of doing banking business to information technology driven solutions. Today, computer based technologies and products are increasingly being deployed in various facets of banking operations to handle transactions such as ATM (Automated Teller Machine), POS (Point-of-Sales), Tele-banking, PC Banking, Mobile Banking etc.

In a nutshell, the facts listed below are some of the challenges being encountered with the traditional banking system ("face-to-face") in Nigeria which led to advent of electronic payment:

1. Long queues in the banking halls.
2. Risk involved in cash movement.
3. Lack of 24 hours-daily service delivery. Significant operating cost.
4. Unnecessary bureaucracy in accessing account information.
5. Staff lackadaisical attitude towards customers.

However, the introduction of electronic banking services shifted the system from the era of 'face-to-face' banking relationship to 'man-to-machine'/'machine-to-man' banking relationship which subsequently address the problems stated above. Now customers can enjoy the benefit of performing banking services at the comfort of their homes anytime without carrying load of cash around.

Donell (2003) viewed electronic banking as banking services that consumers can access, by using Network system or an Internet connection to a bank's computer center, in order to perform banking tasks, receive and pay bills, and so forth. Many other financial services can be accessed via the Internet. To most people, electronic banking means24-hour access to cash through an ATM or paychecks deposited directly into checking or savings accounts (Hillier, 2002).

Diniz (1998) in his view states that Electronic banking encompasses a broad range of established and emerging technologies. Some are "front end" products and services that consumers opt for, such as ATM cards and computer banking; others are "backend" technologies used by financial institutions, merchants, and other service providers to process transactions, such as electronic check conversion. Some are tied to a consumer bank account; others are unrelated to a bank account but instead store monetary value in a database or directly on a card.

Electronic banking services had been fashioned around a given Technology, thus we have electronic banking products classification that are named after their delivery technologies which include:

1. **Internet Banking Services:** Banking services delivered to consumers through the World Wide Web (the internet). Here consumers of banking services transact their business from any computer that is connected to the internet without having contact with any bank staff. Such transaction which may even be performed at a cyber café will require the knowledge of Logon name, Password, token device for authentication and in some cases, a true stamp (this is a unique identifier for every customer logging into an internet banking page).
2. **Mobile Banking Services:** Banking services delivered to consumers via the mobile phone technology. Here consumers of banking services transact using mobile phones with the use of PIN code. Other services available on mobile banking include account enquiries, statement printing, fund transfer, cheque stop-order, transaction alert (debit/credit), bills payment, airtime top-up etc.
3. **Telephone Banking Services:** Banking services delivered to consumers through pre-programmed voice communication medium, generally the telephone technology. This also uses PIN code for authentication purpose. Electronic (Smart) Card Services: Here, plastic cards are made electronically intelligent and used to deliver some banking services, especially payment services to consumers. Generally, the card serves as a purse or wallet in which money is preloaded for future expenses and bill settlement. To achieve a successful transaction will require the knowledge of such card details with unique number or PIN code.

4. **Automated Tellering Services:** These are channel services or medium such as machine terminal (ATM) or handy terminal (POS) that have been pre-programmed to deliver teller services (cash withdrawal, cash deposit, stamp vending, currency exchange, etc) to consumers without the need of having any contact with bank staff. Both ATM and POS are designed to accept plastic cards (either EMV compliant or Magnetic Strip Cards) to deliver financial services to customers. For transaction to be successful on either an ATM or POS terminal, it will require the presentation of physical card and the knowledge of PIN code or signature. POS (Point-of-Sale) Terminal was introduced in 1970 by NCR for making instant payment of goods and services at stores, supermarkets and shopping malls. However, electronic payment via POS requires the use of physical ATM card by swiping it across or inserting in the terminal.
5. **Web Purchase Services:** This is another version of e-payment service rendered via internet websites between service providers such as Airlines, Telco operators, merchants and consumers without the need of physically presenting a plastic card (cardless transaction). Basically, it requires the knowledge of card number, PIN code and CVV at some instance. It is an Electronic Payment System, which allows bank customers' to make online payment for goods and services via the internet with the use of ATM card details and PIN code. This type of transactions does not require the physical presence ofATM card as long as the details are available. Also, in some cases, as it is with master cards, the card number alone suffices for web transactions.

