THE NIGERIA ELECTRONIC FRAUD FORUM (NeFF)

2014
ANNUAL REPORT

e-Fraud:

Fighting the battle, Winning the war

CENTRAL BANK OF NIGERIA

Foreword

NeFF: Improving Card Payments Security and Trust

In 2011, the Central Bank of Nigeria in conjunction with the Bankers Committee embarked on an ambitious project of transforming the Nigerian retail payments system from over-dependence on cash for P2P, P2B and G2P transactions, to the adoption of electronic alternatives for payments. In the course of this journey, studies also showed that security ranks as foremost in the concerns of stakeholders when transiting from cash based system to an electronic platform for payments. This concern was further heightened by cultural developments and quicker evolving global trends, which was in favour of embracing technology and convenience in our payments system.

As a direct response to this concern, the Nigeria electronic Fraud Forum (NeFF) was born in December, 2011. The forum over the years has played an important role in ensuring that we as an industry will continually recognize that we are only as strong as our weakest link. Through information exchange and knowledge sharing on fraud issues, the Forum has proffered solutions that have restored public confidence on card usage in particular, and electronic payments in general.

As an institution, the Central Bank of Nigeria remains committed to ensuring that the safety and soundness of our financial system is not compromised. Our zero tolerance on practices that will undermine the health of our financial institutions remains unshaken. To this end, I assure the Nigeria electronic Fraud Forum of the Central Bank of Nigeria's support in continuing with this fight against e-fraud.

It is therefore with great pleasure that I present the NeFF 2014 Annual Report. I hope you will find this report useful for the rich information it contains, and as a publication of interest that will deepen your understanding of the fight against e-fraud in Nigeria as appropriate measures have been taken to deepen our payments system.

Suleiman Barau
Deputy Governor Operations
Central Bank of Nigeria.

Acknowledgement

The production of this report was made with financial support from all the Deposit Money Banks in Nigeria, therefore, a special appreciation goes to them for the financial support and material inputs.

The Deputy Governor Operations, CBN, Mr. Suleiman Barau was of immense support to the project.

Similarly, the Director, Banking and Payments System Department of CBN, Mr. 'Dipo Fatokun has been a source of great support and inspiration to NeFF, his enormous support and guidance is sincerely appreciated.

Special thanks also go to Messrs Biyi Dosumu, Musa Jimoh, Chidi Umeano, Premier Oiwoh (Chairman CHBO), Tunde Kuponiyi (Chairman CeBIH), David Isiavwe (Chairman ISSAN) and the NeFF Steering Committee members, particularly the review team comprising Joe Obogo, Babatunde Ajiboye, Aliyu Mohammed and Lydia Kuje, for their tireless efforts at reviewing and proof-reading the 2014 Annual Report.

Disclaimer

The Central Bank of Nigeria (CBN) shall not be responsible for the views expressed by contributors/authors in this report. No article shall constitute or be deemed to constitute any representation by the CBN.

Therefore, every contributor/author shall be solely responsible for the contents and views in their articles.

Table of Content

Godwin I. Emefiele (CON)
Governor

Dr. Sarah Alade (OON)
Deputy Governor (Economic Policy)

Suleiman Barau (OON)
Deputy Governor (Operations)

Dr. Okwu J. Nnanna
Deputy Governor
(Financial System Stability)

Adebayo Adelabu
Deputy Governor
(Corporate Services)

NeFF Management Team

- Director, Banking & Payments System Department – Chairman
- Chairman, Committee Heads of Banking Operations
- Chairman, Committee of e-Banking Heads
- Chairman, Committee of Chief Compliance Officers
- Chairman, Committee of Chief Internal Auditors
- Managing Director, Unified Payments Services Limited
- Managing Director, Interswitch Nigeria Ltd.
- Office of The National Security Adviser
- Executive Chairman, Economic and Financial Crimes Commission
- Association of Licensed Mobile Payment Operators (ALMPO)
- Electronic Payments Providers Association of Nigeria (EPPAN)
- Information Security Society of Africa, Nigeria(ISSAN).
- Managing Director, Nigeria Inter-Bank Settlement System (NIBSS)
- Digital Encode – Technical Partner to NeFF

The following Departments and Office in the CBN

- Consumer Protection
- Financial Policy and Regulation
- Information Technology
- Legal Services
- Banking Supervision
- Corporate Communication
- Risk Management
- Shared Services Office

Chairman's Address for The NeFF 2014 Annual Report

'Dipo Fatokun
Director, Banking & Payments System Department,
CBN and Chairman, NeFF.

I am particularly pleased to be able to report that 2014 was another successful year for the Nigeria electronic Fraud Forum (NeFF).

The Nigeria electronic Fraud Forum (NeFF) has come a long way since it was inaugurated in December 2011. Over the years we have remained committed to our core objectives of:

1. Enabling information exchange and knowledge sharing on Fraud issues amongst key stakeholders, with the objective of ensuring collaborative and proactive approach to tackling/ mitigating fraud and limiting occurrences and losses.
2. Serving as an official body that represents the industry's position on fraud related issues, while proffering solutions that restore public confidence on card usage and electronic payments in general.

In furtherance to the above, we have in the course of our activities for 2014 set in motion, steps that have increased information and knowledge sharing, proffered solutions that have been adopted into circulars for the industry, embarked on strategic relationships and structured the administration and management of the forum, through the execution of a Memorandum of Understanding (MoU) which serves to guide the Forum's activities .

In detail, the Forum has been able to deliver on the following:

1. Created an online presence for NeFF to create a platform that will ease access to information.
2. We have entered into collaboration with the Economic and Financial Crimes Commission (EFCC) to tackle card present fraud in Non-EMV environments.
3. We have been able to create a membership schedule comprising of 47 organizations and 145 members.
4. A Memorandum of Understanding (MoU) which serves to guide the Forum's activities has been signed and agreed to, by the industry.
5. The following circulars have emanated from our deliberations at NeFF;
   - CBN Pronouncement on Two-Factor Authentication for Internal Banking Processes.
   - CBN Pronouncement on Card present fraud in Non-EMV environment.
6. Since fraud is globalized, the Forum embarked upon a tour to South Africa from 20th - 24th October, 2014, to understudy the operations of the South Africa Banking Risk Information Centre's (SABRIC) success on combating financial crime, with a view to adopting some strategies to enhance the security of our payment space. The following were recommended;

- Set-up an independent Nigeria Banking Risk Information Centre (NIBRIC). This should be owned by the banks but Central Bank of Nigeria should orchestrate it. This center should be not-for-profit and be wholly dedicated to managing banking risk.
- The model for NIBRIC should be derived from the South Africa model, in comparison with other models, such as SIBSS in Portugal, UK Card Association, etc., taking cognizance of our peculiar environment.
- NIBRIC should start small, think big and scale up fast.
- The first phase of NIBRIC should be commercial crime and the immediate setting up of a forensic laboratory.

These are laudable steps that are designed to create a safer payment system, increase user confidence and facilitate collaboration among players in the payments ecosystem.

The Steering Committee of NeFF has however not rested on its oars, even in the light of the strides achieved. A 30 minute documentary has also been produced on the activities of the Forum. The documentary, when aired, will be a strong tool towards increasing awareness of protective measures that the industry has put in place and communicate common tips to users that will reduce susceptibility to popular antics by the fraudsters.

In closing, I would also like to thank our stakeholders for their continuing interest in, and support for, this Forum and would like to further affirm that 2015 will see a stronger, more committed and proactive fight against e-fraud in our Payments System. We will forever remain poised, even though the battle rages, to win this war.

Tackling Emerging Security Issues with Cyber Intelligence

By Pattison Boleigha,
Chief Conduct & Compliance Officer, Access Bank Plc.

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 have brought about ubiquitous challenges which must be tackled. The challenges have manifested in various forms; Collusion, System failure, Password compromise, Data Compromise, Knowledge gap, Back doors, Identity theft, Terrorism, Session/credential Hijacking, Unauthorised funds transfer, Robbery and ATM ramming, Money Laundering, Denial of service, Hacking, Phishing e.t.c resulting in cybercrimes and frauds.

Doing business on cyberspace therefore needs informed, conscious and calculated management of the inherent risk. Due to the abstract, technical and pervasive nature of the internet, organizations need services of Information Security, Technology, Risk and Compliance experts to manage the risk. They all need to proactively gather and analyze information on security gaps, vulnerabilities, challenges and incidences to track and counter security threats making cyber intelligence a must.

Cyber security risks are inherently complex. These threats are real and can have severe implications if not properly managed.

In November 2013, more than 40 million customers had their credit card and personal information stolen as a result of a data breach at a major retail outlet in the US. The estimated cost of this incidence was close to $150 million.

In reacting to spikes in phishing attacks in the last quarter of every year since 2012 in Nigeria, most banks have invested in anti-phishing solutions to tackle known patterns in an effort to protect their customers. Following several reported cases of phishing related frauds, the Central Bank of Nigeria released a circular in August 2014, mandating all banks to install an anti-phishing solution.

On November 11, 2014, a scam mail was sent purporting to come from CBN with a target to harvest card and online transaction credentials of several banks customers on a single phishing site (a clone of CBN page). It took an informed customer's complaint to expose the attack. Unlike several other cases that takes between 24 to 48 hours to shut down, this phishing site was brought down in less than 2 hours but the number of customers who may have lost funds is yet to be known.

A recent study by the American Bankers Association showed that more than two thirds of cyber security incidents were as a result of phishing attempts.

Competition and race for time to market leaves organizations buying or deploying technology solutions with vulnerabilities which ordinarily would have been better secured before deployment. Actions are not promptly taken when incidents red flags are picked. Calls for prompt blocking of fraudulent funds are not met with the expected inter organizational cooperation. Organizations fight and hide even cyber intelligence to stay ahead in competition but criminals share information knowing that they must keep running to stay alive. They trust themselves even in their evils knowing that no one can succeed alone.

Like the fight against "Ebola Virus Disease", cooperation and collaboration, among peers, professionals, organizations, and sharing of cyber intelligence is key to fighting the menace. We must all work together to develop and implement effective security, compliance and anti-fraud structures, which are absolutely necessary to handle the speed and complexity of transactions and exchange of information on the internet, and effectively tackle cyber incidents, crimes and fraud losses

Some of the steps to achieve this include, putting in place an effective internal control mechanism to curtail the menace of cybercrime, sharing of information by stakeholders during fraud investigation, collaboration with international and local agencies to develop effective strategic responses and preventive measures. Information sharing and continuous training, awareness/sensitization, for stakeholders; users, customers and even the general public is very important.

We also need to continuously benchmark infrastructure and systems against leading best practices in cyber security and encourage improved response to evolving threats and work closely with telecommunications firms, internet service providers, regulators and law enforcement agencies and other stakeholders.

For us in Access Bank, we are strongly resolved in tackling the menace and we are already collaborating with local and international organizations in this regard. We have also resourced our Information Security and Anti-Fraud functions. We will not hold back our commitment to collaborate and cooperate with stakeholders who are also committed to fight cybercrimes.

In conclusion, as our economy grows bigger and our institutions have greater international presence, the nature and extent of cyber risks will continue to expand. It is my hope that sharing of knowledge and experiences will generate new ideas to stem threats of cybercrimes.

Thank you.

Holistic Approach to Electronic Channels Fraud Management

Olusola Odediran
ByCISA, CISM, CRISC, MNIM
Group Head, Information Systems Audit
Diamond Bank Plc

1. Background

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 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 conventional/traditional ways of doing banking business to information technology driven solutions. Today, computer related 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), Internet Banking, Mobile Banking , Web Purchases, Tele-banking and PC Banking.

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:

- Long queues in the banking halls;
- Risk involved in cash movement;
- Lack of 24 hours-daily service delivery;
- Significant cost associated with cash sorting and counting;
- Unnecessary bureaucracy in accessing account information.

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 home anytime without carrying load of cash around.

2. Electronic Payment Channels

Sequel to progressive advancement in computer technology solutions in the early-to-mid-1990s, a new product named as electronic commerce was developed and new methods of delivering financial services emerged. Electronic banking products are often described as banking services delivered through electronic channels. Various 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;

- 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's staff. Such transaction which may even be performed at a cyber café will require the knowledge of Logon name, Password and transaction code for authentication purpose.

- 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 and transaction alert (debit/credit).

- 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 pre-loaded 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.

- 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, et ce teral) 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 for making instant payment for 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.

- 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 of ATM card as long as the details are available.

3. Payment cards varieties

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 in 2003, 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. Types of payment cards deployed in Nigeria include:

Debit Cards: This enables holder access to his bank account online. It is commonly used in Nigeria at POS terminals (for payment of goods or services) and at ATMs for cash withdrawal and account balance enquiry. Examples of different brand of debit cards in use in Nigeria include the MasterCard Maestro, Visa V-Pay or Electron, Interswitch enabled cards (Velve & cashcard), the Quickcash brand of the ATM Consortium Limited and various other proprietary cards.

Credit Cards: This type of card enables holders to make purchases and/or withdraw cash up to a prearrange ceiling, based on the line of credit granted to him.

Dollar Denominated debit/credit cards: It is noteworthy that both debit and credit cards are being issued in local and foreign currency under the platform of Nigerian Switching Companies using the network of MasterCard and Visa International. This has brought international e-commerce to the comfort of homes in Nigeria. Cardholders can stay in Nigeria to participate in auction across the globe, shop and make payment in over 210 countries in the world. With this, Nigerians traveling abroad do not necessarily need travelers' cheque. The volume and value of dollar denominated card transactions has being on the increase, reflecting the potentials of cards market in Nigeria.

4. Associated vulnerabilities with e-payment system in Nigeria

Electronic payment systems have been known to be susceptible to fraud attack. Cards fraud has 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 and session hijack.

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 (5) ways:

a. 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 (Session hi-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.

b. 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.

c. 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.

d. 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 facia 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.

e. 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 BY CLICKING HERE .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.

5. Effective way for managing e-payment fraud

There are multitude of security issues surrounding e-payment services ranging from burglary (outright theft of ATM), suppression (ATM Vault cash suppression, card suppression), account siphoning (Fraudulent Web purchases, unauthorized internet banking transaction, unauthorized mobile money transfer, fake SMS transaction alerts), and cardholder robbery. It is important that all stakeholders within the e-payment industry (Cardholders, Banks, Switching firms, Merchants and Network operators) collaborate together to share and communicate detected fraud techniques. Sharing experiences and knowledge will help the industry in reducing and controlling the emerging trend of electronic payment fraud.

In fact, many organizations subscribe to the philosophy of fraud prevention as "Competitive Advantage" where they guage part of their success by how much fraud they can push off to their competitors. This can be described as a "not in my backyard" approach. Such firms typically are unwilling to discuss or share their fraud management methods with their competitors. Their focus is to implement strategies before their competitors so that the fraudsters will move to their competitors to commit such fraud. Thanks to Central Bank of Nigeria for setting up NEFF (Nigerian Electronic Fraud Forum) which has largely addressed this concern. The ability to jointly collaborate will aid prompt analysis of fraud so as to implement prevention and detection policies which can deter fraudsters from carrying out their intentions.

The underlying issues associated with the rising cases of electronic payment fraud include:

- Cardholders Ignorance on Card Usage security:
  Customers being gullible to phishing/social engineering attack due to lack of awareness on common social engineering techniques such as standing behind a customer and using GSM phone to capture his/her ATM card details. Some customers engage the service of security personnel on duty to assist them in changing their default PIN code thereby divulging such secret information unknowingly.

- Knowledge gap on electronic card product features:
  Some customers are not aware that web purchases could be achieved with their card details without physically presenting such card at the instance of transaction. Hence, such customers get worried when receiving debit alerts for card related transactions while their card is in their pocket.

- Inadequate monitoring of ATM terminals:
  - Lack of camera on ATM terminals to capture the face of fraudsters;
  - Lack of systems based solution to track suspicious transactions;
  - Lack of systems based solution to report compromised ATM terminal.

- Management oversight on production processes:
  - Non-adherence to best practice procedure for card management (PCIDSS)
  - Non compliance with KYC (Know-your-customer) requirement for account opening.

- Weak control measures over operational processes which includes:
  - Risk created by non segregation of transaction limits vis-a-vis optional channels for customers' classification
  - Weak web security design by not incorporating string validation test.
  - Weak security controls over card activation and hot-lisiting process;
  - Poor encryption key management by using default test keys;
  - Non renewal of keys;
  - Poor access control to restricted environment;
  - Ex-banks staff with active login to Card management systems;

6. e-Payment Control Practice

There is an urgent need to put in place fraud deterrence measure in order to manage the growing rate and effectively position the electronic banking product as a

preference in the banking services market. While continuous awareness campaign is highly essential for customers, so also collaboration should be highly encouraged among stakeholders in the e-payment industry with the aim of sharing information relating to fraud management process.

