



A CHANGING PAYMENTS ECOSYSTEM: THE SECURITY CHALLENGE

NeFF

THE NIGERIA ELECTRONIC FRAUD FORUM

ANNUAL REPORT, 2016

FOREWORD

TACKLING E-FRAUD: KEEPING PACE WITH CHANGES IN OUR PAYMENTS SYSTEM

The Moody's Analytics report on the Impact of Electronic Payments 2016 has put on record that increased electronic payment usage added US\$460 million to Nigeria's GDP from 2011 to 2015. Year on Year growth in electronic payment adoption statistics show that Nigeria is firmly on its journey towards a digitalized economy, in which electronic transactions will increasingly play a role in our financial system.

That this digital journey is plagued with land mines represented by electronic fraud would be stating the obvious, as the world over has shifted security policy stances to a more cyber-centric position. The warfare of banking security has changed from what was conventional to a constantly changing strategy in response to the rapid developments in payment technology.

As global news of data breaches increase and the payments environment rapidly changes in form, it is important that we start to critically look at all issued that can become a reality that hits us on the road to an increasingly changed payments system.

The introduction of Blockchain technology as a platform for payments now presents new perspectives in securing our payments system. The Nigeria electronic Fraud Forum (NeFF) has begun conversations around this and must be commended for remaining at the forefront of ensuring that electronic fraud in Nigeria is mitigated using proactive steps such as this.

NeFF's decision to focus on "**A Changing Payments Ecosystem: The Security Challenge**" for its 2016 Annual Report cannot be more apt based on the direction which the future of payments is headed. The contents of this report will no doubt shape the conversations of electronic fraud in the days ahead and is a worthy read for all interested in the security of payments not just in Nigeria but across the world.

The Central Bank of Nigeria will continue to identify with the laudable objectives of NeFF and support its stakeholders in their quest to ensure safety and stability of the financial system in Nigeria.



Adebayo A. Adelabu
Deputy Governor Operations
Central Bank of Nigeria

ACKNOWLEDGEMENT

The production of this report was made possible with resource inputs from most of the Deposit Money Banks in Nigeria. A warm appreciation goes to the banks for their contributions.

The Deputy Governor Operations, CBN, Mr. Adebayo Adegola Adelabu has always been there for NeFF, and was of immense support to this project.

Similarly, the Director, Banking and Payments System Department of CBN, who also doubles as the Chairman, NeFF, Mr. 'Dipo Fatokun, was a source of great support and inspiration. His enormous support and guidance is sincerely appreciated.

The commitment shown by the Chief Executive Officers (CEOs) of Banks in Nigeria, especially as regards sponsorship of NeFF meetings, was remarkable and therefore worthy of commendation.

Special thanks also go to Messrs Biyi Dosumu, Mohammed El-Yakub, Musa Jimoh, Chidi Umeano, Premier Oiwoh (Chairman CHBO), Dele Adeginko (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 commitment and hard work in the production of the 2016 Annual Report.

DISCLAIMER

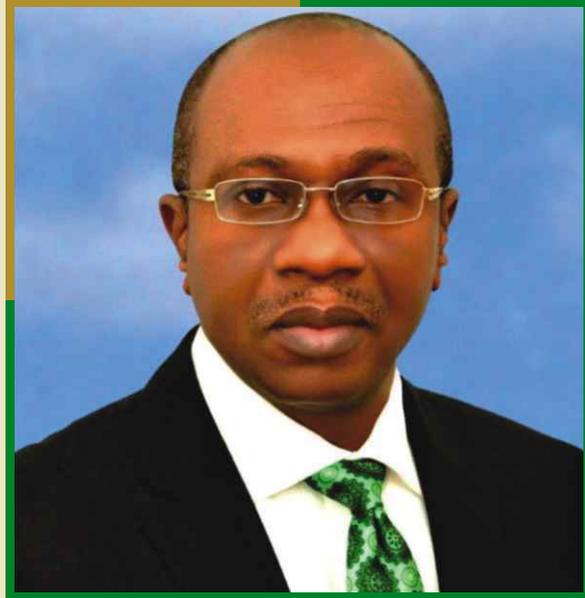
The views expressed in this report are those of the authors and do not necessarily reflect the position of the Central Bank of Nigeria (CBN). No article shall constitute or be deemed to constitute any representation by the CBN.