1.1 Automated Teller Machine (ATM) and Payment cards

Automated Teller Machine is a computerized telecommunications device that provides the customers of a financial institution with access to financial transactions in a public space without the need for a human clerk or bank teller. On most modern ATMs, the customer is identified by inserting a plastic ATM card with a magnetic stripe or a plastic smartcard with a chip that contains a unique card number and some security information, such as an expiration date. Security is provided by the customer by entering a personal identification number (PIN). According to Steve (2002), ATMs are placed not only near or inside the premises of banks, but also in locations such as shopping centers/malls, airports, grocery stores, petrol/gas stations, restaurants, or any place large numbers of people may gather. These represent two types of ATM installations: on and off premise. On premise ATMs are typically more advanced, multi-function machines that complement an actual bank branch's capabilities and thus more expensive. Off premise machines are deployed by financial institutions and also Independent Sales Organizations (ISOs) where there is usually just a straight need for cash.

Although ATMs were originally developed as just cash dispensers, they have evolved to include many other bank-related functions. In some countries, especially those which benefit from a fully integrated cross-bank ATM network, ATMs include many functions which are not directly related to the management of one's own bank account, such as paying routine bills, fees, and taxes (utilities, phone bills, social security, legal fees, taxes, etc). Payment Cards were introduced into Nigeria some years ago but suffered low acceptability at the initial stage due to a number of factors which included amongst others: lack of shared network, epileptic services, limited ATM and Point of Sales (POS) Terminals and high cost of operations.

The Central Bank of Nigeria in an attempt to promote the use of cards for making secured payments in Nigeria, issued relevant guidelines on e-banking in Nigeria in2003, 2009, 2010 and 2011. This has encouraged e-payment initiatives such as the establishment of switching companies that facilitate interconnectivity, introduction of shared ATMs and the establishment of Independent Service Operators (ISO) for massive deployment of ATMs and POS, which gave rise to significant growth in the use of payment cards.

Ezeoha (2005) posited that the hype of e-commerce, e-banking and e-everything is gradually being embraced by Nigerian financial institutions who are poised to be in the vanguard of narrowing the digital divide.

1.2 Associated vulnerabilities with e-payment system in Nigeria

Electronic payment systems have been known to be susceptible to fraud attack. Card frauds have recently become more widespread which can be classified as either internal or external. The internal fraud which is often perpetuated by financial institution staff involves wrong account mapping and card/PIN mailer suppression which is a result of weak control process coupled with management oversight. However, the external fraud is basically direct consequence of hackers' activities which involve unauthorized access to cardholder information via identity theft which can be achieved through Phishing attack, Pharming attack, Skimming attack, Brute force attack, eavesdropping, shoulder surfing, social engineering and session hijack.

Christoslav et al (2003) in a research asserted that ATM services are highly profitable for banks, and banks aggressively market the use of ATM cards. ATMs that are off bank premises are usually more profitable for banks because they attract a higher volume of non-bank customers, who must pay service fees. Unfortunately, customers using off premise ATMs are more vulnerable to robbery. ATM robberies estimates are derived from periodic surveys of banks conducted by banking associations. According to those surveys, there was an estimated one ATM crime (including robbery) per 3.5 million transactions, (Adelowo and Mohammed, 2010).

As financial institutions are migrating to cashless transactions for efficient service delivery, electronic payment system experience must be safe and accommodating as much as possible for customers. However, e-channel fraud trend in Nigeria Economy revealed that Card fraud is increasing since the adoption of International Debit Card by most Nigeria Banks. Research into emerging Card business revealed that one of the most important issues for customers when using Card service is the security of card details and PIN code. With reference to International White paper on ATM Fraud Security, the most precious customer's PIN code may be captured unknowingly to the affected customer in one of the following five ways:

1. **PIN Interception:** PIN code information can be captured in electronic format through an electronic data recorder. Capturing the PIN can be done externally via web purchase in which it is trapped as the PIN is transmitted to the host computer for online verification (Sessionhi-jack). Likewise, PIN can be captured internally by having access to the communication cable of PIN pad inside the POS or ATM Terminal which can easily be done at merchant stores/supermarket or off-site ATM locations. i.e. using key loggers
2. **Fake PIN Pad:** To achieve this, a fake PIN pad is placed over the original keypad as overlay to capture the PIN data and stores the information into its memory. The fake PIN pad is then removed and recorded PINs are downloaded. Fake PIN pads are very identical in appearance and size as the original. An additional type of overlay that is more difficult to detect is a “THIN” overlay that is very transparent and apart from capturing customer's PIN, it also allow the intended transaction to proceed in a normal way.
3. **Shoulder Surfing:** Shoulder surfing is the act of direct observation and taking note of the numbers the ATM cardholder tapped on the keypad. Fraudsters usually position themselves a bit close but not direct proximity to the ATM so as to watch the user as he enters the PIN.