Some of the adoptable control practices are as enumerated below:

a. Public enlightenment on fraudsters' activities and investigation findings.
b. Consumer education on security consciousness while using ATM service.
c. Continuous cardholder awareness on ability to disable and enable their card by themselves when not in use. This will largely prevent Non-EMV transaction fraud rate in which Nigeria Banks do not have chargeback right for transactions performed in United State of America.
d. Strict enforcement of adherence to internal policies and procedures on ATM.
e. Adequate funding of collaborative forum for tackling electronic banking fraud.
f. Fraud status report to CBN for guidance on defining electronic banking policy.
g. Implement moderate limits on card transaction to minimize losses to fraud.
h. Enforcement of a KYC (Know-your-customer) policy for card issuance.
i. Implementation of string value check controls on financial web applications.
j. Initiating a "take-down" for reported phishing websites within 24 hours.
k. Monitoring and flagging suspicious transactions for investigation.
l. Immediate hot-listing (deactivation) of suspected compromised card.

7. Recommendations

Without prejudice, it can be concluded that the rate of e-payment fraud in the Nigerian banking system had significantly increased since the introduction of international debit card with adverse effect on the success and advancement of electronic banking in Nigeria. It has also been found that just like any other product; electronic banking products have greatly influenced customers' taste in terms of banking with convenience. Moreover, both Federal and State Governments are adopting electronic payment system because it has the potential of alleviating corruption and malpractices being experienced over internally generated revenue such as tax. The strategies for curbing the ugly trend of fraud however requires immediate attention by collaboration among banks and switching companies. In addition, CBN should continue to enforce and monitor non-compliance with the various guidelines issued on Electronic Banking System.

TIPS TO USE YOUR CARD SAFELY

Diamond
Your Bank

To protect your account while banking with your card, please always follow the safety tips below:

1. 

You can deactivate and reactivate your debit card on the self service module on Diamond Mobile App.

2. VISA
Our Diamond Visa Card is verified by visa, making it secure for online transactions wherever you are.

3. 

Remember to lift the restriction on your card; if you are traveling to the USA, Asia Pacific countries or any other location where PIN and Chip verification is not required.

4. 
Never reply to emails requesting for your card details. ***Never disclose PIN numbers to anyone.***

5. 
Never write down your Personal Identification Number (PIN) memorize it. ***Make sure you sign your card on the signature panel as soon as you receive it.***

6. 
Make a record of card account numbers and telephone numbers for reporting lost or stolen cards. ***Keep this list in a safe place.***

7. 

Always verify the transaction amount before signing the sales receipt. ***Keep your card in view whenever you hand it to a merchant.***

8. 
Do not leave cards in the glove compartment of your car. ***Never lend your card to anyone. Make sure your card is returned after every purchase.***

For enquiries, call 0700-300-0000 or email enquiries@diamondbank.com

e-Fraud: Fighting the battle, Winning the war

- Ayotunde Kuponiyi
Chairman, Committee of e-Banking Heads in Nigeria (CeBIH)

Introduction

Fraud is an age long threat to business establishments globally. This threat evolves and the magnitude of its devastations varies across different industries. The impact can be assumed to be relatively mild in some industries and grievous in others; especially in the financial sector. So many big and reputable corporations have been abruptly grounded by fraud scourge.

As the payment landscape in the financial sector and commerce in general is changing with the advent of internet, the mode and channels for facilitating payments have evolved over the years with the development of wide range of electronic payment systems.

It is not far-fetched that fraud incidence would definitely keep up pace; as criminals will continually devise nefarious ways to abuse and illegally profiteer from the emerging technologies. The fraud associated with electronic payment is tagged 'Electronic fraud' and popularly called “e-fraud”.

Interestingly, fraud reduction is always one of the cardinal objectives of any electronic payment system. As a matter of fact, the deployment of electronic payments systems has significantly reduced fraud and other financial crimes such as Money Laundering and Terrorism Financing globally. The use of electronic payment systems as tools for perpetuating fraud is a pure case of “Hunter becoming the hunted” just as every manner of crime typically fights back at any obstructive mechanism or structure deployed to fight it.

The development of payment technology may therefore be perceived as mixed blessings. The same technology that makes commerce more efficient and profitable is at the same time systemically creating avenues for perpetuating fraud which culminates in various degrees of losses. In fact, the fissure in electronic payment is so significant that organized crime has been built around eFraud.

The negative publicity created by the media around e-fraud instead of focusing on the benefits and accomplishments so far recorded by the adoption of electronic payment is also not helpful and further compound the public mistrust for the system.

This debacle of eFraud is a global phenomenon and should be treated concertedly, given that information technology has practically removed the geographical divides between

countries and making the globe to become a village. Nonetheless, every nation still has the primary responsibility of developing ways on how best to deal with e-fraud within its own territory.

What is electronic fraud?

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. 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 eFraud as "a fraudulent behavior connected with computerization by which someone intends to gain dishonest advantage"

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. Some countries disproportionate commitments towards fighting e-fraud

Overview of electronic payment in Nigeria

In Nigeria, the adoption of electronic payment system is rapidly gaining ground as evidenced in continuous positive growth in the volume of transactions processed in the country using payment cards and other e-banking platforms over the years; even though the dependency on Cash is still relatively high.

This development affirms that consumers, business and government agencies are embracing electronic payment systems as a reliable medium for facilitating trade- which is the main objective of any e-payment system. Without gainsaying, Electronic payment has become a key tool for improving the efficiency of our Nigerian economy, as it practically eliminates the attendant risks and costs associated with cash management.

The large scale adoption of payment cards and use of Automated Teller Machines (ATMs) which are earliest and still the two major electronic channels for facilitating individual payments

in the country is dated back around 2003- sequel to the release of E-banking guideline by the Central Bank of Nigeria. Although, some banks had deployed these channels long before then but were limited toonly their High Networth and other special categories of customers.

Before this time, Real Time Gross Settlement (RTGS) and Automated Cheque Clearing Systems using MICR were the main "electronic" platforms used by banks and other financial institutions to facilitate payments locally while Swift, Western Union and MoneyGram platforms used for international payments.

A major contributory factor to the rapid adoption of electronic payment system in Nigeria could be attributed to enactment of electronic payment policy by Federal Government Nigeria in 2005, which compels Government establishments in Nigeria to adopt electronic systems for the payment of allocations and salaries including setting a threshold on the maximum transaction amount can processed via paper cheque.

The adoption of the electronic payment system however suffered a major setback due to the widespread cases of fraud incidence notably skimming and account takeover that were characterized with the use of magstripe cards which resulted in consumers apathyand mistrust for cards and other electronic payment channels. In fact, some of the users had to fall back to traditional payment means- cash and paper cheque.

Whilst the exact amount of losses due to e-fraud on cards and other electronic banking platforms cannot be easily quantified, because the victims a lot of the times do not bother to report them, various reports and findings estimate that the total value would exceed 10billion Naira annually.

The significant improvements in the security of payment cards brought about by the full migration to EMV chip cards from magstripe and consistent customer educations on various ways of securing e-Payment have abated the growing fraud level and gradually restoring the lost confidence in the electronic payments in Nigeria. The feat was further consolidated by the following;

1. Intense consumer sensitization campaigns deployed by e-Payment service providers i.e. Banks and platform providers, on ways to safeguard transactions through electronic channels.
2. Awareness campaign embarked upon by the CBN on the use alternate channels towards achieving the objectives of Cashless policy.

The dominance of Cards as the electronic payment instrument is gradually shifting to Mobile and online commerce due to:

1. Increasing penetration of Mobile telephony
2. Introduction of mobile payment (Mobile Money) services and
3. adoption of digital commerce.

This development is expected to drastically change the landscape of electronic payment in Nigeria and is thus imperative for stakeholders to adequately prepare for the future tides and associated risks that may likely come with the full scale adoption of Mobile as a transactional tool/channel and emerging card-not-present (CNP) frauds.

Most common electronic fraud and the techniques

1. Electronic Clearing System fraud: This is a manipulation of account numbers for credit/debit for direct to account payment. This is usually through the interception and alteration of the originating or destination accounts specified in schedule for processing batch payment though electronic fund transfer within same bank or across banks.

2. Phishing: The fraudulent practice of sending emails or pop-up web pages purporting to be from legitimate companies in order to induce individuals to provide personal or sensitive business/account information e.g. credit card numbers, account information, PINs or passwords

3. Pharming: This technique is used in hijacking the web address of service provider. This occurs when a user types in a Web address and it redirects to a fraudulent Web site without your knowledge or consent. The website will look similar to the legitimate site with the intention of capturing your confidential information.

4. Account takeover: This takes place when a person takes over another person's account, first by gathering personal information about the intended victim, and then contacting their card issuer while impersonating the genuine cardholder, and asking for a mail to be redirected to a new address. The criminal then reports the card loss and asks for a replacement card to be sent. They may then set up a new PIN. They are then free to use the card until the rightful cardholder discovers the deception when he or she tries to use their own card and most times the account would have been drained

5. Card-not-present fraud: An unauthorized use of card details over the phone or on the internet

6. Skimming: It is a fraudulent collection of payment card details using typically a small electronic device called skimmer. The device most times is affixed to an ATM or Point-of-Sale terminals and allows criminals to capture customer's card

information including PIN. The advent of wireless technology has made it easier for criminals to remotely download stolen data without physically visiting the terminals.

7. SIM Swap fraud: This occurs when the phone number of a customer is hijacked through fraudulent SIM replacement at aTelco outlet/agent. The perpetrator then uses the mobile line to access the account of the victim usually via mobile banking or receives account sensitive details like PIN through PIN reset request.

Ways to fight and fight e-Fraud

Transaction security is a complex challenge that requires concerted efforts from all stakeholders in the payment space to be effectively dealt with.

Going by Winston Churchill "Winning a war is not exclusive preserve of the Generals but requires a collective responsibilities of everyone"

If the transaction security for facilitating payments via electronic platforms is not guaranteed, the requisite trust for the system to be successful will not be engendered.

Against this backdrop, the stakeholders must constantly fashion out how to deal with the issues of data availability, integrity, authenticity and confidentiality.

Safety and security of transactions in the banking system is fundamental in ensuring consumer confidence. It is therefore an important function and responsibility of the Central Bank to ensure that online transactions can be made in a safe and efficient manner in the economy; in the pursuit of monetary and financial stability objectives.

We are aware of the creative ways in which criminals have attempted to deceive customers over the years and measures were required to be taken by the banks to protect the customers. While it is good to know that banks have played their roles in investing in robust security systems, they must also ensure that customers play their part in protecting their own assets and savings.

The counter-fraud story isn't all about direct financial loss. Shrinkage or loss due to shoplifting has long been in the budgets of high street retailers and just as in online, there is a balance to be had between securing stock and allowing customers the freedom to purchase.

There is an increasing customer awareness and concern around their personal data online and in particular how well organizations in the public and private sector look after their payment information. High profile cases of data loss making headlines in the media do not help with this perception as highlighted in a recent IMRG/eDigital Research study which

showed that of the 2,000 respondents, 50 per cent felt online retailers should be doing more to look after their data.

The challenge for financial institutions and online businesses then is to balance financial risk with the costs of implementing these strategies and the brand impact of getting the balance wrong and upsetting legitimate customers.

1. All financial institutions, processors and businesses that accept card payments should ensure compliance with the Payment Card Industry Data Security Standard (PCI-DSS) by. Given that electronic payment space is predominantly carried out using payment cards, it is imperative that compliance with the PCI DSS standard becomes important for businesses of every size. Interestingly, PCI DSS compliance is now more cost effective and a lot easier to achieve as players can now deal with multiple vendor technology.

2. Electronic payment providers should regularly deploy technology solutions that will continually keep the activities of fraudster at bay. Fraud monitoring tools to detect suspicious transactions and behavior should be made mandatory

3. Review of legal framework to effectively allow the criminalization and prosecution of electronic payment related fraud. To complement the progress made by the various regulatory bodies towards improving the security of electronic payment systems in Nigeria, it is imperative that the nation reviews or enacts laws that will drastically discourage criminals to perpetuate fraud or facilitate the prosecution of electronic fraudster.

   As earlier stated, e-Fraud, is constantly evolving, hence it would be absurd to rely on acts/laws enacted during colonial era to prosecute electronic fraud at this age. For instance, it is still controvertible under the Nigeria jurisprudence if computer generated account statement is admissible in evidence in our courts. Furthermore, full prosecution and conviction of perpetrators of e-fraud will serve as deterrence.

4. The CBN needs to develop a well-articulated Action Plan for the prevention and management of electronic payment fraud in Nigeria. The plan should focus on setting up electronic payment bureau and given the following mandate;

   - Develop a framework on how insurance cover can be provided for all electronic payment related fraud.

   - Set up a bureau for electronic payment, where stakeholders and experts on e-Payment can continually share knowledge and best practice on the ways

to secure electronic payment in Nigeria. The bureau shall also be responsible for keeping records on frauds and their perpetrators.

- Set up a support center where electronic payment users can reach out to either block their cards or electronic account details in the event of fraud alert or incidence. Since most electronic payment users maintain multiple relationships with different electronic providers which sometimes makes it difficult for them to memorize all the contact details of the respective support centers, apart from the fact that some of the centers could not provide 24/7 service. Deploying a unified emergency help line similar to what we have for other emergency services such as police, health and fire services will definitely go along way to reduce e-fraud and in turn boost consumer confidence.

- Certification of all electronic payment platform and system. Similar to the Verified by Visa (VBV) and MasterCard and other security concept, it is important for Nigeria to develop its own stamp of authority for all payment platforms. This will guide users in identifying duly accredited and secure payment platforms in the country. Given that security practice is a dynamic action, the certified platform needs to be audited regularly.

5. Online merchants should always have it at the back of their minds that user convenience is the main thrust of electronic platform and therefore must not be relegated in developing security.

   Just as there is no absolute security for cash-currency, it may be nearly impossible to have same for electronic payment.

   In fact, by relating e-commerce with physical shop experience, no retailer will because of shoplifting want to build barriers. This can make his goods inaccessible to the customers. They would rather increase vigilance or make budget provision to accommodate any loss around any occurrence. In the same vein, it would not be out place if online retailers can have similar disposition to e-fraud. In other words, there should be a trade-off between user experience and cost of protection.

6. Robust dispute resolution mechanism should be put in place. In the event of fraud loss, it is essential to develop a framework that will define the protocol to govern the responsibilities of each category of users in the electronic payment space and also define the standard procedure for resolving dispute in case of breach especially using out-of-court settlement mode and liability shift.

7. Early detection being a key component of fraud management framework, it is very critical for e-Payment users to implement strong internal control mechanism such as prompt reconciliation to assist in early detection or prevention of e-fraud.

8. Awareness and customer education.
   a. There is a need for national awareness campaign on the benefits of embracing electronic payment and ways to safeguard it. The campaign will definitely increase the adoption of e-Payment, increase users awareness of e-fraud thus driving them towards making conscious efforts in adopting key safety measures against e-Fraud.

   b. Going by the saying that "if you don't blow your horn, someone else will use it as a spittoon' the media needs to concentrate more energy on reporting the benefits and accomplishments recorded on e-Payment than efraud menace. This will boost both the consumers and business confidence in adopting the e-Payment systems and thus mitigating the fraud loss impact.

9. Businesses and online merchants need to intensify the sensitization of users on the importance of online security and protection of personal and financial information as effective ways of preventing or managing fraud

10. Finally, with growing convergence on Mobile, the financial service providers and Telecommunication providers will increase collaboration in the areas of KYC, security and consumer data.

Conclusion: To foster consumer confidence in electronic payments and fight against fraud, much has been done and is still ongoing. The Banks and some payment card scheme providers have done a lot in fighting the e-fraud by educating users and deploying technological infrastructure to combat the menace.

However, as the electronic payment ecosystem develops and we witness technological advancements, the potential for payment fraud is expected to increase especially with new threats, such as data hacking and identity theft. Unwavering commitments from all the stakeholders in electronic payment and the citizenry are required for us to win the battle of e-Fraud with the limited available resources.

The future is pan-African

Ecobank has the banking products and services for you

Ecobank accounts to help you manage your finances.

- Ecobank Savings Account
- Ecobank Current Account
- Ecobank MyFirst Account
- Ecobank Deposit Account
- Ecobank African Diaspora Account

Ecobank, banking that's designed for you.

- Ecobank Cards
- Ecobank Mortgage Loans
- Ecobank Rapidtransfer
- Ecobank Western Union
- Ecobank Personal Loans
- Ecobank MobileMoney
- Ecobank Bill Payment Solutions
- Ecobank Business Loans

Ecobank, wherever you need us.

- Ecobank Advance Account
- Over 2,600 ATMs
- 12,300 POS
- 1,284 branches in our network
- Ecobank Internet Banking

ecobank.com

Ecobank
The Pan African Bank

E-Fraud: Fighting the battle, Winning the war

E-Fraud is the use of computing devices and information technology to commit crime in which some kind of deception is used for personal gains which is usually financial in nature. The industry adoption of the e-payment channels as the preferred channel of payment has increased the incidence of electronic fraud. With globalization and advances in technology, fraudsters have become increasingly sophisticated with wider reach to unsuspecting customers which has resulted to huge losses recorded by financial institutions and its customers, Nigeria inclusive. These heightened incidents of fraud have therefore brought to the fore several pain points to the customers and banking industry as a whole.