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

TABLE OF CONTENT

Foreword	iii
Acknowledgement	iv
Disclaimer	v
The Governor and his Deputies	viii
Chairman’s Address for the NeFF 2016 Annual Report	ix
A Changing Payments Landscape: The Security Challenge	1
Fraud Landscape in Nigeria - 2016	7
Transaction Summary – 2016	8
Transaction by Products	9
Transactions Monthly	10
Foreign Transactions	11
Foreign Transactions Summary	11
2016 Fraud at a Glance	13
2016 Fraud Summary	14
Fraud per Channels	16
Fraud by Platform	18
Fraud per Month	19
Fraud per Quarter	20
Fraud in the Last Three Years...	21
Unique Individuals who benefitted from fraudulent transactions	23
Fraud Reported by Other Financial Institutions (OFIs)	24
Cheque Summary 2016	24
2016 Fraud Trends	27

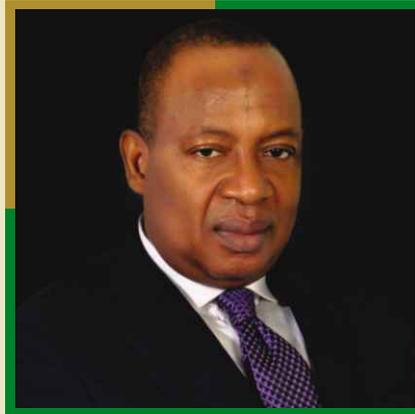
Fraud Trends by Channel	28
Fraud Rate	29
Survey	31
Fraud Desk Survey 2016	31
Industry Security Survey 2016	33
Photo Gallery: 1st Quarter Meeting of NeFF	34
Fraud Outlook 2017	35
Forecasts for 2017	35
Potential Mitigation	36
Securing the Nigerian Payment System: Change Being The Only Constant	37
A Changing Payments Ecosystem: The Security Challenge (Skye Bank)	43
Photo Gallery: Unveiling of the NeFF 2015 Annual Report	50
A Changing Payments Ecosystem: The Security Challenge (UPSL)	51
Blockchain Technology: Opportunity, Risk and Implications for Financial Institutions & Regulators	55
Photo Gallery: NeFF End of the Year Retreat	60
MMM Ponzi - Analysis of Financial Implications in the Nigerian Banking System	61
Internet of Payment Things (IoPT): The Security Concerns	67
A Changing Payments Ecosystem: The Security Challenge	73
Photo Gallery: End of the Year Dinner	76
Credible, Reliable and Efficient Payments System as a Panacea for Curtailling Money Laundering/Terrorism Financing (ml/ft) Risks in Nigeria Financial System	77
Photo Gallery: End of the Year Dinner	81



Godwin I. Emefiele (CON)
Governor



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



Suleiman Barau (OON)
Deputy Governor, Corporate Services



Adebayo Adelabu
Deputy Governor, Operations



Dr. Okwu Joseph Nnanna
Deputy Governor, Financial System Stability

CHAIRMAN'S ADDRESS FOR THE NeFF 2016 ANNUAL REPORT

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

The story of the evolution of money is well known. Humans have transitioned over the years using a payments system that depended on trade by barter, to one that is largely characterized by bytes. Technology has been the platform for this change and has changed the basis of exchange so consistently that the idea of a physical currency is now threatened.