4. **Fake ATM Camera and Card Reader (Skimming):** Another way of gaining access to customer PIN unknowingly is to install miniature video camera by a fraudster which can be discretely installed on the ATM facial panel or somewhere close to the PIN Pad in order to record the PIN entry information. A fraudster may also attach a false monitor and card reader on top of the ATM actual monitor. The false monitor and card reader record the account information and present a message to the customer that the transaction cannot be completed. After the customer might have left, the fraudster will return to remove the portable device.
5. **Unsolicited E-mail:** Unsolicited e-mails which are products of phishing and pharming attack are used to mislead ATM cardholder by notifying them that "in order to continue using your card for ATM transactions, you MUST register your card(s) online immediately.
6. **Unsolicited assistance at ATM points:** Recently, fraudsters have besieged ATM terminals in search of vulnerable bank customers offering to help them and subsequently defrauding them of cash.

If you do not register your ATM card(s) immediately, you will no longer be able to use your cards with the ATM machines or for ATM transactions and your card(s) will be cancelled or terminated". Once a customer innocently clicks on the link, his card details will be captured and reported on the fraudster's dedicated server.

1.3 What is Electronic Fraud?

Emeka (2007) in an article stated that as the number of ATM card holders continues to grow daily as result of e-payment awareness and deployment of more than 3,000 ATM cash points by Nigerian banks across the country, activities of card fraudsters appear to be on the increase. Majority of Nigerian banks, notably United Bank for Africa, warned ATM card users nationwide against disclosing their ATM card details to a second party as a result of fraudsters who are said to be on the prowl. Diebold (2002) stated some ATM Frauds in a paper titled "ATM Fraud and Security".

There is broad range of definitions for Electronic fraud; but the key reference in the various definitions is the fact that electronic platform and losses are involved, Michael, (2003). The losses in some cases go beyond material losses such as reputational damage and competitive advantage making it difficult for organizations to adequately determine the true impact of e-fraud in financial terms. For example, the US Department of justice describes e-Fraud as a fraud scheme that uses one or more components of the Internet - such as chat rooms, e-mail, message boards, or Web sites-to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to other connected with the scheme".

Graham however defines e-Fraud as "a fraudulent behavior connected with computerization by which someone intends to gain dishonest advantage" Furst et al (2005).

Some of the reasons for the growth in e-fraud are:

1. Increasing market size of e-commerce.
2. Increasing demand for technological changes.
3. Low awareness by consumers and business on basic Information System securities practice such as the use of antivirus and firewall.
4. Proliferation of malicious codes and hacking tools.
5. Harsh economic realities

The use of ATM is not only safe but is also convenient. This safety and convenience, unfortunately, has an evil side as well that do not originate from the use of plastic money but rather by the misuse of the same, Chris (2006),.This evil side is reflected in the form of “ATM frauds” that is a global problem. The use of plastic money is increasing day by day for payment of shopping bills, electricity bills, school fees, phone bills, insurance premium, traveling bills and even petrol bills. The convenience and safety that credit cards carry with its use has been instrumental in increasing both credit card volumes and usage. The world at large is struggling to increase the convenience and safety on the one hand and to reduce its misuse on the other. An effective remedy for prevention of ATM frauds, however, cannot be provided unless we understand the true nature of the problem.

Brunner et al (2004) states that; the ATM fraud is not the sole problem of banks alone. Itis a big threat and it requires a coordinated and cooperative action on the part of the bank, customers and the law enforcement machinery. The ATM frauds not only cause financial loss to banks but they also undermine customers' confidence in the use of ATMs. This would deter a greater use of ATM for monetary transactions. In a bid to meet the insatiable quest for improved service delivery and better quality of living, technology has responded with a speed that now spells the direction for businesses and style of living. Yet pervasiveness of the internet, imperfection of man and technology, race for time and market, and greed has brought about ubiquitous challenges which must be tackled. The objective of this study is to implore statistical quality control (process control) tool to monitor the e-banking fraudulent rate in Nigeria. We therefore implore the use of Cumulative Sum Control Chart to achieve this objective.