Electronic fraud can be broadly divided into two categories:

i. Card Fraud which involves the fraudster either skimming the card details or outright stealing of the card and using the card to conduct transaction via ATM/POS/Web. Transactions on card fraud are rampant in non-EMVcountries like US where PIN is usually not required.

ii. Phishing & Identity Theft is when the fraudsters send fake e-mails or web link to unsuspecting victims with the hope of stealing their bank account details, card details, usernames and passwords or infect their computer with Trojan which allow them control the system should the victim follow the instruction contained in the e-mail.

Therefore, in order to tap from the opportunities in the e-payment space, which has been identified as a major channel to drive financial inclusion, there is need for relevant stakeholders to implement strong authentication and transaction security systems to secure customers as well as the e-payment environment.Nigerian financial institutions in conjunction with the Central Bank of Nigeria have over the years, made remarkable progress in combating electronic fraud. Some of the effective measures put in place in fighting and winning the war on e-Fraud are highlighted below.

I. Enforcing Second Factor Authentication (2FA) on all Financial Channels: The second factor authentication adds additional level of protection to the transaction. It is best practice to implement the 2FA on all financial application and card products. This control is largely to protect theft of the identities of staff of financial institutions and use of same to post fraudulent transactions. This type of fraud scheme was very rampant in the Nigerian Banking space a few years back and substantial sums of funds were lost to fraudsters who perfected the act of using hard/soft devices to capture the login credentials of unsuspecting members of staff of banks and using same to process transactions on either their core banking application or on the other funds transfer platforms.

   Before the directive from the Central Bank of Nigeria for Financial Institutions to implement this control measure, most institutions have on their own done so and this has resulted in a marked reduction in the losses associated with this fraud scheme.

ii. Setting Limits on the various Payment Channels: Financial institutions have harmonized the financial limits on the different payment channels in line with the CBN directives. These limits have helped reduce the exposure in the event of compromise. Prior to this initiative, fraudsters had taken advantage of the lack of limits to increase their loots. This control, will only work when other complementary controls are in place. We have seen instances where fraudsters on their own, after gaining access to financial platforms, increased the limits to enable them move substantial funds.

iii. Authentication of all Card Transactions: The industry have implemented chip + PIN validation for all card present transactions as well as VBV/secured code for all card-not-present (CNP) transactions. More so, the implementation of PIN enforcement for all magnetic stripe transactions. This has helped card fraud cases to drop significantly. However, this is a temporary measure pending October 16, 2015 when EMV liability shift in US will come into effect.

iv. Inclusion of Information Security in Project Management: Inclusion of information security during the analysis and design stages of business solutions have helped to identify and close platform vulnerabilities, which are usually exploited by fraudsters. Available statistics have shown that institutions where this is standard practice are more able to prevent fraud by ensuring that adequate controls are built into their systems than those who do not.

v. Compliance with Regulatory Directives: The CBN through regular circulars and directives has kept the industry on its toes in terms of compliance with measures that are aimed at making the payment system safer.

vi. Implementation and Adherence to Information Security Standards: Banks have implemented and adhered to various international security standards. This has improved the way cardholders' data are transmitted, processed and stored. Some of the standards are the Payment Card Industry Data Security Standard (PCI-DSS) and International Standard Organisation Information Security Management System (ISO27001: 2013 ISMS).

vii. Enterprise Network Security Management: A lot of measures have been taken at the enterprise level to ensure that banks remain secured. Hardening of servers and endpoints, data loss prevention programs, anti-virus protection, proper network segmentation and firewall restrictions have gone a long way to keep the fraudsters at bay.

viii. Automation of System Activities: Monitoring ensures that suspicious transactions are promptly identified and investigated. A dedicated electronic transaction monitoring team is put in place to actualize this objective. A number of monitoring tools have been implemented for monitoring electronic transactions, system configuration changes, network traffic, data base activities and systems logs.

ix. Implementation of Electronic Fraud Risk Management: This ensures prompt detection and prevention of complex fraud schemes, minimizes losses, maximizes customers' trust and reduces reputational risk. Moreover, investigators can focus on the most urgent and actionable fraud alerts. Thus, there exist:

- Pre-built fraud scenarios
- Event identification, correlation and surveillance across the enterprise
- Intelligent alert correlation from point fraud solution
- Real-time monitoring and interdiction capabilities
- Comprehensive case management

x. Training and re-training of Staff on emerging trends: Understanding the need to train staff on various emerging dynamics of electronic transactions is germane. This ensures competitive edge in the market and promotes safety, efficiency and productivity which overall, improves the profitability of the electronic products.

xi. Employee Background Check & Know Your Customer (KYC): Each new employee adds to the business and security risk of the organization. Background check is an effective way to discover potential issues regarding an employee that could affect the business. In the same vein, verifying the identity of the customer can help reduce identity theft, financial fraud and money laundering. Know Your Customer is a regulatory policy and has recently included the Bank Verification Number (BVN) biometric enrollment. This project which is driven by the CBN when concluded, would improve security and identity management of all banks' customers.

xii. Collaboration among Stakeholders: The internal stakeholders (Business, Technology, Operations, Risk and Control teams) hold regular review sessions on e-banking performance and emerging issues. There is also active collaboration with external stakeholders (DMBs, NeFF, CeBIH, CBN, NIBSS, etc.) for exchange of ideas and solutions to identify industry problems.

xiii. Continuous Customer Awareness: This is an important aspect of the information security program. Without adequate awareness, most of the resources spent on technology would not achieve much. This is because the chain is only as strong as the weakest link. The bank is continuously educating customers through e-mail and SMS notifications, newsletters, adverts, banners and jingles on how to secure their financial transactions.

Conclusion

While we understand the plight in finding solution to the rising incidence of e-fraud, we must point out that the trend has severe consequences for the financial industry in the country, and would impact negatively on bank customers' relationship, which is anchored on trust.

However, it is worthy of note that our resilient fight is gradually winning the battle, but a lot still needs to be done. The fraudsters are always looking for the next opportunity to exploit. Stakeholders should therefore strive to be steps ahead at all times to beat them at the game. There is need for more investments in preventive measures while pursuing expansive programs thus ensuring that relevant controls are embedded in all e-payment systems (people, process and technology).

www.fidelitybankplc.com

FIDELITY

Don't Trust Everything You see

Things are not always as they seem especially online.
Here are a few tips to protect you from internet scammers:

- Do not share your personal financial details
- Visit only trusted websites
- Do not share ATM card PIN or internet banking passwords.
- Create strong passwords
- Check privacy settings on your devices and online accounts.
- Protect devices that are connected to the internet.

Fidelity Bank will never ask for your personal banking details like internet banking password or ATM PIN.

WAYS TO BANK WITH US

Branch | ATM | Internet Banking | Mobile Banking | Contact Center

Contact us on +234(1)4485-252, +2348003433548 or email true.serve@fidelitybankplc.com

Fidelity Bank Plc
we keep our word...

e-Fraud: Fighting the battle, Winning the war – FirstBank Story

Today, all aspect of banking is technology driven. The extent to which a bank remains competitive is dependent on how pervasive technological solutions have been deployed to enable its processes perform more efficiently.

FirstBank as a key player in the industry has been in the fore front of utilization of technology to power its processes and service delivery. Technologies in the area of core banking, internet banking, mobile banking, SMS alert banking, collections, etc, are among the solutions in use.

Just as the saying goes, “where there is a carcass, the vulture will gather.” The switch to automated operation and services delivery has thrown up challenges associated with activities of criminally minded individuals. These criminals are taking advantage of inherent weaknesses in technological solutions and infrastructure to perpetrate criminal acts.

Electronic fraud is now a big industry and e-criminals are coming up with sophisticated ways to defraud banks of customers' deposits and hard earned revenue.

To this end, FirstBank responds to these challenges through various technological, process and people approaches.

In 2009, the bank was the first in the industry to go for ISO 27001:2005 Information Security Management Systems (ISMS) certification. The bank got certified in early 2010. In 2011, the bank achieved BS25999 - Business Continuity Management Systems (BCMS) and this was eventually upgraded to ISO 22301 BCMS. The bank also obtained Payment Card Industry Data Security Standard (PCI DSS) in 2013.

Our Automated Teller Machines have been upgraded to meet EMV standards, installed components and protective guards against anti-skimming and video recording devices. Close circuit cameras and security guards are mounted to provide surveillance for ATM terminals.

The bank acquired and installed various tools and anti-fraud solutions to monitor customer transaction behavior and pattern. We have setup a top of the pack Security Operation Centre equipped with best in class security appliances and adequate manpower to alert customers of suspected fraud. The infrastructure operates both at detective and preventive mode 24/7. To provide additional layer of security against fraud for both card present and card-not-present scenarios, the bank installed user friendly, adaptable, quick to act fraud

and risk prevention solution that will function in true real-time and put customers' in-control of defining activities that could take place on their chosen electronic payment platforms.

The bank has installed anti-phishing solution to frustrate phishing attacks against its websites and internet banking platform. Our Internet banking platform is equipped with two factor authentication (Token), One Time Password capability, beneficiary management and limit based transfer regimen. Communication between customer and our online banking application is encrypted end-to-end.

SMS and E-mail alerts are promptly sent to customers whenever transactions are consummated on their account(s); allowing them to monitor their activities on-the-go.

There are adequately trained and certified security professionals within the bank with relevant certifications like Certified Information Systems Security Professionals (CISSP), Certified Information Systems Audit (CISA), Certified in Risks and Systems Controls(CRISC), and various other certifications such as ISMS, BCMS and PCIP.

A crack team of investigators are on ground to quickly handle fraud incidents by unraveling their root causes, provide remediation and share lessons with stakeholders to forestall future occurrences and/or minimize impact.

Security awareness campaigns are conducted regularly for both internal and external stakeholders. Our customers are routinely communicated to alert them of prevailing malicious social engineering attack techniques being exploited by fraudsters. This helps to educate customers to be conscious of their personal identifiable information and protection against identify theft.

Secure Banking Experience

– The GTBank Recommendation

Fraudsters use a variety of persuasive techniques to gain the confidence of their targeted victims. These techniques are often referred to as 'social engineering' and are used to coerce people into freely giving away security information, access to accounts or even handing over their cash.

Guaranty Trust Bank Plc, one of Africa's foremost financial institution and leader in innovative banking has constantly developed platforms to provide secure banking to its esteemed customers. With its great bias for technology, GTBank has installed several new technologies and introduced a number of internal procedures to prevent fraud on customers' accounts.

Commenting on the recent rise in popularity of an old-style email and phone scam; Guaranty Trust Bank's advice to its customers is that they should never disclose their PIN, Passwords, Token Codes or any personal financial information as a result of someone calling over the phone or sending an email to click on a link – wherever they claim to be from. If customers appear to have already been a victim of this scam, they should contact the bank immediately on a number they know to be correct.

GTBank is continuously developing and implementing security enhancement to ensure the integrity of our online banking platform. Our goal is to protect the online safety and the confidentiality of our customers.

The Bank further advised its customers that fraudsters typically gain the confidence of their targeted victims by claiming to be from their bank. Most of these scams can be stopped easily, provided bank customers:

- Do not disclose PINs, Token Codes, login details and passwords in response to any email or telephone caller claiming to be from your bank
- Always give cold-callers a cold reception
- Destroy any document or receipt that contains personal financial information when you dispose of them.
- Do not fall prey to any website that looks similar to GTBank's website. Always check the URL (https://)
- Create strong passwords for their internet banking login and card details.

Guaranty Trust Bank has always been committed to the safety of its stakeholders' funds. A few years ago, the bank installed a whistle blower platform to help mitigate instances of

fraud whilst resolving customer service related issues. The channel enables customers, staff and other stakeholders of the bank to report unethical or unprofessional conduct by its employees without revealing the complainant's identity. The GTBank Whistle Blower is a very secure platform that is hosted on the bank's website for easy access.

Authorities at the bank have stated that they remain ardently committed to proper practices and preventive mechanisms that safeguard the properties of its stakeholders. The bank intends to continue strengthening its security processes at all touch points, whilst promoting its value system, which is hinged on international best practice, professionalism, ethics, integrity and superior customer service.

Guaranty Trust Bank's leading role in the provision of secured technological platforms to its customers recently received international applauds as the bank was awarded a Payment Card Industry Data Security Standard certification (PCIDSS). PCIDSS certification is worldwide security standards maintained by the Payment Card Industry Security Standards Council (PCISSC) to detail acceptable technical and operational requirements, which help organizations that process credit/debit card payments, prevent credit card fraud, hacking and various other security vulnerabilities and threats. A certificate of compliance was issued to the bank validating its compliance as a level 1 Acquirer and Issuer under the Payment Card Industry Data Security Standard, version 3.0.

The bank also holds a Standards Organisation of Nigeria (SON)'s International Standards Organisation (ISO) 9001:2000 certification in recognition of quality management systems and conformity with global best practice.

The bank has in place, a Communication Policy which ensures appropriate disclosure and transparency in its communication while taking into account the concept of confidentiality between the bank and its customers, and bank secrecy. This contributes to maintaining a high level of accountability and safeguards the integrity of the bank's financial reporting.

The bank has since then invested heavily in improving its AML systems and controls, including significantly increasing the resource of its compliance department and hiring additional personnel. GTBank remains committed to the highest levels of governance and controls in all of its businesses and also to ensure that its AML controls are fully compliant with regulatory standards in all the countries it operates in.

Securing our e-Channels

Introduction

The banking/ financial industry of the 21st century operates in a complex and competitive environment characterized by changing factors and highly unpredictable climate, thus, information communication technology (ICT) is at the fore front as the basis of innovation to provide up to date software and facilities to aid banking. The financial industry is one industry that is using this new ICT media to offer its customer value added services and convenience. This system of electronic interaction between the consumers and the services offered by the financial industry is known as the electronic banking system.

Electronic banking therefore is the use of computer/ electronic devices to retrieve and process banking information (statements, transaction details, etc.), and to initiate transactions (payments, transfers, service requests, etc.) directly with a bank or other financial services provider remotely via a telecommunications network. Generally, electronic banking is a relatively new industry that enables individuals and businesses to interact with their financial services provider via non-traditional means from virtually anywhere in the world.

Concerns about electronic Banking

Since electronic banking is a new technology with many capabilities and potential problems in equal measure, users are hesitant to use the system. The use of electronic banking has brought many concerns from different perspectives. Consumers of the electronic banking platform have raised concerns about this new medium of interaction. Since many large transfer of funds is done by customers, these customers are concerned about the security of their funds. At the same time, the customers also consider the potential savings in time and bank charges plus inherent risk associated with this system. Banks are pressured from other financial institutions to provide a wide range of financial services to their customers. Banks also profit from handling financial transactions, both by charging fees to one or more participants in a transaction and by investing the funds they hold between the time of deposit and the time of withdrawal, also known as the “spread”. With all these concerns raised, there’s an increased need by the bank to put in place security measures to checkmate possible fraud and loss of customers funds and income, and when this is in place it will increase trust and patronage of electronic platform.

e-Products within the Bank

- Debit Cards (MasterCard and Verve)
- Pre-paid Cards (MasterCard and Verve)
- Point of Sale (POS) Terminals

- POS/ mPOS Terminals
- ATM/ Kiosk Terminals
- Mobile Banking
- Internet Banking

Security Features on e-Products / Channels

The notion that security services is not cheap is well established and therefore Heritage Bank has put in place numerous solutions to ensure adequate security of its eProducts/ eChannels against fraud and crime with emphasis on industry best practice. These solutions were put in place having existing customers in mind, and most of all, to be able to provide secure and favourable banking product to the public using eChannels. Heritage Bank will continually invest in security solutions to guarantee the safety of its investments and that of its customers.

The following are key security solutions implemented by the bank;

- National Fraud Service (NFS)
- MasterCard InControl
- ScoreBridge
- Anti-Skimming Device
- PINGuard
- ATM Security Solutions
- Password/ Security Question/ Transaction Password and Transaction PIN
- Trusteer

National Fraud Service:

This solution is provided by MasterCard to protect MasterCard cardholders, financial institutions as well as merchants against criminal activities. This system is used to monitor and evaluate all transactions processed on the MasterCard network and quickly detect high-risk transactions in real-time using state-of-the-art detection technology.

The service is unique to MasterCard users only (credit and debit cards inclusive) and it cuts across all transactions made across all channels, including but not limited to, ATM, POS, Web and Mobile.

MasterCard InControl:

This security solution empowers cardholders to individually and independently specify parameters that determine the usage of their credit, debit and prepaid cards, and even block transactions that are deemed inappropriate. Additionally, it enables the customers to receive real-time alerts on card activity via email or SMS. Consequently, one can manage his/ her finance more efficiently whilst spending with greater confidence and assurance of security of funds.