In June 2016, a transaction was consummated that promised to re-define payments, as we know and use it. A thousand Canadian Dollars was transferred between two small banks, one in Canada and the other in Germany. Total transaction time was 20 seconds. This transaction is recorded as the world's first international interbank blockchain payment. The advent of Blockchain Technology has caused a stir around the world and that this will be the underlying technology that will support payments in the years to come, is no longer a moot point.

Coming back home, in the Nigeria InterBank Settlement System (NIBSS) report of the Nigerian fraud landscape for the year 2016, fraud cases in the year of review grew by 82% over figures reported in 2015 and a whopping 1200% over 2014 on the back of rising usage of new payment platforms. However, actual losses reduced by 2.7%, when compared to the losses in 2015. The story behind the figures clearly shows that as we move further down the digital path in payments, fraud attempts are bound to increase and the test of our strength as an Industry will be how effective the collaboration among all stakeholders in warding off this imminent threat to the payments system is, not only domestically but also internationally.

The Nigeria electronic Fraud Forum (NeFF) has consistently provided that unique platform that enables the proactive sharing of resources to combat a common enemy, e-Fraud. Collaborations under NeFF have given rise to decisive outcomes that will steady the ship of our Payments System in Nigeria. Interventions in our Law Enforcement model has been made, attention of the Judiciary has been drawn to the need for more training of our judges on cybercrime, useful discussions have commenced with our telecom regulator in the face of an increased use of mobile platforms for payments (occasioned by the introduction of USSD), on more protective measures for users.

In November, 2016, the NeFF Steering Committee had its retreat at the Transcorp Hotel in Calabar, with the theme; "Rethinking the Future of the Nigerian Payment System". This was in appreciation of the rapid changes being witnessed in Payment Systems all over the world. Major outcomes from the retreat were as follows;

1. Consumer Education through an Industry Wide Awareness Program under a model where the cost of awareness is partially but not entirely borne by stakeholders should be prosecuted. As this will bring greater efficiency and reach to bear on the education of consumers on contemporary fraud issues.
2. That the Central Bank of Nigeria should increasingly monitor and control the risk posed to the National Payments System by Other Financial Institutions (OFIs) and extending Bank Verification Number (BVN) compliance to their customers.
3. The Industry should take full advantage of the BVN for more effective fraud control.
4. Advocacy for the early passage of the Payment System Management Bill should be further intensified.
5. NeFF will collaborate with the National Information Technology Development Agency (NITDA) to implement a National policy document on cloud computing.
6. NeFF to set up an Industry Committee on blockchain technology to monitor developments and make recommendations among others.

All the above will be pursued by NeFF, by ensuring that its relevant stakeholders who have mandates over the recommendations pursue it with both vigour and speed. A major deliverable for NeFF in the coming year will be to organize a workshop that will take a critical look at the Cybercrime Prohibition and Prevention Act 2015.

The Nigeria electronic Fraud Forum (NeFF) has over the last one year embarked on knowledge exchange sessions, aimed at understanding the impact, implications and responsibilities of all stakeholders, particularly those operating within the financial services sector, since the above Act became law. Revelations from this engagements show quite clearly that certain provisions of the Act need more clarity and the responsibilities given to stakeholders, more definition.

The workshop has been slated to hold within the first quarter of 2017, with the theme; “Tackling Enforcement Challenges Under The Cybercrime Act”. It is important for the Industry to have a workshop like this, as it will provide the opportunity for stakeholders to collectively brainstorm on the right direction to take in implementing the law, so as not to undermine the steady growth witnessed in our Payments System in the last 5 years.

Based on the content of our activities in 2016, our intended plan of action in 2017 and being not unaware of the changes that have impacted payments systems, we are proud to present our Annual Report for 2016 titled; “A Changing Payments Ecosystem: The Security Challenge”. It is our view that as fraud trends continue to be observed across the world, it is important that mitigating strategies should align also with changes in form and platforms of payments.