Fig. 1: E-Fraud Channels

2. MATERIALS AND METHODS

In this section the Standard CUSUM chart was introduced to monitor electronic banking fraudulent rate.

2.1 The Tabular or Algorithmic CUSUM for Monitoring the Process Mean

Let observations y_i denote the loss amount (₦) of fraudulent channels (ATM, POS, Web, Across Counter, Internet Banking, Mobile and Cheques) and is distributed with mean **μ** and variance σ^2. If μ is the target for the quality characteristics y_i, i.e fraudulent (₦). Then the cumulative sum control chart is formed by plotting the quantity

$$C_i = \max(0, S_{i-1} + y_i - K) \qquad 1$$

Where y_i the attribute to be controlled and K is is the target value. If $S_i \geq H$ (the decision interval), an out of control of non-conformance detection of increase in fraudulent rate. Thus, it can be used to monitor fraudulent crime rate, so as to curb the global menace to minimal if not eradicated whenever a shift in the process mean is detected.

The starting values of $C_0 = 0$

The statistics $C_i^+ = \max(0, S_{i-1} + y_i - K)$ **2**

Equation (2) is called one sided upper r CUSUM.

The procedure CUSUM control chart consist of taking samples of size ***n*** and plotting the cumulative sum versus the sample number, where **μ** is the sample mean, **K** is the reference or allowance value and is referred to as decision limits. Although, many curves and monographs have been developed for the specific value of **K** and **H**, those developed by (Goel, A. L. and Wu, S. M., 1971) and (Kemp, 1961), are commonly used.

K (the reference value or allowance value) is often chosen halfway between the target value ***μ*** and out-of-control value of the mean μ_1 that want to be detected quickly.

Thus if $\mu_1 = \mu + \delta\sigma$ **3**

Then

$$K = \frac{\delta}{2}\sigma \qquad 4$$

One Sided Approximate of Average Run Length (ARL)
The approximate for ARL is given as:

$$ARL = \frac{e^{-2\Delta b} + 2\Delta b - 1}{2\Delta^2} \qquad 5$$

Where $\Delta = \delta^* - k$ for the upper one-sided CUSUM C_i^+, $b = H + 1.66$ and $\delta^2 = \frac{(\mu_1 - \mu)}{\sigma}$. The quantity δ^* represents the shift in the mean, in the unit of σ, for which the ARL is to be calculated.

If either C^+exceeds the decision interval *H*, the process is considered to be out of control. The reasonable estimate of *H* is $H = 5\sigma$.Thecontrol chart was plotted using **MINITAB 14**.

3. RESULTS AND DATA ANALYSIS

3.1 E-Fraud emerging trend

According to an ACFE article of November 2013, an online protection firm (iovation) identified Africa as the continent with the highest percentage (7%) of its online transactions in 2012 as fraudulent, with the highest percentages from Nigeria and Ghana. iovation identified the common fraud trends to be credit card fraud, identity theft, profile misrepresentation, and online scams and solicitations. Also, the Nigeria Inter-Bank Settlement System Plc (NIBSS), in its 2014 report on e-payment fraud in Nigeria established that electronic transactions as well as e-frauds are on the increase in Nigeria as reflected on the two (2) tables below:

Table 1: Transaction volume and value (2013 & 2014) processed by NCS categorizedby Payment types

	Transaction Volume		Transaction Value	
	2013 count (₦)	**2014 count (₦)**	**2013 count (₦)**	**2014 count (₦)**
POS	11,258,846	24,607,497	22,990,3237,909	447,459,739,698
Instant Payments	17,967,646	42,540,034	11,674,496,434,771	21,148,614,937,311
EFTs	30,134,545	30,203,908	14,218,018,800,813	14,536,388,062,398
Cheque	14,698,538	16,070,494	8,069,550,477,646	7,725,215,739,533
Total	**74,059,575**	**113,421,933**	**34,191,968,951,139**	**43,857,678,478,940**

Source: NIBSS report - 2014 E-Payment Fraud Landscape in Nigeria (page 3)