This technology is a key tool for issuing banks to build loyalty with existing cardholders, attract new ones, and in turn, achieve financial inclusion.

ScoreBridge:
This is a fraud detection application that checks the region of transactions against the timing. This solution takes a look at previous pattern of transactions and also the place and location last transaction and compares it against current transaction, and if there is discrepancy, it spots it.
This has been able to mitigate web based fraud and card cloning fraud.

Anti-Skimming Device:
This helps to monitor the entire card reader environment and restrict illegal insertion/ intrusion of fraudulent devices. This security system is installed on the ATM and is not visible from the outside.
The device is able to frustrate both digital and analog skimming attacks.

PINGuard:
This is installed on all ATMs to safeguard customers personal identification numbers (PIN). The device is installed directly on top of the electronic PIN pad (EPP) to reduce the exposure of customer's PIN thus mitigating shoulder surfing, etc.

ATM Security Solutions:
Advanced ATM security solutions make it extremely difficult for intruders/ robbers to succeed with physical ATM attacks. These security systems are designed to detect intrusion attempts and react immediately by frustrating the efforts via delay techniques whilst also alerting the relevant authorities for adequate response.

The solution includes but is not limited to CCTV cameras, access control, burglar alarms, electronic safe enhancements, etc. with remote monitoring capabilities.

Password/ Security Question:
This is available on internet and mobile banking that stops unauthorized access and reduces fraud on customers account. This form of security is a stop gap to unauthorized access to customer's internet banking.

Trusteer:
This prevents/ mitigates against phishing attempts on the internet banking platform thereby frustrating efforts to harvest customers' login credentials when the platform is being used.

Conclusion and Recommendations
The Internet enhances the interaction between two businesses as well as between individuals and businesses and has grown exponentially, with more than 30 million users

worldwide currently. As a result of this growth, electronic banking has emerged and offered tremendous market potential for today's businesses. The banking industry has benefitted from this new phenomenon offering its customers with a wide range of services.

Heritage Bank is focused on research and innovation within the financial services sector to avail electronic solutions that will promote convenience to its customers. In a bid to reduce security vulnerabilities, Heritage Bank ensures that multiple solutions - both software-based and hardware-based systems – are deployed to meet the ever changing industry threats.

For sustenance and growth of the electronic banking business, the security solutions and the privacy aspects provision need to be dynamic. With the security and privacy issues addressed, the future of electronic banking is deemed to be prosperous.

whatever channel **you** choose...

...you get the same **PREMIUM** experience.

CARDS | POS | KIOSKS | ATMs

ONE
BIGGER, BETTER

CALL: 0700-HERITAGE (0700-4374 8243); 01-2369000

Heritage Banking Company Limited RC: 19868

www.hbng.com

Heritage Bank

e-Banking Risk Management:
Marrying Technology with Traditional Tools

Moore's Law has proven that in today's world, the rate of growth and change of technology is exponential. Implication of this is that technology is constantly changing in a steady progression. Our world is driven by technological devices whose size and price appears to be inversely proportional to their speed, efficiency and capability. This dramatic advancement has also caused a major efficiency boost to other industries and in some cases, creating uniquely new ones.

Traditional banking is fast paving way for electronic banking as the new way of providing financial services; it has expanded the markets, created new products and services and provided an avenue for reduction in operating cost for banks. More broadly, the continued development of electronic banking has contributed to improving the efficiency of the banking and payment system, removing traditional barriers to transactions thereby reducing the cost and time of retail transactions both locally and internationally. Consumers and merchants now enjoy a greater level of efficiency and convenience while transacting (making or receiving payments).

As transactions became faster, less cumbersome, more ubiquitous, more impersonal/faceless, so did the risk of theft, fraud and technological failure or crash also increased. Generally, the surge of e- Banking has not introduced new risks to doing transactions but has increased and amplified existing risk. The threat of cash theft remains basically the same in nature, but just so happens to be done faster, easier and with huge impacts - as such new risk management challenges such as the need to increase speed of detection and accuracy in prediction has now crystalised.

Identifying and defining an organization's risk appetite vis-a-vis ability and willingness should be the starting point before embarking on any e-business venture. Once the risk threshold is defined and adequately communicated, minimum security guidelines and control standards should be established by the bank in relation to its electronic banking activities. This can be done by the development of security policies and controls, geared towards ensuring that set appetite or thresholds are not breached, identified risk are constantly monitored and the bank adequately protected at all times.

Effective e-banking risk management can only be achieved with adequate investment in cutting edge technology – fire walls, transaction and customer authentication, data security, data encryption and audit trails. While the importance of investing in technology and its application to combating risks associated with e-banking cannot be denied, it is important that financial institutions and their risk managers pay utmost attention to the traditional control measures like pre-employment employee screening, adequate and effective segregation of duties, enhanced physical security, extensive training and awareness of

staff, customers and general public on e-banking threats they may be exposed to, and how to manage them.

The highly dynamic nature of today's technology and the ever changing customer expectations and needs make it difficult for the risk manager or security analyst to keep a tab on identified risk exposure and the prevention of attendant losses. Banks must learn how to use the mix of technology and traditional control measures as a means of preventing the manifestation of inherent risk in e-banking.

e-Fraud: Fighting the battle, Winning the war

Introduction

As Banks intensify their drive for bigger market share, more products and services are getting more complex. As products and services get more complex, the need for technology to drive actualization of product offerings is becoming important by the day. These technology platforms, as good as they are in providing fast, reliable and robust transaction processing system, have also expose banks to unprecedented online fraud through the activities of hackers and fraudsters. The increase in the use of electronic cards as a means of payment for goods and services has also added significant risk to banks' portfolio of fraud typology. It is the realisation of the negative impact of fraud on a bank's growth that is propelling fresh initiatives in the fight against fraud.

It is no longer sufficient to detect fraud after it has happened; the focus has now shifted to fraud prevention through the application of people, process and technology oriented initiatives. To ensure that transaction processing technology platforms remain reliable and safe at all times, banks have continued to implement many anti fraud initiatives aimed at ensuring the safety and security of customers' transactions. Some of the initiatives are presented below:

Types of e-Fraud

Identity Theft: An identity theft occurs when a fraudster has acquired enough personal information of the genuine account holder, and is able to satisfy all the conditions prescribed by the financial institution before a transaction is consummated. As dependency on internet for transaction processing continues to grow, online identity theft has become more rampant. Staff and customer sensitization programs on the proper handling of sensitive account information are key to preventing this type of fraud.

Fraud Perpetrated By Relations: Fraud by relations, friends and associates is on the increase. We have seen cases where very close associates of target victims were able to successfully orchestrate fraud on accounts belonging to a relation/friend. The fraudsters usually leverage on the opportunity provided by close relationship to obtain vital information from the target, and then go further to use the information to commit fraud.

The strongest defence against this type of fraud is customer education. Customers should be sensitised on the importance of keeping their sensitive account information confidential.

Internal Fraud: This is a situation where employees of financial institutions either by themselves or in collusion with others, perpetrate fraud on either customers' accounts or on internal accounts. This type of fraud is not really new, but online banking has added another channel through which a fraudulent employee can steal. Financial institutions should not allow employee unrestricted access to customer sensitive data. All online transfer platforms

should require the use of PIN/Token before transactions are consummated. Additionally, sensitive data such as PINs (Primary Identification Numbers), credit cards numbers, account numbers, etc, should be encrypted.

Types of Fraud Threats

There are two broad categories of fraud sources namely; Application and Network based threats.

Application Threats: Transaction processing applications are usually the main target of fraudsters because online transaction processing platforms are the most visible to the fraudster/hackers. They can interact with it legitimately or otherwise, hence their preference for such applications as a first line of attack. In most cases, all that is required is to steal legitimate customers' vital login credentials and use such information to commit fraud. That is why most systems security infrastructure such as firewalls proxy servers, intrusion detection systems, cannot prevent this type of fraud. Customer education and sound internal control process in financial institutions is the best form of protection.

Network-Based Threats: Network devices and infrastructures are usually the target of sophisticated hackers. These hackers are usually interested in harvesting customer sensitive data for various reasons. Some hackers attack corporate network for pride while some hack for financial gains. Whatever the reason for the hacking, the impact on the targeted financial institution is usually devastating. Over the years, financial institutions have deployed a host of tools to fight this type of threat. Infrastructures ranging from firewall, intrusion detection systems and in some cases, full blown security operation centre (SOC) have been used to mitigate the negative activity of the hackers.

Fraud risk mitigation tools

The broad category of risk mitigation tools are focused on people, processes and technology

People

People are usually the most important factor in any fraud prevention strategy. This is because it is the people that perpetrate fraud and it is only other people that can effectively stop them from doing so. Staff and customer education remains on the top of agenda in the fight against fraud. Staff in all areas of operations in financial institutions must be properly trained in operations and control activities. It is only when the staff knows what to do in all situations that they can proactively identify fraud and stop it before it happens. Similarly, awareness campaigns should be run for customers on how to protect their sensitive data and other related matters. When people are properly trained, and the right information consistently and regularly passed down to customers, fraud will be effectively controlled.

Process:

After people, process is usually the next in line for financial institutions in their fraud fighting strategy. All areas of the organisation should have strategy document that encompasses

policies, procedures and sanction grids. All these documents should be prepared based on best practices and established process frameworks. In financial institutions, certain processes are becoming very import in the fight against fraud. Some of these processes are:

1. Know Your Customer (KYC): Financial institutions should put in place KYC processes that can effectively be used in fraud investigations. Usually with sound KYC processes, possibility of fraud can be identified before the actual act. Financial institutions are therefore advised to strengthen the KYC practices as a way of fighting fraud
2. Transaction Monitoring: Fraudsters are usually not comfortable if they know that their activities are under scrutiny. They usually target areas of operations that are not properly monitored and launch their attacks against such areas. Financial institutions should implement automated fraud monitoring solution across sensitive online transaction platforms as a way of keeping fraudsters in check. In recent times, transaction monitoring through the implementation of behavioural monitoring solutions has proved very effective in the fight against fraud at the application level.
3. Other Key Processes: Other processes that are key to fraud prevention are professional employee recruitment processes which should incorporate proper background checks, staff imbibing good work ethics and professionalism, and general staff orientation towards fraud prevention.

Technology:

Although, technology is usually considered to be the last when deploying fraud strategy, it is by no means very important. Modern day banking is characterised by complex product offerings, dynamic customer service options and voluminous transactions data across transaction processing platforms. This modern day banking characteristics have left banks with no choice but to implement relevant technologies in the fight against fraud. To remain relevant for sustainable growth, banks must continue to invest in technologies to drive their fraud prevention strategy, which also complements the activities of people and process effectively.

General Anti Fraud Tips

1. Customer Education is very key if the fight against fraud in the financial institutions is to be effective.
2. When sending information to customers over the internet, due care should be taken by financial institutions to ensure that such information does not get into wrong hands.
3. Customers should be encouraged to properly scrutinize their statements of accounts and promptly point out inconsistencies to their bankers for investigation.
4. Customer should imbibe the habit of shredding used confidential bank documents they wish to destroy. Simply throwing such documents into the thrash bin or tearing them is not sufficient to prevent such information from getting into wrong hands. Burning them may not even be a solution, as some left over prints may still be visible on the burnt documents.

5. Customers should avoid unsecure online shops where the possibility of a compromise of their account details is high. They should always check out for security symbols and good references before shopping.
6. All computers engaged for online transactions should be properly secured by keeping the anti virus, anti malware, etc, up to date. Firewalls should also be activated for further security.
7. Customers should be encouraged to beware of online or email scams that solicit their personal information. A bank will never request for such sensitive information through public platforms such as emails and open websites
8. Customers should be encouraged never to write down their passwords, security questions and other sensitive information. Such information are better secured by keeping them in memory.
9. When carrying out transactions using ATM terminals, a customer should visually inspect the ATM machine for any abnormal devices such as skimming device. They should also ensure that no body is watching over their shoulder to capture their PIN
10. If a customer suspects that any of his sensitive account information may have been compromised, he should immediately notify his bank for immediate reset. Customers should promptly change default PINs/Passwords

Conclusion

While the internet offers great opportunity, its pervasiveness also poses a real threat to every business including financial services. The fight against fraud is for all stakeholders in the financial service industries. As the saying goes, “a chain is only as strong as it's weakest link”, hence the need to strengthen all players to play their roles in accordance with best practices. Collaboration and sharing of information on fraud are also very key in the ongoing fight against fraud. Everybody must be vigilant and stay abreast of developments in the financial service sectors in order to totally win the fraud war.

Homeorabroad

Experience a world of cashless transactions with Skye Bank e-commerce solutions

Mobile Banking | Merchant Banking | Internet Banking | ATM Services

- **High level security is guaranteed with MasterCard secure code**
- **Access to over 30 million ATMs worldwide**
- **No extra charge on POS and Web transactions**
- **Access to Quick Teller Services**
- **Competitive conversion rate for international transactions**

Convenient. Safe. Secure.

Call our yes! CENTER on 0700 SKYE BANK, 0700 7593 2265, 0806 988 0000, 01-448 2100

Follow us on:

Nigeria • SierraLeone • Guinea • TheGambia

www.skyebankng.com

Skye Bank

Expanding your world

Fight against e-Fraud:
The five (5)-way approach for Nigerian Banks

Introduction

The Association of Certified Fraud Examiners (ACFE) describes fraud as any intentional or deliberate act to deprive another of property or money by guile, deception, or other unfair means. Based on this premise, one can describe Electronic Fraud (e-Fraud) as an intentional or deliberate act by anyone or group of people to deprive a bank (and/or its customers) of money (or equivalent value) using or targeting the bank's electronic payment channels and platforms.

E-Fraud; an 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 categorized by Payment types

	Transaction Volume		Transaction Volume	
	2013 count	2014 count	2013 (N)	2014 (N)
POS	11,258,846	24,607,497	229,903,237,909	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 (N)	2014 Loss Amount (N)	% Change
Cards	ATM[1]	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	2,120,881,512	680%
E-commerce		13,948,390	58,994,920	323%
Mobile		6,787,544	13,328,957	96%
Cheques		8,693,770	4,448,600	-49%
Total[2]		485,194,350	6,215,987,323	

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

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

The way forward

In order to arm Nigerian banks against e-Fraud, the leadership of each bank 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. It is important for banks to pay attention to the following five (5) 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, analyse and prevent) fraudulent transactions on the internet/mobile banking, card platforms and other electronic payment channels. A bank should not deploy a fraud monitoring solution just to meet regulatory requirement/deadlines, but should ensure that it performs due diligence in identifying, selecting, funding and implementing a scalable and effective fraud monitoring solution. On implementing such solutions, banks should also set up a dedicated fraud monitoring team that will review and action fraud alerts that would be triggered by the system.

After implementing a fraud monitoring solution, each bank's stakeholders should perform an objective post-implementation review in order to identify fraud trends (pre and post implementation), false positives alerts, undetected e-frauds and possible need to update the solution's configuration in order to address noted gaps.

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.

It is important to perform independent and objective reviews to reassure ourselves that our IT security frame-work is up to relevant international standards. Beyond obtaining accreditation, banks should implement cyber security controls that will reduce the impact of an advanced attack as perpetrated by Carbanak, the considerations should include, in addition to general IT controls the implementation of application, whitelist to prevent execution of unknown/ unauthorized software on systems, implementation of strong authentication controls and isolation of critical systems within the banks' network to prevent unauthorized access.

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.

In order to mitigate this inherent risk, the leadership of each bank should firstly consider the implementation of fraud detection/prevention frame work that will flag suspicious / sensitive activities by employees and vendors on the electronic payment channels for further investigation.

Secondly, it is imperative that banks train their internal control, audit and investigation employees on required skills to review and investigate IT solutions as knowledge gap may increase the risk of not detecting e-Fraud incidents.

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. The best tool is for banks to conceptualize and design effective (easy-to-understand) awareness campaigns that will assist people to identify and respond to these threats. While email warnings may protect a bank from being liable for phishing fraud, it may not protect such bank from the risk of reputational damage. Nigerian banks should consider embarking / promoting a massive nation-wide awareness campaign.

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.

In addition, the leadership of Nigerian banks in conjunction with the Economic and Financial Crimes Commission (EFCC) and the Central Bank of Nigeria (CBN) should consider requesting the National Assembly to pass a bill that will aid the prosecution of financial crimes. Such requests should include a dedicated court for prosecuting financial crimes involving Nigerian banks and providing more explicit details in 2013 Cybercrime bill.

Conclusion

E-Fraud as a subset of cybercrime is like a war that is not expected to end; at least not in the nearest future. Also, just as a war may involve several battles, likewise is e-Fraud which continues to emerge with new trends. It is therefore essential for Nigerian banks to individually (and collectively where necessary) implement fit-for-purpose fraud monitoring solutions, standard IT security framework, controls that will minimize internal employee frauds, an intensified e-fraud awareness campaign and a collaborative venture to prevent fraud and prosecute fraudsters.