As we manage to keep up with new payment technology, our ability to push security ahead of these developments appears to be a greater challenge. The various papers that have been presented in this report will attempt to do justice in what will be a lingering question in the years to come, seeking to find answers that will balance security against the speed of payments.

We know that the speed and convenience which an increasingly effective payments system brings to bear on our daily transactions would pale into insignificance when thrown against the light of consistent attacks and possible losses. We must start seeing ourselves less as an industry and more as a community in putting our hands on the deck of e-fraud mitigation. The ointment of a nimbler payment system will always appear attractive, however if adequate attention is not paid to security, it might as well just be the fly in that ointment.

Our thanks go to all our stakeholders for being worthy partners in the quest to meet the objectives of NeFF. We will not relent in this war against e-fraud and it is our firm belief that we shall prevail.

A CHANGING PAYMENTS LANDSCAPE: THE SECURITY CHALLENGE

By **Gbolabo Awelewa**

Profile: Gbolabo is a Business Information Systems & Enterprise Security Architect with over a decade's experience in the design, development and management of secure Information Systems and Enterprise infrastructure.

As the Chief Technology Officer at Coronation Merchant Bank, he is responsible for providing vision and leadership in the development and implementation of bank-wide Information Technology and Cyber Security initiatives.

Prior to joining Coronation Merchant Bank, he was Head, Application & Database Security Management at UBA. Before that, he was Interswitch's Head of Information Systems & Security Management. He's a Certified Chief Information Security Officer, Business Continuity Management Specialist and a FinTech enthusiast.



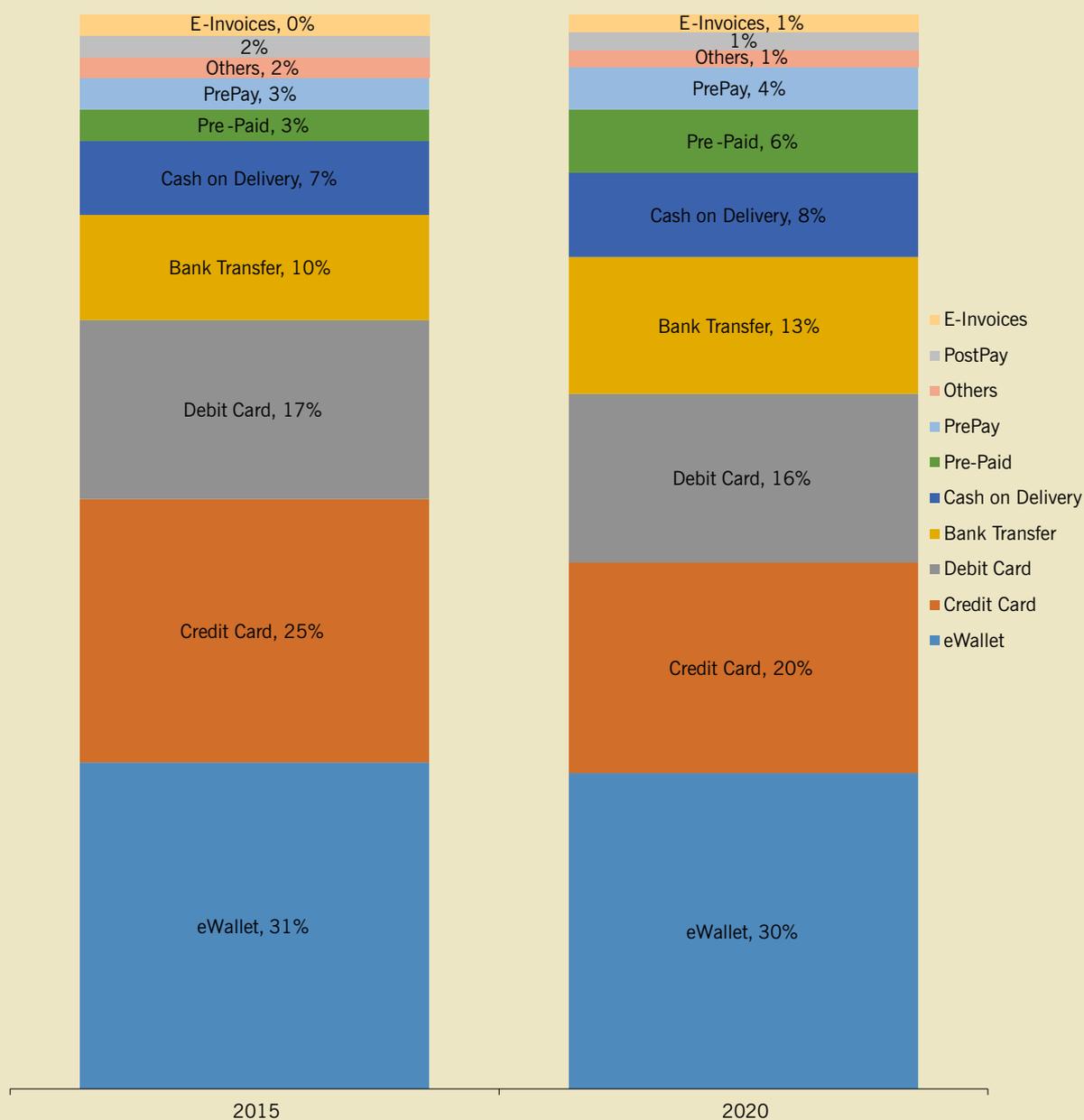
The global system of payments is evolving at a remarkable pace. Our initially barter-based society has evolved through cash, into cheques, then cards, and is now moving into the digital frontier of virtual wallets and mobile platforms. Whereas, at some point in the history of payments, one could only pay with cash, we now have a plethora of alternatives namely: Online payment services (Paypal/Worldpay), Electronic Bills Payment (Internet Banking), Wire Transfer (local or international), Direct Credit (initiated by payer), Direct Debit (initiated by payee), Debit Cards, Credit Cards, and good old Cheques.