Table 2: Fraud actual loss amount trend by channels in terms of percentage change between 2013 and 2014

Channel		**2013 Loss Amount (₦)**	**2014 Loss Amount (₦)**	**% Change (₦)**
Cards	**ATM**	54,999,829	2,688,669,292	4789%
	POS	5,851,443	157,610,831	2594%
	Web	109,298,898	1,031,239,284	844%
Across Counter		13,851,780	140,813,927	917%
Internet Banking		271,762,696	212,0881,512	680%
E-commerce		139,48,390	58,994,920	323%
Mobile		6,787,544	13,328,957	96%
Cheques		8,693,770	4,448,600	-49%
Total		**485,194,350**	**6,215,987,323**	

Source: NIBSS report - 2014 E-Payment Fraud Landscape in Nigeria (page 14)

Based on the submissions from table 2 above, one can infer that e-Fraud is on the increase in Nigeria from year 2013 to 2014; a continuous threat for which Nigerian banks should strive to keep at the barest minimum.

Control Chart

In order to monitor the fraudulent rate in Nigeria, the values in table 2 were compressed in MINITAB 14 using CUSUM control chart technique.

For year 2013, recall that the target value is μ=60,649,294, the subgroup size is n =1, the process standard deviation is σ = 92537112, and suppose that the magnitude of the shift we are interested in detecting is 1.0 σ =1.0(92,537,112). Therefore, the out-of-control value of the process mean is μ_1 = 60,249,294 + 92,537,112 = 152,786,406. We will use tabular CUSUM with *K* = 462,685,556 (because the shift size is 1.0 σ and σ = 1) and H= 462,685,560.

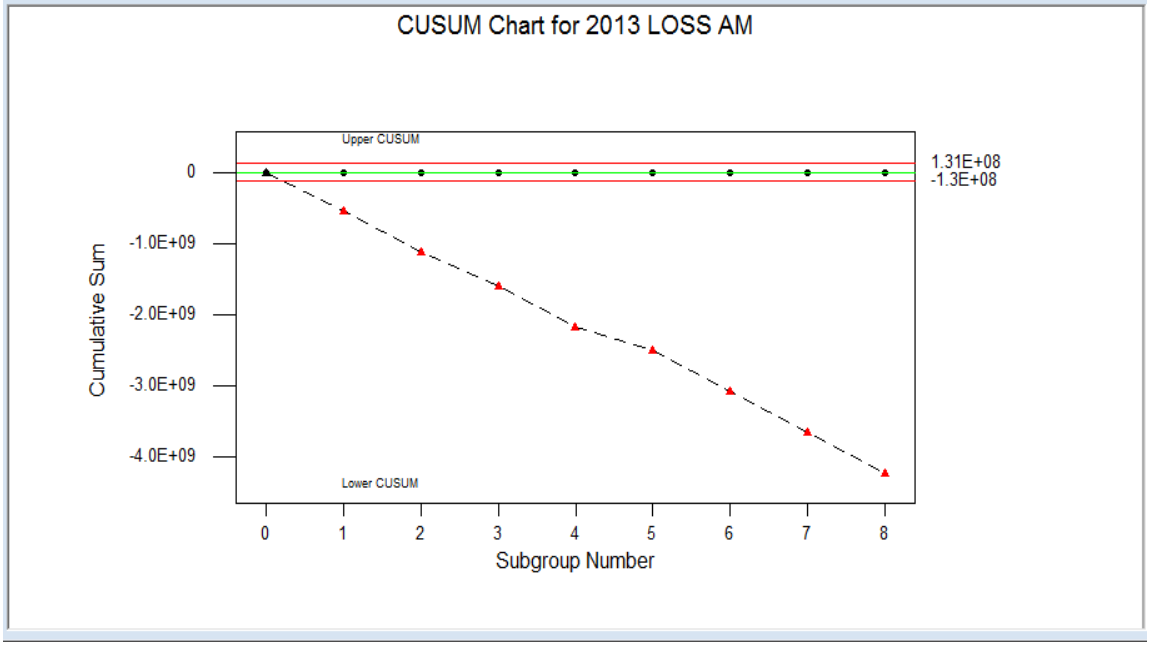

Fig. 2: CUSUM chart for e-fraud in Nigeria for the year 2013

From figure 2 above, the upper control limit (UCL) is 1.31 billion naira. Since none of the upper CUSUM plots fall outside the UCL, the fraudulent process is still said to be in statistical control.