In KPMG's words "the battle against cybercrime is a typical example of a rat race that is difficult to win. The least one can do is to try to stay as up to-date as possible".

Bring your thoughts to life

For every need, there is a Stanbic IBTC card to bring your thoughts to reality. Stanbic IBTC cards are safe when used to make payments via POS and online merchants as well as withdrawing on ATMs.

Verified by VISA MasterCard SecureCode

www.stanbicibtcbank.com

"Moving Forward is a Trademark of South Africa Limited"
Stanbic IBTC Bank PLC

Stanbic IBTC Bank

A member of Standard Bank Group

Moving Forward ™

e-Fraud: Fighting the battle, Winning the War
– The Standard Chartered Bank perspective.

Electronic fraud or e-fraud in its short form as it is commonly called, is financial loss or fraud perpetrated through an electronic platform or product. The ease and convenience that electronic products and channels offer, is an attraction to new users and a source of loyalty to many users who have embraced the new way of payment.

Electronic banking means that banking customers are no longer restricted to the 'brick and wall' of the traditional bank as customers can access banking services at any time of the day and from anywhere in the world using various electronic banking services such as ATMs, internet and mobile banking. However, this also presents a challenge to many organisations, people and societies that use or interface with technology for the conduct of financial transactions.

E-fraud is not an emerging financial crime; the problem is global and cuts across various sectors of the world economy as billions of dollars are lost to organised and opportunistic crimes. Its impact is not only financial, it also affects the brand and reputation of an organisation, impede its market share, which eventually affects the growth of the economy and affects lives and livelihood of citizens.

It is commonly believed that e-fraud is prevalent in the financial services industry as criminals would typically follow the money; hence the need for deposit money banks to have robust systems and processes to address the challenge. The Central Bank of Nigeria (CBN) has also not relented in its efforts at churning out their various policies and mandates to serve as guidelines for deposit money banks to help improve the risk management practices in the financial system.

In Nigeria, available statistics show that the problem of e-fraud is not any less serious than what obtains in the rest of the world. According to the Nigeria Inter-Bank Settlement System (NIBSS) 2014 report on fraud, the Nigerian financial system lost over N6.2billion to fraud in 2014 when compared with previous year loss figure of N485million in 2013. Most of the fraud loss was attributable to e-fraud. The sheer size of the 2014 fraud loss and the trend it shows ought to give every well meaning participant in the Nigerian financial system a serious cause for concern.

The outlook of e-fraud in the Nigerian financial system is expected to continue in the direction that the NIBSS 2014 fraud report presents. This is so because, e-fraud is closely indexed to electronic payment which is fast growing at an unimaginable leap and bound, fuelled by various innovations in payment technology, Government and CBN initiatives such as Nigeria's policy on cashless economy and the implementation of its Financial System

Strategy (FSS 2020) on one hand, and an emerging technology savvy generation of young people on the other.

All of the above influences mean that electronic payment will continue to play a major role in the Nigerian financial system and deposit money banks must continue to wage the war against e-fraud differently from the old way they have fought the war against traditional fraud in banking. There needs to be a change in orientation and evolve a new and creative way to combat the problem.

A good starting point in the fight therefore must begin from the top. Management must re-assess its thought about fraud, set the right tone and accord fraud risk management the right attention.
Today, most organisations do not have a robust fraud risk management system in place and most view fraud risk management as a cost centre and a barrier to business. They place less importance to invest in fraud risk management capabilities due to increasing competition and declining revenue margins while searching for new, innovative and cost effective ways of delivering banking products and services to customers who are increasingly demanding better banking services at little or no cost.

Winning the battle against e-fraud also means that the organisation must set its fraud risk-return appetite and map out its strategy to keep fraud losses within set threshold. To achieve this, the organisation must employ multi-dimensional and smart approach to stay ahead of fraudsters at all times and not just respond to fraud incidents when they happen.

Fraud risk management is seldom given the serious attention it deserves until a major incident occurs, and when this occurs, response is usually reactive and handled in a haphazard manner focused on apportioning blame, and not the problem.

Organisations should put their fraud experience to use in improving their systems, policy and processes to prevent recurrence as lessons learnt. This should be documented, shared or internalised.
The fight against e-fraud cannot be won in isolation. Within the organisation, everyone must buy into the crusade and participate actively in combating the threat of fraud. The war would not be won if fraud is treated as the responsibility of a particular function.

The fraud risk management effort should be co-ordinated by the fraud risk manager or a designated authority with the requisite knowledge and skills who must work with relevant stakeholders to assess products, processes and the systems and channels used for product delivery for fraud risk, first at the point of introduction, when changes are introduced and periodically to ensure that they are not vulnerable to fraud. This pre-supposes that the fraud risk manager must constantly upgrade and sharpen his skills to understand the

various functions that impact on fraud risk, remain sensitive to changes in the fraud environment, and be able to make a case to senior management for the needed investment to fight fraud effectively. He/she also must collaborate with other players in the industry in search of fraud intelligence and to present a common front against fraudsters.

In fighting fraud, the focus should be more on prevention. Any opportunities for fraud identified in the course of fraud risk assessment or fraud investigation must be mitigated against using appropriate process or system controls. Electronic products should be developed with risk mitigations in mind using technology with in-built protection mechanisms.

Access to banking service via remote channels must be subjected to strong and preferably dynamic authentication procedure. The system must be protected against possible intrusion and unauthorized access from both internal and external parties. Any fraud attempts experienced must be thoroughly investigated, documented and lessons learnt, built into the system to prevent recurrence.

Customers should be well educated about the product and given safety tips to reduce vulnerability to fraud. Customers must also be engaged on a continuous basis to keep them abreast of fraud threats and preventive measures.

However strong an organisation fraud defence system might be, fraud is inevitable to business operations. Nonetheless, the organisation must have systems and processes in place to detect fraud incidents promptly when they do occur. Fraud detection could be system based using rule or neural fraud tools. Maker-Checker, callbacks, account reconciliation, speak-up/whistle blowing, and a host of other processes to serve as veritable detection mechanisms and must be encouraged and promoted. Fraud thrives where the likelihood of detection is low. Conversely, fraud detection reduces the likelihood of fraud.

When fraud occurs, the organisation must seek to understand what went wrong. The primary focus of investigation therefore, should be to understand the root cause of the incident and to prevent a recurrence. Often, when fraud occurs, the general expectation is to see the fraudster arrested at all cost while the root cause is left unattended. While it is good to bring e-fraud, like every other crime to justice, this must not been done at the expense of leaving the financial asset of the organisation to further risk.

The fraud risk manager must put a framework in place for reporting and responding to fraud incidents. The speed of response to fraud incident is very critical to containing fraud loss. Anyone discovering a fraud should be able to contact the bank at any time to report the incident so that the bank can take immediate action to stop the fraud. The bank must explore

every window of opportunity open to it, to recover fraud loss provided the associated benefit will exceed the cost of recovery.

In summary, a good fraud management strategy must incorporate Prevention, Detection, Investigation, Recovery and Deterrence.

Standard Chartered has long recognised the risk posed by fraud and has since put in place structures, systems and policies to ensure that fraud risk is managed intelligently to keep fraud losses at a tolerable level in the organisation

The role of Audit Trail and Logs Management in systems security, fraud detection and prevention

By Olokor Raymond
(Security Operation Centre, IT Risk Group, UBA)

1.0 Introduction/Definition

Fraudulent activities detection and prevention is among the topmost challenges facing financial institutions across the globe including Nigerian banks and other members of the Nigeria Electronic Fraud Forum (NeFF). The Association of Certified Fraud Examiners estimates that 5% of organizational revenues are lost to fraud as more than $3.5 trillion are annually defrauded on a global basis. Among recent reported cases include J.P. Morgan Chase Bank and Targets Retail Stores where about 76 million and 40 million credit cards details were stolen respectively by hackers. This resulted in huge financial loss, litigation and reputational damage to both organizations.

Many organizations are blind or not aware of the series of malicious and fraudulent activities occurring daily in their information systems due to non-existing audit logs or lack of end-to-end review of captured audit trails. Hence, this article seeks to discuss the relevance of audit logs in computer security, fraud detection and prevention.

What is an Audit trail?

Audit trail is a set of security events that documents the sequence of activities affecting an operation. It is largely a detective control that can be used to identify fraudulent activities, discourage and prevent its reoccurrence.

What is Audit log Management?

Audit log management refers to the process for generating, transmitting, storing, analyzing and disposing of computer security log data. It is difficult to manage the high volume of logs generated across computer systems in an organization manually. The use of Security Information Event Management (SIEM) tools is recommended for audit logs management and processing.

2.0 Systems Security Position of Most Organizations.

The lack of audit trails and effective logs management in most organizations have resulted to the following security gaps;

1) Some organizations keep audit trails in silos and have no functional SIEM solution to centrally support daily security monitoring, events review and investigation.
2) Most organizations are not aware of attacks targeting their key assets as they are blind to such attack locations, sources and may occur for months undetected.

3) Sensitive data of some organizations including systems passwords are accessed by unauthorized users without the platform custodians' knowledge.
4) Most organizations do not have full visibility to configuration changes on the network, user activities and access (internally and externally).
5) In some organizations, audit trail are not completely enabled for performance reasons and most systems related investigation cannot be completed.
6) Series of malwares including key loggers, backdoors and Remote Access Trojan (RAT) exist in most organizations network without administrator knowing.
7) Audit trails are disabled by hackers to conceal attacks and evade detection.

3.0 Importance of Audit Trail and Logs Management:

Among the key benefits of audit trail and logs management are;

1. Improved Security and Visibility – It gives end to end view of organization's security posture per time, based on reviewed audit logs of events across platforms.
2. Fraudulent Activities Detection and Prevention – Audit logs can reveal fraudulent activities including hacking attempts and unauthorized access that is used to fine tune security controls and prevent subsequent attacks.
3. Financial Loss and Reputational Damage Prevention – Audit logs review helps to identify malicious activities that can cause financial loss, litigation and unquantifiable reputational damage, among others.
4. Risk Management Capability Demonstration – Audit logs management helps to show organization's proactive risk management ability and gives required assurance to key partners including customers, regulators and auditors.
5. Compliance and Certification Fulfillment – Required audit logs are used as proof of regulatory compliance during systems security audit and can help a company to easily fulfill various security certifications including PCI-DSS and ISO27001.
6. User Accountability and Non-repudiation Enforcement – Audit trail tracks each user activities to prevent against denial or non-repudiation of such actions.
7. Helps in Forensic Investigation – Audit log provides evidence to support forensic investigation when prosecuting a case.
8. Identification of rogue software - Antimalware logs are used to detect malware activities including malware blocked and infected systems.
9. Systems Troubleshooting, Error Detection & System Improvement – Audit log report helps to identify key errors for correction and improvement.

4.0 Key problems of Audit Logs Management

Some of the challenges of audit logs management in organizations include:

1. Lack of required audit logs management infrastructure due to low budget and management support for information systems security.
2. Inability to effectively scope, identify and prioritize areas of systems security risk in alignment with the organization's risk appetite and emerging threats.

3. Difficulty in seamlessly integrating series of silo audit log sources with different reporting formats into a central log management system.
4. Inadequate storage resources to warehouse and retain high volume of systems logs from various platforms across the enterprise within the stipulated retention period.
5. Inconsistent log contents with different time stamps across different systems
6. Difficulty of preserving the integrity of logs and protecting them against tampering.
7. The challenge of ensuring that the availability of required audit logs at all times.
8. Challenge of manually managing, reading and administering the various logs.
9. Shortage of experienced manpower and inability to technically interprete, analyze, correlate and generate required management reports from available audit logs.

5.0 Recommendations for Effective Audit Logs Management

The following are recommended to reap the benefits of audit trail and log management for systems security, fraud prevention and detection;

1. Management of organizations should prioritize and invest in systems security by providing required security tools including audit logs management infrastructure.
2. Organization should have a robust security policy covering audit trail and logs management plan to cater for the organization's areas of identified risks.
3. All stakeholders should work together to ensure that audit trails are enabled in all critical systems - network devices, database, operating systems and applications.
4. All systems should be synchronized with a central time (NTP) server to ensure consistency of time stamp across platforms for reliable events correlation.
5. Audit trails should be comprehensive, including time stamp, source address, destination, event id or activity description among others.
6. Audit trails should be written to write-once device or written to a dedicated logging servers running on separate machine from the hosts generating the event logs.
7. A robust central Security Information Event Management (SIEM) solution should be implemented to ease audit log collection, correlation, analysis and reporting. Access to the SIEM should be monitored and read-only granted to all investigators.
8. Adequate storage space should be provisioned to warehouse, store and retain audit logs for the retention period stated in the organization's policy.
9. Audit logs should be backed up and tested periodically to ensure that required events are completely logged and available when required.
10. Subject to the audit log retention and destruction policy, audit logs should be destroyed in a fashion commensurate with the security classification of the data.
11. A team of trained security personnel should daily review, monitor audit logs and generate incident reports for instant response and security controls fine tuning.
12. Security Operation Centre (SOC) equipped with various security tools including functional SIEM solution should be established to quicken incident response.

6.0 Conclusion

Information systems security attacks and related frauds are becoming disrupting and more damaging daily, and frequently forming major Newspapers headlines across the globe. Like

most organizations, despite the huge investment in security by J.P Morgan Chase Bank, the attack of June, 2014 was not noticed until 3 months after. Also, the security alert flagged by the security tool of Target Retail Store during the attack (Dec, 2013) was ignored resulting to huge financial loss, litigation and reputational damage.

In line with best practice recommendations in this Article; audit trails should be enabled for all critical platforms and integrated to a central SIEM solution. The logs from all systems should be monitored and reviewed daily to protect the organization.

Tackling e-Fraud across online channels

These are interesting times. Legend has it that one of the biggest bank robbers known to the world as Willie Suton (1901 – 1980) was asked why he robs banks, and his reply was, 'that's where the money is'.

Willie Sutton did well at his profession: He was a daring and resourceful robber who used disguises and trickery to achieve his ends, including dressing as a policeman, window washer, maintenance man, bank guard, mover, Western Union messenger, and striped-pants diplomat. Over the course of his career, he made off with an estimated $2 million in ill-gotten gains.(FBI Files 2015)

As celebrated as Suton was during his time, robbing a bank then was a big challenge and involved huge investments in criminal tools like guns, ammunitions, equipments to study the bank security systems, change of guard sessions, location and security of vault etc.

Today with electronic channels, the investment needed to rob a bank is very low. Robbers need not even live in the country of where their target bank is located.

Willie Suton (wherever he is now) will probably be envying the present day e-bank robbers.

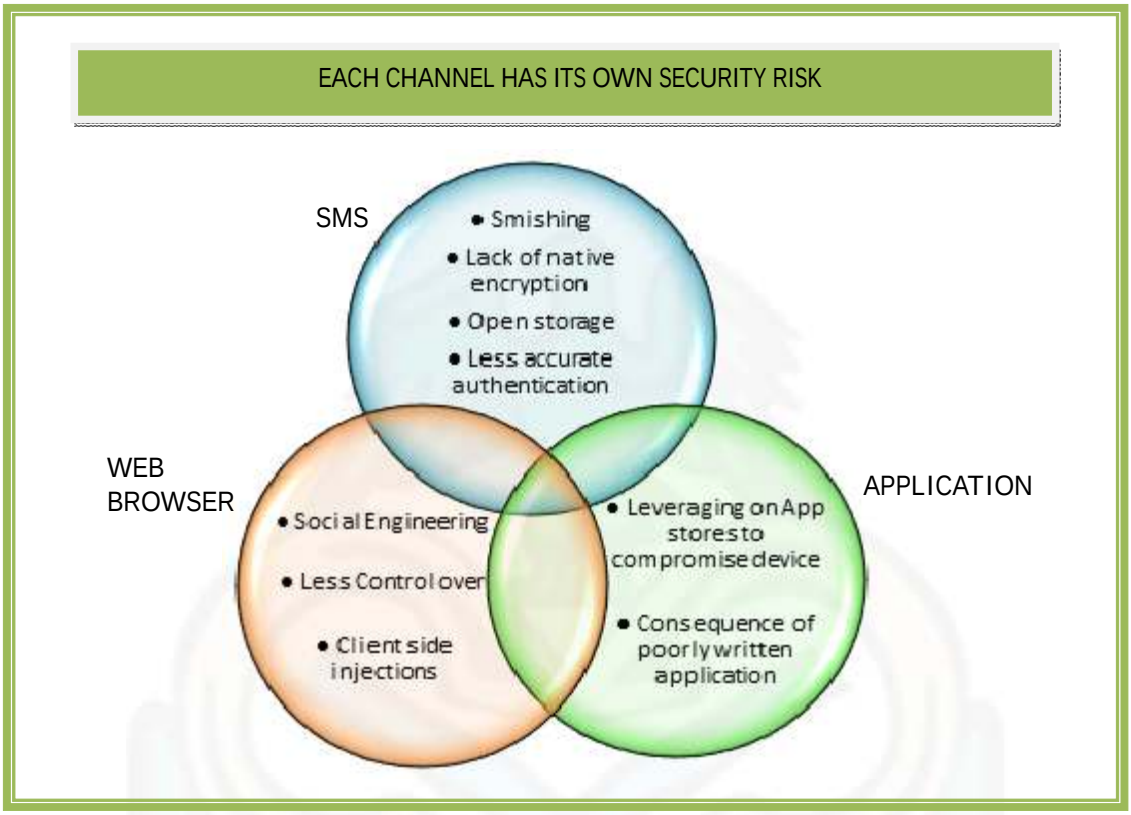
As the global community embraces and adopts the increasing varieties of banking channels and electronic payment options, the rise in cases of electronic fraud has necessitated the need to evaluate the vulnerabilities of the e-channels stakeholders.