Players in the payments space have ranged from the traditional ones (such as banks) coming up with new payment solutions; to new non-bank institutions (such as Paypal and Google) performing traditional payment functions; to even those players attempting to circumvent existing payment systems completely (such as Blockchain service providers and crypto currencies like Bitcoin); all in the bid to find new ways of ensuring that customers are able to pay for goods and services received, and that merchants or businesses are able to receive payment for goods sold and services rendered.



These payment platforms have been so successful that Capgemini reports that “global non-cash transactions grew at 8.9% in 2014 to reach 387.3 billion, the highest growth rate since 2005” – a growth that was driven by developing markets which grew by 16.7% in 2014 compared to mature markets which only grew by 6.0%¹

Figure 1 - Global payments by type 2015 and 2020.



Source: Global Payments Report, November 2016. WorldPay

The heightened activity in payments has been largely attributed to four major shifts being observed in the global payments landscape². First, the ongoing digital and technology revolution, championed by the smartphones and mobile internet has revolutionised digital payments; next, the entry of non-bank institutions (like Google, PayPal, and Worldpay) offering payment services and products; third, customers (consumers and merchants) are becoming more demanding and expect instant payment solutions; fourth and finally,

progressive changes in the regulatory framework. These four factors have given rise to a burgeoning industry recording three trillion transactions per year globally, worth around US\$ 13 trillion in aggregate³.

The advent of marketplace innovation in payment methods, technology and the influx of participants raises important policy issues for the regulators to consider. While on one hand, it is necessary to create an enabling environment for innovations in payment technology which will improve customer convenience, transaction efficiency and overall benefits to the economy, it is also equally imperative that adequate protections be incorporated into the regulatory framework so that customer confidence in the payment system is maintained and even improved. Achieving this balance in policy and regulatory framework development is paramount as it has enormous implications for the economy. Three core issues to be addressed by regulators and policy makers have been identified by the American Bankers Association (ABA)⁴.