For year 2014, also recall that the target value is μ= 776,998,415, the subgroup size is n =1, the process standard deviation is σ = 1,069,650,857, and suppose that the magnitude of the shift we are interested in detecting is 1.0 σ =1.0(91,069,650,857). Therefore, the out-of-control value of the process mean is μ_1 = 76,998,415 + 1,069,650,857 = 1,846,649,272. We will use tabular CUSUM with *K*=534,825,428.5 (because the shift size is 1.0 σ and σ = 1) and H= 5,348,254,285.

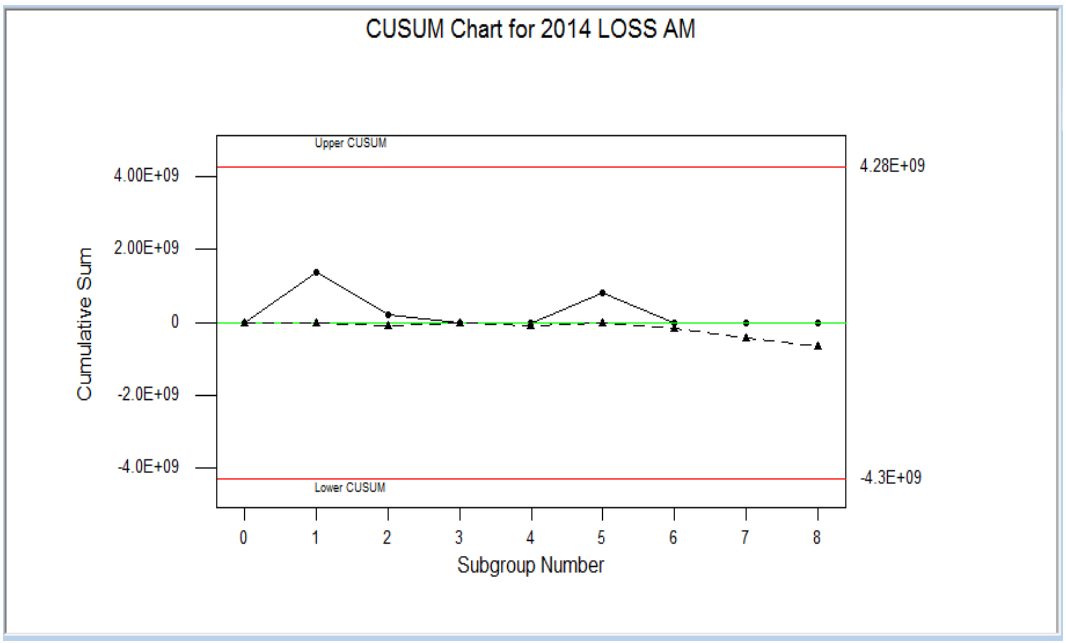

Fig. 3: CUSUM chart for e-fraud in Nigeria for the year 2014

From figure 3 above, the upper control limit (UCL) is 4.28 billion naira. Since none of the upper CUSUM plots fall outside the UCL, the fraudulent process is still said to be in statistical control.

4. DISCUSSION OF RESULTS

The submissions in table 1 and 2 infer that e-Fraud is on the increase in Nigeria which is still a continuous threat for which Nigerian banks should strive to keep at the barest minimum.

For the year 2013, the fraudulent reference value H= 462685560 and the UCL= 1.31 billion naira. From figure 2, it can be seen that since none of the upper CUSUM plot fall beyond the UCL, the process is said to be in statistical control.

Also, for the year 2014, the fraudulent reference value H= 5,348,254,285 and the UCL= 4.28 billion naira. From figure 3, it can be seen that since none of the upper CUSUM plot fall beyond the UCL, the process is said to be in statistical control.

5. CONCLUSION

Conclusively, e-fraud is still on an increasing trend in Nigeria since, the CUSUM methodology was used to monitor the fraudulent process in order to detect whether the fraudulent rate has gone out of hand and it was observed that the process is in control. Therefore, this technique may be an efficient tool in monitoring the e-fraud level.