Identifying the attendant risk of the e-banking platforms and deployment of technical infrastructure to combat the menace will ultimately boost the customers' trust, whilst offering safer banking environment. This piece sheds more light on the present e-fraud trends and highlights some strategies that should be adopted to prevent occurrence of e-fraud in the future.

Electronic Banking is an all encompassing term as it includes online banking, mobile banking and other e-channels. It may be revolutionizing the banking business, but it comes with tremendous risks on transactions and resource security.

Transactions that were manually processed in the past are now electronically done remotely and in real time. While this development of e-banking has brought with it, new products and ways of doing business, it has also spurned a wide variety of fraud and channels of perpetrating them. More often than not, the channels used in perpetrating this fraud are over the network, internet or electronic card products - hence the term e-fraud.

As banking processes become more dependent on networking technology, financial institutions are now the prime targets of electronic fraud.



This illustration above highlights the different kind of threats that is associated with the various channels

Some of the various channels/ devices used by fraudsters to perpetrate this electronic fraud are:

1. ATM/Card-Related Fraud
   - Skimming (Counterfeit Card Fraud): It is a replication of electronic data to allow valid authorization to occur.
   - Lost/Stolen Card Fraud: When a stolen or lost card is fraudulently used by unauthorized cardholder
   - Interception Issue: Occurs when card is stolen from mail system or in-transit.

2. ATM Video Fraud: A tiny video attached to ATM by fraudsters to capture and transmit digital information including PAN and PIN

3. Scam Mails: Scam mails are of two categories:
   - Phishing: Mails sent by fraudsters to customers asking them to confirm some online banking details. With the details provided, customer's card could be cloned and used in defrauding them.
   - Pharming: A malicious code is often placed on the bank's user domain name system which then directs traffic to fraudulent website.
   - Smishing: SMS phishing uses cell phone text messages to deliver the bait to induce people to divulge their personal information. The hook (the method used

to actually capture people's information) in the text message may be a website URL, but it has become more common to see a telephone number that connects to an automated voice response system.

4. Malware: is a category of malicious code that includes viruses, worms, and Trojan horses.
5. Spyware: Secret code hidden in an otherwise harmless programme. It permits unauthorized access to a computer.
6. Social Networking Sites – Criminals invest time and money on Social Networking sites with the objective of obtaining user names and passwords to bank sites from unsuspecting bank customers. Taking advantage of lack of information for bank customers they visit these sites and use one trick or the other to get the customers to provide them with their access details while pretending to be their friends.

Malware tops the current fraud trend in the online space. Phishing has also evolved over time as it not only looks to steal customer's credentials but also infect their machine with malware. In terms of card fraud, Lost and stolen cards, skimming is used to perpetrate Card Not Present (CNP) transactions through online purchases. Mobile devices are also prone to more severe threats than personal computers partially because they lack security measure that are more common on personal computers such as antimalware software, personal firewalls and built-in-web browser security tools.

Nigeria financial institutions are putting in place various measures to combat the above electronic fraud. Unity Bank Plc has put in place measures to prevent her customers from being a victim of e-fraud. The potential risks involve in key areas of electronic channels has been identified and state of the art solutions have been incorporated thereby bringing e-fraud cases to low levels in the bank. For online card transactions, a one-time password (OTP) is generated and sent to customer's registered phone number. The OTP is a second level authentication measure which is inputted to authorize the online payment transaction initiated. This has helped greatly to tackle the Card Not Present (CNP) fraud challenges. Monitoring tools have been put in place to monitor every transaction and send alerts when an irregular form of transaction is carried out.

Also, in compliance with the recent CBN rule, every transaction in a non-EMV country has to be pre-authorized by the customer. All these measures are to complement the bank's culture of strictly adhering to the PCI-DSS (Payment Card Industry Data Security Standard) policies.

Education of customers on fraud prevention tips is another key measure Unity bank uses to prevent fraud. A monthly communication is sent to customers highlighting the below card security tips.

- Use latest browsers
- Always look out for strange objects on ATM machines before using it.
- Choose a PIN that is different from your birth date, address or telephone numbers

- Make sure you use your card details on trusted website
- Always know where your card is
- Never respond to mails requesting for your online banking details.
- Do not reply to junk email giving you an option to click on a link to be removed from the mailing list
- Do not give out any personal information via email
- Don't fall for making-money schemes. The old phrase, "if it sounds too good to be true, it probably is“
- Don't give out your card to anyone online, unless you know who you are giving it to, and have verified that they are who they report themselves to be.
- Don't just accept just anything on social networking sites if you are not sure of its source
- You get a wall post from a friend you never interact with asking you to click on a link- don't
- You get a wall post from a friend, prompting you to watch a You Tube video that you're supposedly tagged in – look before you leap
- Don't join any group on social networking sites unless you understand what they are about
- Avoid giving untrustworthy games and apps authorization to your phone
- Don't let people you don't know see your profile. Use those privacy settings and block anyone you're not friends with.
- Don't update your status every ten minutes and do not over share
- Don't sign up for Facebook games or applications without checking to see if they might have viruses.
- Do a Google search or read reviews on the game or application to see if it has malware.

Unity Bank recommends that financial institutions use the following measures to tackle e-fraud in organization:

- Real time fraud processing and tracking of transactional data
  Enhanced customer education on risks, threats and preventive measures
- Have an enforceable IT Security Policy. Implement and enforce an acceptable usage policy covering the use of social networking sites.
- Permit access only to social networking sites that have obvious business benefits. Access only to users with a business need to access them.
- Train your Control staff to become Social Media Security Certified Professionals
- Contingency Plan – Take prompt action if confidentiality is compromised
- Reviewing value/frequency threshold
- Out of band transaction verification

To this end, combating fraud in electronic banking is a never ending story due to new technology innovations in the financial sector. Industry leaders need to think about feedback reporting and measurements as part of a cross-channel anti-fraud strategy. Such reporting and metrics are part of a financial institution responsibility to reduce fraud in order to improve return on investment (ROI) and more importantly, to maintain customers' trust.

References

Willie-Sutton,'Where the money is', http://www.fbi.gov/about-us/history/famous-cases/willie-sutton accessed 08/04/2015

Protective Steps by Zenith Bank in fighting fraud against e-Payment System

In the past one decade or so, methods of effecting banking and other financial transactions in Nigeria have become a lot more sophisticated. Transactions which were hitherto consummated in the banking hall are now being carried out via various electronic channels (e-channels) that offer convenience and safety. However, these payments and payment methods are often targets of fraud. Fraudsters use a variety of techniques to tamper with an organization's security controls in order to obtain funds. Thus, securing these e-payment systems is not only critical to e-business, but also a daunting challenge globally. Protecting against payments fraud is often a cat-and-mouse game, especially as technology continues its rapid evolution.

In the 'electronic environment' fraud occurs in a variety of forms, such as phishing, skimming, shouldering and theft, cash trapping, etc. Many parties are involved in fraud prevention: banks, transaction processors, Point-Of-Sale (POS) terminal suppliers, brand owners, as well as business owners and consumers. It is the duty of the police and the law to track down criminals and fraudsters. But as a bank, Zenith bank has continued to embark on security measures including investing significantly to ensure the safety of its electronic payment transactions. Examples of such security enhancing measures that have been undertaken include the migration to secure chip-based payment cards to address card counterfeiting fraud, the introduction of a second factor authentication to strengthen authorization of online banking transactions and the implementation of SMS alert to mitigate card fraud.

Overview of New Electronic Payment Systems

Before discussing the protective steps towards securing e-payment systems, it is pertinent to briefly describe the e-payment systems themselves. Essentially, transactions are consummated using various channels like the Internet, Automated Teller Machines (ATMs), Point of Sales (PoS) terminals and the mobile phones. The Internet is a global network connecting millions of computers. According to Internet Live Stats, as at December 30, 2014, there were an estimated 3,037,608,300 Internet users worldwide. ATM is computerized machine that permits bank customers to gain access to their accounts with a magnetically encoded plastic card and a code number. It enables the customers to perform several banking operations without the help of a teller, such as to withdraw cash, make deposits, pay bills, obtain bank statements, effect cash transfers. Point of Sale, or POS as it is more commonly abbreviated, refers to the capturing of data and customer payment information at a physical location when goods or services are bought and sold. The POS transaction is captured using a variety of devices which include computers, cash registers, optical and bar code scanners, magnetic card readers, or any combination of these devices. A mobile phone is a wireless handheld device that allows users to make calls and send text messages, among other features.

Protective Control and Security Measures

The risks of electronic payments fraud are real and multiplying every day. As Zenith Bank customers rapidly move up the value chain of e-Payments, the fraudsters also follow them. Criminals today coordinate fraud schemes across all transaction channels. The wide range of access points for financial information -- including smartphones, tablets, office, and home computers - gives fraudsters an array of options to plan and execute their attack. To keep up with this rapidly growing threat, the bank continues to study the market and see where it needs to change procedures and where it needs to apply any technology, depending on how it sees the security situation relating to e-payment. To that effect, Zenith bank has adopted strategic approach to electronic payments fraud prevention as follows:

- Two-factor authentication: Two-factor authentication is a security process in which the user provides two means of identification from separate categories of credentials; one is typically a physical token and the other is typically something memorized, such as a security code or pin.

- Deployment of anti-fraud monitoring solution: The bank has also deployed various anti-fraud monitoring solutions that identify transactional behavioural pattern, geographical and device profiling. This is aimed at detecting unusual transaction pattern.

- Customer Education: The bank has embarked on consumer awareness and education in order to reduce Identity theft or payment data theft. This would help the user in adopting active and cautious attitude when doing transaction using various e-payment channels. It could teach them to be aware of possible risks, avoid e-scams, and minimize giving information to merchants when buying online. This would increase consumers' responsibility in keeping personal data secured in physical and virtual world.

- Anti-skimming technology on payment channel: The bank has also deployed anti-skimming technology on all its Automated Teller Machine (ATM) terminals to prevent the installation of skimming devices by fraudsters. Skimming is a technique used by criminals to copy personal data from the magnetic strip on an ATM card. The deployment of this anti-skimming technology ensures fraudsters do not have access to customers' card details using skimming devices.

- Regular penetration & vulnerability Testing: Having taken deliberate steps to secure its e-payment ecosystem, Zenith bank conducts regular penetration and vulnerability test. The tests attempt to exploit the vulnerabilities in a system to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat to the application.

- Source code review and testing: To prevent attack from malicious sources, Zenith bank uses superior Code review tools to review, find, and eliminate vulnerabilities before an application goes “live” and helps identify flaws in applications. Code review procedures are done in various forms such as pair programming, informal walkthroughs, and formal inspections.

- Deployment of web application firewall: Zenith bank has deployed web application firewall to protect web applications/servers from web-based attacks. It is intended to block web attacks before they can reach vulnerable applications.

- Deployment of anti-malware solution: To combat malicious code on individual computing devices and IT systems, Zenith bank has deployed anti-malware software. It is intended to protect the bank against infections caused by many types of malware including viruses, worms, Trojan horses, rootkits, spyware, keyloggers, ransomware and adware, among others

- Conformation to industry standards: Zenith bank has continued to comply with Industry standards as set by the Central Bank of Nigeria (CBN) such as the Payment Card Industry Data Security Standard (PCIDSS). PCI DSS is set up to provide organisations with a minimum set of prescribed control to proactively protect customer account data and prevent its disclosure to malicious third parties.

- Ensuring end to end encryption: Sensitive data that travel over a Zenith bank's network are securely encrypted from the point of data entry to the point where the data is processed. Sensitive data may be user name, password, credit card number, etc.

- Restriction of access to systems: Zenith bank has taken measures to minimize internal tampering with the computer system. The bank has taken precautionary measures which include monitoring the use of computers and network by users. The physical access to computer is limited by use of passwords and magnetic card reader to verify the identity of the user.

In conclusion, with the ever evolving e-payment channels, detecting fraud in real-time is not easy. However, Zenith bank's fraud prevention and management systems strive to reduce fraud significantly by using and combining many existing techniques, as well as new ones. The bank continues to use industry standard security rules, solutions to provide advanced protection from all types of online and offline transaction fraud in electronic payment systems. Zenith bank strives to stay ahead of these increasingly sophisticated criminals by implementing integrated real-time fraud detection and prevention system with data analytics capabilities well positioned to repel malicious attacks.

Cybercrime: A Risk Information Centre to the rescue

By Onajite Regha,
(CEO, Electronic Payment Providers Association of Nigeria, E-PPAN)

The Nigerian financial sector has adopted electronic payment channels as a mode to promote retail financial services to the teeming population of banked consumers and previously excluded citizens in the country. Concerted efforts by the financial sector stakeholders in Nigeria have seen the country propelled towards global trends in payment systems development. These developments are to ensure efficiency and effectiveness in the delivery of financial services in the country using the national payment system. “Payment System refers to an integrated system that facilitates the transfer of funds. Such a system would include all the aspects necessary to facilitate a payment within a modern economy, which include the legal and regulatory framework, the processes and rules, the infrastructure (IT, telecommunications, devices, etc.), the banking systems, clearing and settlement systems, security and risk management procedures and processes, and so on.” (Walter V. Volker, 2013)

As in every clime, the National Payment Systems (NPS) are regulated by legislation. In Nigeria, the Central Bank of Nigeria is charged with the responsibility of administering the Banks and Other Financial Institutions (BOFI) Act (1991) as amended, with the sole aim of ensuring high standards of banking practice and financial stability through its surveillance activities, as well as the promotion of an efficient payment system. In line with its mandate, the Central Bank over the years, has effectively promoted the efficiency of the NPS and in April 20th, 2011, the CBN introduced the Industry Policy on Retail Cash Collection and Lodgement (IITP/C/001) otherwise known as the Cashless Policy. One of the intent of the policy is to facilitate the growth of electronic payments and increase availability, reliability and security of electronic channels. We can categorically say that the intent of increasing availability of the channels is being met very fast.

A recent presentation by the Deputy Governor Operations of the CBN, Alhaji Suleiman Barau, shows that the new cashless policy of the CBN has driven adoption of PoS by 550 percent to N312billion in 2014 from N48 billion in 2012. While web transactions increased by 108 percent, mobile money witnessed an increase of 8,400 percent between 2012 and 2014 amongst growth of other related e-payment transactions. The industry today celebrates this progress and financial players are encouraged to improve on their services and increase market share both locally and internationally.

However, as the financial industry celebrates the successes and as cashless transactions gain momentum, the nation is witnessing an upsurge of cybercrimes encouraged by the advancement made by introducing technology into payments. According to Wikipedia,

cybercrime is any crime that involves a computer and a network. Explaining further Norton.com says it is simply a crime that has some kind of computer or cyber aspect to it. To go into more detail is not as straightforward, as it takes shape in a variety of different formats. Webopedia gives examples to include: hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cybercrimes when the illegal activities are committed through the use of a computer and the Internet. The Interpol website (http://www.interpol.int) also states that cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual.

Therefore, I dare to add that addressing cybercrime is a growing urgency.

Cybercriminals are stepping up their attacks on financial institutions by gaining control of customer devices with highly advanced man-in-the-browser malware and spear-phishing attacks. They then conduct real-time credential theft and take over accounts. In a recent real-time account takeover scheme, cybercriminals used malware to steal user credentials at login and block users from logging in to online banking, after which the criminals used the stolen credentials in real time to log in to victims' accounts and pass back any secondary authentication requests to users in order to bypass the bank's security and gain full access to accounts. Compared to any other time in its history, the payment card industry faces an increasing variety of security challenges as the transaction environment grows in size and complexity.

It is important to note that the rising trend of electronic fraud is not peculiar to Nigeria; rather, it is a global phenomenon but we are witnessing a geometric growth of fraud as the country adopts more of electronic channels for payment. According to a MasterCard publication on Global fraud Management Overview (2011), “On a global level, fraud continues to migrate from more secure to less secure regions and channels”. This obvious shift is accelerated by an increasingly adept and organized criminal community that seeks to exploit security vulnerabilities and commit fraud. Criminals are targeting not just unmonitored, stand-alone, point-of-interaction devices, but also launching sophisticated attacks on the private networks of well-known entities, such as major data processors and top-tier merchants. All of these factors can lead to fraud attacks that can cause erosion in confidence and global acceptance as financial institutions seeking to avoid risk may move to block transactions at a country or regional level. “

The stakeholders in Nigeria landscape have not rested in their oars. Just as the industry has used collective actions to grow the proliferation of the electronic payment channels and users under the leadership of the CBN, they have also recognized the need to use the same strategy to confront electronic crimes. This has helped to reduce the amount of crime we currently find in the industry. For an example, the introduction of the chip and pin into the Nigerian card space

found the crime type associated with magnectic stripe card reduce by 99%. Other cybercrime types have led the banking industry to implement several policies and practices to reduce the intensity of cyber criminals' attacks.