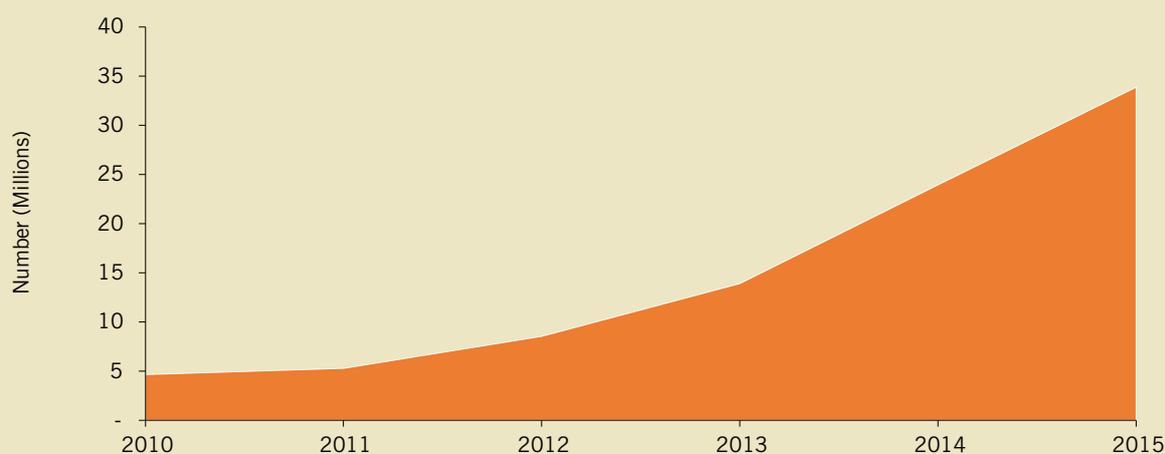
- 1. Consumer Protection** – Regulators and policy makers are saddled with the responsibility of ensuring that consumers are adequately shielded against unauthorised charges, and that the procedures for disputing charges are properly defined. Regulators are also responsible for ensuring that the regulations governing the activities of non-bank payment service providers are well defined in order to prevent the degradation of customer confidence.
- 2. Competitive Equity** – Regulators and policy makers must evolve their policies and frameworks to accommodate the growth of the payments landscape and the introduction of new technologies. They must ensure that all participants, whether incumbents or new entrants, operate by a similar set of rules and standards so that all participants have as equal as possible, incentives to innovate.
- 3. Payment System Integrity** – Because payments are the facilitators of commerce, the overall stability, efficiency and integrity of the payment system must never be in question. All players in the industry must ensure that adequate controls – subject to appropriate government oversight – are implemented to maintain the overall integrity of the payments system.

It is against this backdrop that this article attempts to discuss the challenge of maintaining the integrity of the payments system with respect to the changing payments landscape in Nigeria.

Although non-cash and non-cheque payment solutions were made available relatively recently in Nigeria, in comparison with the Western world, the pace of growth of the payments industry in the country has been remarkable. The World Bank Global Payments Systems Survey⁵ reports that the number of cards (debit and credit cards) grew from 4.7

million in 2010 to nearly 34 million in 2015. The number of mobile money accounts in the country grew from zero to 10 million in the same period, representing a Compound Annual Growth Rate (CAGR) of 49% and 27% respectively.

Figure 2 - Number of Cards (credit & debit) in circulation in Nigeria.



Source - World Bank Global Payments Survey (2015)

With this surge in adoption and usage of payment systems, there has been a rise in the incidence of fraud in the Nigerian payments landscape. Of the nearly 44 trillion Naira in payments made across Nigeria in 2014, over 7 billion Naira was reported as the value of “attempted” fraud and 6.22 billion Naira was the actual loss value reported⁶. The Nigeria Inter-Bank Settlement System Plc (NIBSS) report also shows that in the same year, ATM fraud was the most attempted with 491 incidents and Internet Banking recorded the highest fraud value of 3.2 billion Naira.