6. RECOMMENDATION

From our findings, since e-fraudulent rate is on an increasing trend, though still in statistical control. In order to arm Nigerian banks against e-Fraud, the leadership of financial institutions (banks) should bear in mind that the fight against e-Fraud does not only require electronic tools but in addition, a focus on the electronic transaction underlying processes and associated risks. The banks should pay attention to the following considerations:

1. **Implementing fit-for-purpose fraud monitoring solutions**: In recent times, Nigerian banks have invested in several Information Technology (IT) solutions in order to meet their business goals, but while this is imperative, it is also important to invest in solutions that will monitor (detect, analyze and prevent) fraudulent transactions on the internet/mobile banking, card platforms and other electronic payment channels.
2. **Overhauling IT security**: Nigerian banks may not have recorded any cyber-attack with a high impact as the recent Carbanak attack but no financial institution should wait until such an attack occurs as it is better to be proactive rather than being reactive. Also, a periodic review of IT procedures to ascertain the relevance and to prevent fraudsters from being ahead.
3. **Paying attention to the "enemies within"**: If you consider your level of dependency on IT solution experts and vendors, internal control structure (that may or may not pick IT control deficiencies) and the ever-increasing trend of employee dissatisfaction, then you will agree with the fact that banks have potential internal loopholes that may aid e-Fraud.
4. **Intensifying anti-fraud awareness campaigns**: A lot of e-fraud cases are aided by underlying social engineering schemes, phishing scams and instances of identity theft. It may surprise you that most solutions cannot guarantee the detection and prevention of phishing scams especially when they target customer-initiated (self-service) transactions.
5. **Implementing a formidable e-Fraud detection-prosecution process**: Nigerian banks should setup a centralized fraud monitoring team (comprising dedicated fraud monitoring employees from all Nigerian banks), this should be setup to compliment the implementation Heimdall solution. This will improve the turnaround time for inter-bank liaison whenever there is a need to prevent fraudsters from withdrawing/transferring fraudulent funds.

REFERENCES

1. Adelowo, S.A and Mohammed, E.A. (2010). Challenges of Automated Teller Machine (ATM) Usage and Fraud Occurrences in Nigeria–A Case Study of Selected Banks in Minna Metropolis, *Journal of Internet Banking and Commerce,* (15)2. pp. 1-10
2. Brunner, A., Decressin, J. and Kudela, B. (2004). Germany's Three-Pillar Banking System Cross Country Perspectives in Europe, Occasional Paper, International Monetary Fund, Washington DC. IMF Occasional Paper No. 233
3. Chris E. M. (2006). Bank ATM Security Advice: Effective Method of Security Measures. Virtual Banking. Journal of Internet Banking and Commerce, 11(1), pp. 1-56
4. Christolav, E. A., Marianne A.H. and Jeanne M. H. (2003). US Consumer's and electronic banking 1995- 2003. Board Division of Consumers and Community Affairs. Los Angeles
5. Cynthia B. (2000). The measurement of white-collar crime using Uniform Crime Reporting (UCR) Data. Department of Justice, Federal Bureau of Investigation, New York.
6. Dele, K. (2007).ATM in Nigeria Banking Operation. Nigeria Daily Trust Newspaper, June 12 2007, pp.22
7. Diebold I. (2002). ATM fraud and security: White Paper, New York.
8. Donnell Y.K. (2003), New System of banking; Drawill Publications, New York. pp.24-25.
9. Emeka A. (2007). Fraud Alert - Banks Raise Fresh Alarm on ATMs, Vanguard Newspaper Lagos
10. Ezeoha, A. E. (2005). Regulating Internet Banking in Nigeria, Problem and Challenges- Part1, Journal of Internet Banking and Commerce 10(3), pp. 5-33
11. Ezeoha, A.E (2006), Regulating Internet Banking in Nigeria, Problem and Challenges-Part 2. Journal of Internet Banking and Commerce, 11(1), pp. 1- 60
12. Furst, K, .Lang, W. and Nolle, E. D. (2002) , Internet Banking Development and Prospects: Working Paper, Center for Information Policy Research, Harvard University
13. Hillier, D. (2002). Money Transmission and the Payments Market, Financial World Publishing, Kent UK.
14. Michael S.S. (2001).Robbery at ATM: Problem-Oriented Guides for Police Series Problem-Specific Stuides Series No. 8. New York
15. Steve W. (2002): Automated Teller Machines; CGAP Staff and Exchange, CGAP IT Innovation Series Los Angeles.