Notable among them are:

- Working committees comprising of heads of department of Nigerian banks responsible for internal controls, risks, and compliance functions etc were established. Some of the notable ones include the Committee of Chief Internal Auditors of Banks; ; The Committee of e-Banking Industry Head (CeBIH); Committee of Chief Inspectors of Banks in Nigeria etc.
- The industry created the Nigeria Electronic Fraud Forum (NEFF) which is chaired by the Director, Banking and Payment Systems Department of CBN. Its membership comprises of all significant players in the value chain of electronic payments in Nigeria. This forum meets very regularly and acts as a nodal point for dissemination of information and knowledge sharing in the industry. The forum has also continued to explore options at improving strategies for tackling fraud in the Nigerian payments landscape.
- The on-going implementation of an industry-wide anti-fraud management system.
- The annual e-payment fraud conference hosted by Electronic Payment Provider Association of Nigeria (E-PPAN), which gives the industry an opportunity to review progress and recommend ways forward for talking fraud in the region on an annual basis.

While all these initiatives contribute in some way to address the emerging menace of fraud in the industry, it has widely been noted that none of them addresses the pressing need to have a body/institution that dedicates 100% of its time to combating fraud. This is a wide gap in the industry ecosystem especially when we recognize that the small groups of sophisticated criminals perpetuating these frauds have no other business than crime and give crime a 100% of their time. Therefore, to achieve tangible result in combating crime, the industry must unanimously empower a single specialized entity to serve as a nodal point for tackling all types of bank frauds.

Of note is that these criminals are always one step ahead in the game. A lot of time the providers and security agencies play a catch-up to the ever-changing antics of these criminals. In this case what is required therefore is for the industry to change its strategy in combating the cybercriminals. In a paper presented by Justice Atilade, the Chief Judge of Lagos State at the Annual E-Fraud Conference 2014, the Chief Judge noted that "what must change are the tools and resources deployed to tackling e-crimes."

For a while now E-PPAN has advocated for a Banking Risk Information Centre as a channel to fight fraud. Based on this the Association in 2013 has signed a partnership with SABRIC (a model Centre) to work with it in achieving this dream in Nigeria. The partnership with SABRIC will facilitate the Nigerian Banking Industry to set up an institution that will fight crime on behalf of the collective whole of the banking and related industry in Nigeria. To strengthen this

relationship between South Africa and Nigeria, the Central Bank of Nigeria led the banking industry with attendance from the law enforcement agencies for a study tour to South Africa with the mission to create new strategies for combating electronic payment fraud in Nigeria. During this visit the Nigerian community met with the management of SABRIC led by its Managing Director, Ms. Kalyani and also with the following: the Managing Director of Payment Association of South Africa (PASA); The Managing Director of Banking Association of South Africa; and The provisional commissioner of Crime Investigation in the South African Police.

SABRIC interface with a range of external organisations and public and private partners, most notably to progress crime risk reduction activities. Its key stakeholders are the major banks. Its principle business is to detect, prevent and reduce organised crime in the banking industry through effective public private partnerships. The company provides crime risk information and consequence management to the banking industry and CIT companies. One of SABRIC's key responsibilities is co-ordination of activities to address organised bank related crime, i.e. violent and commercial crime. They provide a range of services to their clients including representation and lobbying, project management support, research and developing industry best practices for crime reduction.

Lessons from South Africa corroborate the principle of collaboration for fighting crime. The South African Police, the payment association, and the banking association all correlated their success of checkmating bank related crime to the strategy of the risk information centre.

A proposed risk information centre for Nigeria will therefore act in the interest of the entire industry in the following capacity:

- Maintain a comprehensive banking fraud database
- Serve as nodal point for information analysis and dissemination on bank fraud
- Provide relevant support to law enforcement agencies
- Drive industry awareness programs for the general public
- Drive institutional local and international collaborations to fight fraud
- Support the banking industry in designing and implementing collaborative programs to fight fraud
- Contribute to making the Nigerian banking sector safer and instil customer confidence

The beauty of a central banking risk information centre is that individual companies and institutions can preserve their original mandates as it relates to crime fighting. The Nigerian Banking Risk Information Centre will only support the existing processes without necessarily duplicating any functions or upsetting the existing ecosystem in the criminal justice process. Going the route of a common risk information centre will reduce the cost of fighting cyber criminals in terms of finances and resources. It will provide a holistic view by which every individual organisation can appraise their positions. The immediate alert system will also help to reduce the occurrence of same crime types in different organizations.

The risk information centre will lead to faster arrests and quicker resolutions of criminal matters. The centre will take up a central approach in assisting the law enforcement agencies and the judiciary as well. Onyekachi Ubani Esq. (former Chairman, NBA, Ikeja) opines in his paper delivered at the E-Fraud Forum 2013 that "Authenticating electronic evidence is an exercise of the court's judgment and it involves a delicate act of balancing the risks of acceptance against its benefits. The principles are not so clear cut because this is a period of gestation. The bottom line in the issue of authentication however is that the court must be satisfied that the evidence adduced is sufficient to lay the foundation as enshrined in section 84 of the Evidence Act." The industry therefore needs an expert witness that can guide the judge to understand the enormity of the crime. One other advantage that comes with this approach is the effective public private partnerships which allows the centre to sign agreements with all stakeholders and reduce the amount of time needed to get subpoena or bureaucratic processes that usually delays investigations.

One must also remember that cybercrime does not stop at borders. As pointed out in the 2009 European Commission report Protecting Europe from Large-Scale Attacks and Disruptions: Enhancing Preparedness, Security, and Resilience. The majority of cyber threats demand swift collaborative international action, as adversaries and cyber criminals will not wait until multiple national authorities finally agree to act. Having a non-profit/non-government centre could be a quick reference point for international communications. According to the CEO of Kaspersky "Cyber weapons have the power to disable companies, cripple governments, and bring whole nations to their knees by attacking critical infrastructure in sectors such as communications, finance, transportation and utilities." Bearing this in mind it becomes foolhardy for the nation or the financial industry to continue with fragmented approach to fighting cybercrime. As India's Minister of Communications and IT Kapil Sibal declared on the release of the country's National Cyber Security Policy 2013: "...instability in cyber space means economic instability. No nation can afford economic instability, therefore it is essential not just to have a policy but to operationalise it."

Let me conclude by saying that it will be imprudent to expect that crime can be completely eradicated as this is a major means of survival for a peculiar kind of people. The best we can have is a united front against cybercrime. On a lighter note, I will borrow a leaf from the movie Power Rangers, a long-running American entertainment children's television series featuring teams of costumed heroes. These powerful superheroes are able to utilize special powers and pilot immense assault machines, called Zords, to overcome periodic antagonist. When enemies grow to incredible size (as nearly all do), Rangers utilize individual Zords that combine into a larger Megazord. This entity looses any individual identity and with one voice and coordinated effort the enemy is made to bow to a superior force. In relations to our industry, every individual organisation has invested and will continue to invest in people, technology and processes to exorcize crime, but with far less the amount spent individually, a collective effort will result in greater impact.

References

1. Volker W. V. (2013) – Essential Guide to Payments
2. http://www.hallmarknews.com/nigeria-recorded-impressive-growth-electronic-payment-system-emefiele/
3. http://www.webopedia.com
4. www.interpol.int/Crime-areas/Cybercrime/Cybercrime
5. www.norton.com
6. Building the case against the electronic criminal: what to look out for, Paper presented by Ubani C, Esq at the Annual Payment System and Fraud Conference 2013
7. http://www.ecb.europa.eu/press/pr/date/2014/html/pr140225.en.html
8. Patrick de Graaf (2013) SMART international collaboration needed to fight cyber crime: http://www.theinformationdaily.com/2013/10/11/smart-international-collaboration-needed-to-fight-cyber-crime
9. http://www.itpro.co.uk/unified-threat-management/19711/kaspersky-ceo-leads-calls-greater-collaboration-fight-against-cyber#ixzz3TVgsHjvk
10. http://en.wikipedia.org
11. Legal Challenges and Solutions in Fighting Electronic Fraud, Paper presented by Justice Funmilayo Atilade, Chief Judge of Lagos State at the Annual Payment System and Fraud Conference 2014

Security is a Service

By Michael Nuciforo
(Mobile Consultant, Innovator and Futurist)

Ever since the concept of banking was first developed hundreds of year ago, the very foundations of the banking industry have been focused on two core elements – the concept of money and securing it. If you were to analyse the history of money, from the very first use of coins, to loans and the advent of paper money, the very purpose of the banking industry was to provide a mechanism for accessing and securely storing money. When you think of banking in this context, it's quite ironic that in modern times, security has become almost of secondary importance for bankers and their customers. Whilst customers expect their money to be secure, they are not enthusiastic about it – they prefer a simple user experience over higher security. Due to this, a lot of banks globally have invested heavily in new innovations while reducing expenditure in security. It is important that as the Nigerian banking industry goes through a period of significant change and innovation, a security mind-set should be prioritised more than ever. Nigeria should look at the recent bank hacking attacks in other countries as a strong warning. In a time of global cyber warfare, security should be treated as a service not an afterthought. If the Nigerian Central Bank and its member banks are to get it right, security can be a key factor in Nigeria achieving strong growth, economic stability and prosperity.

With more and more global security threats emerging every day, it is becoming clear that having a secure and robust security platform is going to be a key enabler to achieving strong growth in the Nigerian banking industry. As more citizens become banked and adopt mature financial practices, there is a need to assist and educate these new customers in security best practice. It is a challenge that is not encountered by Nigeria alone. Even in mature banking markets such as the US and Europe, there are challenges. In a recent US study, the primary reason given for not using new forms of digital and mobile banking was security. Four in ten respondents had concerns that prevented them from using these services. This type of consumer sentiment could become a major issue in Nigeria as banks attempt to switch customers from offline banking to online banking. The difficulty lies in trying to educate consumers that online banking is indeed secure and actually more secure than holding money physically.

The key to a successful security strategy is to ensure that the approach and benefits can be easily communicated to a basic customer. There is no point having the most sophisticated security controls in the world if a customer does not understand it, or can not see the benefits of it. It is also important the enhanced security is weighed up against the user experience. There is again, no point in having a strong security system if customers do not want to use. So for Nigerian banks and the Central Bank, there is a need to constantly balance user experience, security and risk against emerging threats. This is very

complicated and requires constant assessment and improvement. It is also important the Nigerian banks consider the effort and timeline in implementing new security technology. Security also closely relates to how quickly a bank can bring new services to market. One of the longest lead times on any project is security approval. With security assessments and penetration testing being on the critical path, the more robust your security platform is, the less time you need to spend debating whether your feature is going to create additional security loop holes.

From a customer perspective, the best security solutions are integrated and consistent with the form factor of the device, and if that means setting up a tailored approach – go for it. It is important that Nigerian banks give their customers the flexibility to customise their security controls to cater for their own personal preferences. This is an increasingly vital part of the security mix. In banking markets such as Asia, customers have full control over their own specific security rules, limits and treatments based on the customer's location, direction or situation. Each customer is different, has their own financial situation to consider, relationships and stakeholders and preferences. Giving customers the flexibility to choose their own security means that you are less likely to annoy some customers. Flexibility also means greater adoption. In Australia, when Commonwealth Bank mandated SMS verification on all payments, there was a big backlash of dissatisfaction from customers. Whilst some customers applauded the move and where happy for the second level of authentication, other customers despised the fact that they had to do something extra. If Commonwealth Bank had taken the approach of allowing customers to have their own choice, then more customers would have been happy.

With new banking technology and security protocols, Nigerian banks have an excellent opportunity to maintain control of their environment from a strong starting position. In Europe especially, some banks have really struggled from migrating from old legacy systems and platforms to the new digital world and have therefore suffered repeated hacking attacks costing tens of millions. Nigerian banks have the opportunity to utilise the latest device, behavioural, location and transaction profiling techniques to protect their ground. Organisations such as 'Trusteer' offer banks advanced Malware and Jailbreak detection API's which can be updated without subsequent client releases. These can be coded into native app builds using standard code libraries. Finally, banks can use firms like Melbourne IT for rapid identification, takedown and analysis of fake apps and websites targeting mobile products and services. The Central Bank of Nigeria also has a clear role to play. The Central Bank can look at best practice and lessons learned from overseas to make better judgement calls about the policies it should implement. The Central Bank can also get ahead of the banks themselves by drafting clear and accessible guidance for bank to ensure safe and secure banking whilst on the move is becoming increasingly important. In many cases the banks themselves want to be told what best practice is.

Ultimately, Nigerian banks and the Central bank must work together. They must not wait and see, they must move and act in harmony. As more and more people start to use mobile and online banking, fraudsters will start to follow. In its '2014 Threat Predictions' report, McAfee forecasts that over the next 18 months, attackers will improve on their skill set, attackers are likely to bypass PCs and go straight after Mobile banking apps. This is not a mere threat. There have been a number of large scale attacks already this year in the space of a few months. The Central Bank must always keep one eye open through effective identification and assessment of the emerging security threat landscape, from both closed and open sources. The Central Bank must not assume that because they have strong policies in place today, that they will be strong in the future. Threats evolve, new threats emerge and new technology brings its own risks again.

The security landscape is constantly moving, as soon as you think you are one step ahead, you are one step behind. The Central Bank and its members need to be ready to act so, they should establish a dedicated Security Working Group that is empowered, funded and resourced to deliver tactical and strategic changes in response to evolving mobile security threats. The last thing you want to do when an issue goes down is be haggling over budgets and resources. By having funding and resources allocated at the start of the year, small changes, minor enhancements and tactical fixes can be deployed rapidly. By bringing a cross-functional working group together of different member banks, each bank can learn from each other and support each other. The protection of banking assets should be a collaborative effort, not a competition. The Central Bank of the USA, Canada and the UK have both established security and payments working groups that have proven to be very successful in bringing together different groups. I would strongly recommend the same happens in Nigeria. A monthly meeting can be chaired where existing policies are evaluated, new policies are debated and new processes and technology are assessed.

Whilst a large amount of accountability does rest with the Central Bank, the Nigerian banking industry itself must work diligently to identify and reduce any security risks. Most bank products, strategy and marketing teams have extensive roadmaps outlining what features they aim to launch over the next few years. Have you ever seen something similar for security? Rarely. Nigerian banks must set a clear online security strategy that links together with the channels product backlog. Adequate investment in security related initiatives should be provided. There should be a priority placed on ensuring the integrity of the banks systems. One of the number one reasons security is not a primary scope candidate is that fraud losses are generally tracked at group level, not at an initiative level. This is also linked to how security initiatives are structured. They are generally managed as group initiatives and benefits are not tracked accurately. By treating security as a service, you can start tracking its impact on hard benefits such as improved customer acquisition and most importantly, a reduction in fraud. If the product manager for your mobile project felt accountable for these benefit areas, then security would automatically get a higher priority.

The Central Bank should also take a leading role in leading trials and assessments of new technology. Biometrics technology such as iris scans, face recognition or finger print scanning has been touted for years. Australian bank, ANZ, recently announced that they are looking to deploy finger print based ATMs. In the UK, we have seen excellent traction in schools with WisePay who are deploying finger print scanning technology that allows children to purchase goods in school canteens around the country. Why are Nigerian banks not doing this yet? Not sure. There has been a significant improvement in biometric security over the last few years, and of any option available, biometrics is likely to be the solution capable of converting the unconverted. These types of technologies should be formally assessed as soon as possible, with trials initiated with any interested member banks.

Mobile Applications present many security challenges, but also opportunities. By augmenting the inbuilt platform controls provided by Android, Blackberry and Apple, and innovatively exploiting native mobile capabilities, we can improve our customers' security and provide a more frictionless user experience. The "3-way trust" that is established during App Enrolment can be used as a transparent second factor of authentication (something the user has). This provides a more frictionless experience for customer logon and payment journeys. Leverage and augment existing platform data protection controls to protect confidential and highly confidential information. Implement authentication controls which leverage existing mechanisms and exploit new opportunities that mobile presents, improving customer experience and advocacy wherever possible. Protect inbound and outbound communications between the application and our server-side components or third party sites or components.