With these facts in mind, and considering the rate at which new technologies come on-board, and new payment solutions are introduced, payment systems regulators and policymakers in Nigeria have a lot on their hands if customer confidence in the system is to be improved upon. The European Banking Authority (EBA) has put forward a number of guidelines which could be of use in this regard under the following headings⁷:

- 1. Governance** - Payment Service Providers (PSPs) should implement and regularly review a formal security policy for internet payment services. This policy should be documented properly, reviewed regularly and approved by senior management with oversight from the regulators. It should define security objectives, risk appetite, roles and responsibilities, and a plan for the management of sensitive payment data with

regard to risk assessment, control and mitigation.

2. **Risk Assessment** - PSPs should carry out and document thorough risk assessments with regard to the security of internet payments and related services, both prior to establishing the service(s) and regularly, thereafter.
3. **Incident Monitoring and Reporting** - PSPs should ensure consistent and integrated monitoring, handling and follow-up of security incidents, including security-related customer complaints. PSPs should establish a procedure for reporting such incidents to management and, in the event of major payment security incidents, the competent authorities.
4. **Risk Control and Mitigation** - PSPs should implement security measures in line with their respective security policies in order to mitigate identified risks. These measures should incorporate multiple layers of security defences, where the failure of one line of defence is caught by the next line of defence (“defence in depth”).
5. **Traceability** - PSPs should have processes in place, ensuring that all transactions, as well as the e-mandate process flows, are appropriately traced.
6. **Initial Customer Identification Information** - Customers should be properly identified in line with the anti-money laundering legislation and confirm their willingness to make internet payments using the services before being granted access to such services. PSPs should provide adequate “prior”, “regular” or, where applicable, “ad hoc” information to the customer about the necessary requirements (e.g. equipment, procedures) for performing secure internet payment transactions and the inherent risks.
7. **Strong Customer Authentication** - The initiation of internet payments, as well as access to sensitive payment data, should be protected by strong customer authentication. PSPs should have a strong customer authentication procedure.
8. **Enrolment for, and provision of authentication tools and/or software delivered to the customer** - PSPs should ensure that customer enrolment for, and the initial provision of the authentication tools required to use the internet payment service and/or the delivery of payment-related software to customers is carried out in a secure manner.
9. **Log-in attempts, Session time out, Validity of authentication** - PSPs should limit the number of log-in or authentication attempts, define rules for internet payment services session “time out” and set time limits for the validity of authentication.
10. **Transaction Monitoring** - Transaction monitoring mechanisms designed to prevent, detect and block fraudulent payment transactions should be operated before the

PSP's final authorisation; suspicious or high risk transactions should be subject to a specific screening and evaluation procedure. Equivalent security monitoring and authorisation mechanisms should also be in place for the issuance of e-mandates.

- 11. Protection of Sensitive Payment Data** - Sensitive payment data should be protected when stored, processed or transmitted.
- 12. Customer Education and Communication** - PSPs should provide assistance and guidance to customers, where needed with regard to the secure use of the internet payment services. PSPs should communicate with their customers in such a way as to reassure them of the authenticity of the messages received.
- 13. Notifications, Setting of limits** - PSPs should set limits for internet payment services and could provide their customers with options for further risk limitation within these limits. They may also provide alert and customer profile management services.
- 14. Customer access to information on the status of payment initiation and execution** - PSPs should confirm to their customers the payment initiation, and provide in good time, the information necessary to check that a payment transaction has been correctly initiated and/ or executed.