Proactive monitoring of digital storefront for unauthorised applications is a domain that is becoming increasingly important. With this in mind, there is increasing demand for security specialists to review site and application source code and perform custom tests to detect security vulnerabilities. Getting these assessments done by a third-party also adds a layer of protection, as a significant amount of bank fraud is performed internally. The Nigerian Central Bank should set up an independent tasks force that is approved for doing these security reviews. Bi-quarterly reviews should be mandated for all member banks. During the development lifecycle, it is important to set standards with our developers and testers about the appropriate protocol. One step you can take is to publish a set of guidelines and rules to assist developers in building websites and applications that are absent of security vulnerabilities. During the testing phase, static and dynamic automated code review tools can detect security vulnerabilities during the development and testing phases of a project. This, coupled with penetration testing and code obfuscation, should be enough to protect your systems and render the code unreadable to a hacker attempting to understand how it works

Recent advancements in the market, such as Apple's recent launch of Apple Pay and Touch ID also shift the game in terms of security and convenience. As part of Apple's iOS 8 preview, it was announced that the Touch ID fingerprint capability would be opened up to developers to allow apps to use this as a method of user authentication. This technology is very

unique because it scans sub-epidural skin layers in the finger, therefore making it less susceptible to false readings and rejections than optical solutions in the market. By using a multi-faceted skin layer approach, it is harder for a hacker to spoof than optical – it almost makes it impossible. Apple insists they do not store the fingerprint itself, which implies it is stored as a non-reversible encrypted one-way hash for comparison against subsequent scans.

Nigerian banks should also look to agree a formal industry-wide fraud guarantee. In countries such as Australia and the UK, this is very popular. Banks essentially guarantee to refund customers who suffer from legitimate acts of fraud via their online and mobile channels. I firmly believe that Nigerian banks need to start promoting this service. The Central Bank should work with its members to develop a consistent fraud guarantee that is consistently presented across digital channels at all relevant opportunities – especially login. A logo should be created and anytime online or mobile banking is promoted in Nigeria, this 'fraud guarantee' logo should be used. By having an industry wide agreement in place, this can create a strong perception that banking online is secure. Banks also need to ensure that the way they design their mobile service should give an immediate impression of strength and safety. Use icons, colours, gradients and tone of voice to improve the perception. Customers will subconsciously notice. Banks should also provide simple, clear and accessible guidance for customers to ensure safe and secure banking whilst on the move.

As Nigeria moves forward, both economically and from a banking perspective, it has an opportunity to really advance itself through a strong banking foundation. As online and mobile banking adoption increases, there will be numerous new revenue and security opportunities that can be utilised. One of the greatest advantages of mobile banking is that it is with your customers all of the time. It is the greatest communications tool ever invented. Mobile should not just be treated as a vertical channel but a horizontal capability that can be leveraged across the bank. From a security perspective, it can be used as a delivery channel for services such as card fraud alerts or to validate card not present transactions. It can also be used to validate overseas transactions. Customers can be notified when their card is used, or by validating that they are overseas, they can ensure transactions are not blocked by the banks fraud systems. Whilst these concepts might seem like pipe dreams, they are happening in other countries and will soon start happening in Nigeria.

If Nigerian banks treat security as a service, rather than something that you just have to do, you change the mind-set of your organisation and the industry as a whole. If you think of security as a service, you will also ensure the customer experience is better. With the risks of a major cyber-attack being more prevalent, it is time for Nigerian banks and the Central Bank to start working together to deliver cross-competitor solutions and frameworks. The good news is that technology is improving all the time and also reducing the load on the customer. Ultimately, security is becoming the most important aspect of banking services – customers demand and expect their money to be safe – so what are you going to do? The decision is yours, Nigeria.

Fighting the battle, Winning the war: Systemic measures to mitigate e-payment fraud in Nigeria

Electronic Fraud is booming with the proliferation of the use of the Internet and associated technologies for financial transactions, and this warrants a baseline level of awareness and vigilance at all levels of the payment ecosystem. When electronic fraud is committed, it behoves every institution, whether or not it is ultimately responsible, to be aware of how electronic fraud (e-fraud) occurs and the ways in which it can be mitigated. Furthermore, awareness of these issues, in an age in which most customers use the Internet in one way or another, simply makes good business sense. Taking steps to minimize e-fraud risk and building customer confidence benefits consumers and builds trust in the industry as a whole.

Problem definition

Online banking fraud is divided into three distinct categories, each of which poses a unique threat to customers and institutions. The three categories are:

Identity Theft

This gets the most attention from the media and is of highest concern to consumers.
Identity theft can be extremely difficult for its victims. It can take months or even years to correct the damage it can cause. If the fraudster has acquired enough information to satisfactorily answer the questions asked by the financial institution, he or she will be able use the information to commit fraud. Because the level and types of questions asked can determine whether or not an identity theft succeeds, those questions must be crafted so that only the true person will know the answers.

Friendly Fraud

This kind of fraud, also referred to as “family fraud,” refers to fraud committed using information that belongs to a trusted friend or family member. As much as financial institutions, independent organizations and the media communicate to consumers that they should not share confidential data, many people do share their information with close friends and family. A growing number of identity theft cases indicate that some close friends and family members will pretend to be the customer and defraud that individual.

Internal Fraud

This type of fraud is not new, but the electronic channels have added other media through which an employee can commit fraud. If a financial institution allows employees access to customer data, and that data is the same information needed to gain access to customer accounts, an employee can easily commit fraud. Because of this, financial institutions require a password or PIN for online banking / ATM and POS transactions where password or PIN is stored in an encrypted format. Another option used is the truncation of account

numbers and customer data to limit employee access to the full numbers. Of the three types of fraud, internal fraud can be the most costly and potentially damaging to financial institutions.

Risk mitigation tools

In order to mitigate risk associated with e-fraud, all financial institution's policies and systemic controls should create an environment in which fraud can be prevented, detected, monitored and benchmarked against industry standards.

These policies and controls should:

- Require "reasonable efforts" to be made to ascertain the true identity of individual customers and/or the stated business purpose of each commercial enterprise with which the bank conducts business.
- Have a know your customer (KYC) policy that includes the following for personal account opening:
  - Proper identification of the customer;
  - Validation of the customer's residence or place of business;
  - Consideration of the source of funds used to open an account;
- Have adequate ongoing monitoring systems in place to identify suspicious transactions, such as structuring, transactions inconsistent with the nature of a customer's stated business purpose, and unusual wire activities. Various operational controls are available to mitigate fraud risk, including:
  - Monitoring transactions coming in and going out of deposit accounts using reports that identify a certain threshold and history of the activity over a specific time frame;
  - Creating reports that monitor large deposits; and
  - Tracking ATM / POS activity based on amount thresholds over a certain time frame.

Standardization

As incidents of data breaches and card fraud continue to grow, businesses must be more aware in protecting themselves. To assist businesses and financial institutions guard against such issues, the CBN instituted an industry wide standardised security framework and subsequently mandated compliance by deposit money banks. Two of the frameworks are the Payment Card Industry Data Security Standard (PCI DSS) and ISO 27001 Information Security Management Systems (ISMS) Mitigating e-payment fraud using PCI DSS and ISO 27001 Controls

The controls below clearly highlight the necessity for the adoption of the two standards by the players in the electronic payment space. Some of the key requirements that have assisted organisations in mitigating fraud are:

Proactive Controls:

1 Background check for systems owners and custodians of critical payment applications (PCI DSS Req.12.7, ISO 27002 A.7.1,A.7.2,A.7.3)

2 Implementation of 2 factor authentication to prevent identity theft, compromise of both Inputter and Authorizer in the bank, limiting internal compromise leading to internal fraud. (PCI DSS req. 8.2,)

3 Implementation of data loss prevention technologies to lock down USB, PS 2ports access to safeguard the implant of key loggers within the bank internal systems. (ISO 27002 A.8.3.1)

4 Implementation of fraud management systems to define behavioural pattern for all systems users

5 Implementation of separation of duties across all critical systems within the bank (PCI DSS Req.6.4.2, ISO 27002 A.6.1.2)

Detective Controls:

1 Implementation of Security Information and Events Monitoring (SIEM) technology solution to monitor all users activities within critical payment applications and supporting infrastructures for event correlation in the case of internal/external compromise (PCI DSS Req.10, ISO 27002 A.12.4,A.16.1)

2 Implementation of Database Activity Monitoring (DAM) technology solution to monitor all user activities to critical payment databases (ISO 27001 A.9.1,A.9.2,A.9.4)

3 Implementation of File Integrity Monitoring (FIM) technology solution to monitor unauthorised critical files modification (PCI DSS Req.11.5)

4 Implementation of CCTV for active physical security monitoring (PCI DSS Req. 9.1.1, IS0 27002 A.11.1, A.11.2)

Consumer Education

Consumer education is critical to preventing electronic fraud. Most individuals will take action if they believe it will decrease their chances of being victimised by fraud, as long as the action does not significantly inconvenience them. By educating customers, financial institutions can decrease their fraud losses.

The following are consumer tips to prevent e-fraud. Institutions can share this information with customers through various channels, such as postings at the branches, flyers sent with monthly statements, emails, through a Web site, and/or by request to a call centre.

Consumer Tips to prevent Identity Theft and Other forms of Fraud

- Ensure you know the person/entity you are giving information to, over the Internet.
- Monitor your accounts and monthly statements thoroughly, ensuring that all the activity is accurate. If your account statements are late, immediately contact your bank(s) to ascertain if and when they were mailed.

- Always thoroughly tear or shred personal information, such as ATM and POS receipts
- Only do business with Internet companies that use a secure form to capture private information, such as an account numbers or credit card numbers. (The key symbol on your browser status bar indicates whether or not a page is secure.)
- Ensure your computer(s) are equipped with anti-virus protection and firewalls to help keep trespassers out. Always back up your data.
- Never divulge personal information to anyone, as identity fraudsters often obtain information through social engineering.
- Confirm the legitimacy of an online business by clicking on the solid lock or key symbol on your browser window, which provides information about the merchant from the server certificate. If the certificate was issued by an independent certificate authority, due diligence has been performed on the business. If someone has cloned a site, the site will not have a certificate. If the certificate name does not match the site, do not use it and notify the institution.
- Always protect your account information. Do not write your personal identification number (PIN) on your ATM/Debit Card.
- When using your ATM, cover your hand when entering the PIN number to protect the information from shoulder surfers.
- Carry only those pieces of identification you absolutely need, and keep them secure.
- Always log off from your online banking session.
- If you suspect your identity has been stolen, contact your financial institution and the authorities immediately.

Conclusion

Identity theft, “friendly fraud” and internal fraud conducted via various electronic channels pose significant threats to the financial services industry and customers. However, while there are certainly a great number of unknowns, many serious threats are known and containable, and can be mitigated with the good banking practices outlined here.

While the electronic channels offer great opportunities, their pervasiveness also pose real threats to every business. In contrast to other technologies, lack of participation in online technology will not protect a financial institution from its dangers. For example, a customer’s account can be compromised if someone fraudulently uses his or her account for an online transaction, whether or not the institution where the account is held offers online banking. Further, an institution that does not offer certain services, such as online bill payment, will likely find that its customers often look to the institution for help when problems arise with that technology. Financial institutions cannot afford to be uninformed in these situations, nor

can they simply be passive players. Instead, all institutions must be vigilant and stay abreast of developments in electronic transactions.

There is not, nor will there ever be, a perfect strategy to eliminate risk to financial institutions and customers. However, the widespread use and adoption of the aforementioned mitigation strategies can minimize many risks and make e-payments safer for consumers and institutions. When online payment is more secure, and consumers have confidence in the services their financial institution provides, everyone will benefit.

References

https://www.huntington.com/security/fraudmitigationstrategieschecklist.htm
http://www.bits.org/publications/fraud/FraudInternetBank0403.pdf

What's The Scam?

By Babatunde Ajiboye
Secretary, Nigeria electronic Fraud Forum (NeFF)
Shared Services Office, Central Bank of Nigeria.

With the advent of the Cashless Policy in 2012, Nigeria has witnessed a steady growth in both value and volume of e-payments across all channels. This increase has also widened the exposure for fraud incidences. While it is a fact that fraud can only be limited and not eliminated, a lot of payments scams need not contribute to the statistic of e-fraud if certain pre-emptive steps in educating users of e-products are taken and promptly too.

Due to this ever increasing threat there is a greater need to improve upon the way consumers learn about fraud prevention – keeping everyone safer. As the age long adage goes, "Prevention is better than cure", costs incurred in setting barriers against the fraudsters could be saved if we observe some basic ethics in our conduct while dealing in the e-divide.

This paper will focus on 3 major fraud windows that have become prevalent in our environment, Phishing, Spam and Spyware.

1. Phishing: 'Phishing' is a technique used to gain personal information for purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses or financial institutions. Spam filters provide some defense against phishers by intercepting their messages, but the target is elusive. The best defense is vigilance by the individual user, because things are not always what they seem to be, you should be skeptical about any unsolicited emails.

What to do when you have a suspected Phishing mail: If you suspect that an email or text message you received is a phishing attempt:

- Do not open it. In some cases, the act of opening the phishing email may cause you to compromise the security of your Personally Identifiable Information (PII).
- Delete it immediately to prevent yourself from accidentally opening the message in the future.
- Do not download any attachments accompanying the message. Attachments may contain malware such as viruses, worms or spyware.
- Never click links that appear in the message. Links embedded within phishing messages direct you to fraudulent websites.
- Do not reply to the sender. Ignore any requests the sender may solicit and do not call phone numbers provided in the message.
- Report it. Help others avoid phishing attempts

2. Spam: Spam is the common term for electronic 'junk mail' unwanted commercial electronic messages. The vast majority of email sent every day is unsolicited junk mail. Examples include:

- Advertising, for example online pharmacy, pornography, dating, gambling.
- Get rich quick and work from home schemes.
- Hoax virus warnings.
- Hoax charity appeals.
- Chain emails which encourage you to forward them to multiple contacts (often to bring 'good luck').

How spammers obtain your email address;

- Using automated software to generate addresses.
- Enticing people to enter their details on fraudulent websites.
- Hacking into legitimate websites to gather users' details.
- Buying email lists from other spammers.
- Inviting people to click through to fraudulent websites posing as spam email cancellation services.
- From names/addresses in the cc line, or in the body of emails which have been forwarded and the previous particpants have not been deleted.
- The very act of replying to a spam email confirms to spammers that your email address exists.

How to spot spam:

- Spam emails may feature some of the following warning signs:
- You do not know the sender.
- Contains misspellings (for example 'p0rn' with a zero) designed to fool spam filters.
- Makes an offer that seems too good to be true.
- The subject line and contents do not match.
- Contains an urgent offer end date (for example “Buy now and get 50% off”).
- Contains a request to forward an email to multiple people, and may offer money for doing so.
- Contains a virus warning.
- Contains attachments, which could include .exe files.

The risks:

- It can contain viruses and spyware.
- It can be a vehicle for online fraud, such as phishing.
- Unwanted email can contain offensive images.
- Manual filtering and deleting is very time-consuming.
- It takes up space in your inbox.

Remember, scams are designed to trick you into disclosing information that will lead to defrauding you or stealing your identity.

3. Spyware: Spyware is software that is installed on a computing device that takes information from it without the consent or knowledge of the user, and gives that information to a third party. With so many types of malicious software being spread around the Internet, it is important to be aware of what spyware is and what spyware does. Spyware is a general term used to describe software that performs certain behaviors, generally without appropriately obtaining your consent first, such as:

- Advertising
- Collecting personal information
- Changing the configuration of your computer

Spyware is often associated with software that displays advertisements (called adware) or software that tracks personal or sensitive information. However, that does not mean all software that provides ads or tracks your online activities is bad. For example, you might sign up for a free music service, but you "pay" for the service by agreeing to receive targeted ads. In signing up, you must understand the terms and agree to them, you may have decided that it is a fair trade-off. You might also agree to let the company track your online activities to determine which ads to show you.

What does Spyware do?

Knowing what spyware does can be a very difficult process because most spyware is designed to be difficult to remove. Other kinds of spyware make changes to your computer that can be annoying and can cause your computer to slow down or crash.

These programs can change your web browser's home page or search page, or add additional components to your browser you don't need or want. They also make it very difficult for you to change your settings back to the original settings.

How to prevent Spyware:

The key in all cases is whether or not you (or someone who uses your computer) understand what the software will do and have agreed to install the software on your computer.

A common trick is to covertly install the software during the installation of other software you want, such as a music or video file sharing program.

Whenever you install something on your computer, make sure you carefully read all disclosures, including the license agreement and privacy statement. Sometimes the

inclusion of unwanted software in a given software installation is documented, but it might appear at the end of a license agreement or privacy statement.

Adherence to these very basic tips can be compared to curing the fear of flying. Being security conscious when we engage in online activities can make our e-payment interactions to be likened to flying premium class. Ignoring these tips however, can bring about the tension and anxiety of a passenger travelling on coach. We hope the former will be chosen over the latter. Happy Flying!!

Babatunde Ajiboye works with the Shared Services Office of the Central Bank of Nigeria. He also is the Secretary of the Nigeria electronic Fraud Forum (NeFF).

Printed by GAPHY MULTI-SERVICES 08033050923