Footnotes

¹ Capgemini, BNP Paribas. (2016) World Payments Report. <https://www.worldpaymentsreport.com/> Accessed March 2017

² The Boston Consulting Group. (2016) Digital Payments 2020: The Making of a \$500 Billion Ecosystem in India. <https://www.bcg.com> Accessed March 2017

³ Accenture. (2013) Digital Payments Transformation: From transactions to consumer interactions. <http://www.accenture.com> Accessed March 2017

⁴ American Bankers Association. (2013) The Changing Face of the Payments System: A Policymaker's Guide to Important Issues. <http://www.aba.com> Accessed March 2017

⁵ The World Bank. (2016) 2015 Global Payments Systems Survey (GPSS). <http://www.worldbank.org>. Accessed March 2017

⁶ The Nigeria Inter-Bank Settlement System Plc. (2014) 2014 E-PAYMENT FRAUD LANDSCAPE IN NIGERIA. <https://www.nibss-plc.com.ng> Accessed March 2017

⁷ The European Banking Authority. (2014) Consultation Paper on Implementation of Guidelines on Security of Internet Payments EBA/CP/2014/3. <http://www.eba.europa.eu>. Accessed March 2017

FRAUD LANDSCAPE IN NIGERIA - 2016

A Report by the Nigeria Inter-Bank Settlement System (NIBSS) Plc

Introduction

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

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

The industry recorded about 82% increase in the reported fraud case when compared to 2015 and over 1200% when compared to 2014. Despite the 82% increase in the reported fraud cases, with an estimated NGN2.19 billion loss to fraud, the industry was able to reduce fraud by 2.7% when compared to the 2015 figure. Comparing the attempted fraud against the actual loss, the industry was able to salvage 49.7% of the total amount attempted by these fraudsters within the year. These figures informed us that there are more attempts on yearly basis with different innovation tricks or modus operandi to take advantage of the system.

Looking ahead into 2017, the financial industry as a whole must collaborate to ensure a wider gap exists between the attempted fraud and actual loss. The analysis in this report would allow us to benchmark and also understand where the vulnerabilities lie. The industry must come together and implement an effective solution against these vulnerabilities.

Transaction Summary – 2016

2016 witnessed a significant transaction increase across all payment channels in both volume and value in spite of the economic recession. In contrast with 2015, there was a 71.43% spike in volume of transactions processed through the NCS (Nigeria Central Switch).



The Nigeria Central Switch provides interoperability and flexibility of consummating transactions between various institutions within the country's financial space. Table 1 depicts the comparison between total transactions recorded in 2015 and 2016.

The volume of processed transactions in 2016 amounted to 278,744,529, while the value was over NGN 64 trillion. While there was an increase of 71% in volume of transactions, there was also an increase of 31% in the value of transactions compared to 2015.

The Nigeria Central Switch (NCS) recorded electronic transaction of over NGN64 Trillion in 2016

Year End	Volume	Value
2015	162,598,740	48,932,506,699,512.20
2016	278,744,529	64,186,537,023,217.30
% Change	71.43 % Increase	31.03 % Increase

Table 1: Summary of transactions processed by the NCS

Transaction by Products

In 2016, there was an increase in NIP (NIBSS Instant Payment) transaction volume and value. When compared to 2015, NIP exceeded other products both in volume and value. POS and NEFT (NIBSS Electronic Fund Transfer) took the second and third position in terms of volume respectively. The significant increase in NIP transactions is due to its capability to be deployed on different channels

PRODUCT	VOLUME	VALUE
NEFT	25,292,938	12,454,968,222,832.20
NIP	154,504,034	38,214,621,790,755.80
CHEQUE	11,719,847	5,829,549,268,628.46
POS	63,715,203	758,996,505,702.53
eBILLSPAY	1,026,886	339,407,748,304.04
CENTRAL PAY	70,239	1,442,064,836.87
NAPS	3,986,067	753,689,705,802.99
eREFERENCE	331,711	16,868,700.00
MOBILE	3,677,302	143,886,729,277.00
ABC	14,420,302	5,689,958,118,377.48
TOTAL	278,744,529	64,186,537,023,217.30

Table 2: Summary of 2016 transactions by Products

and its adaptability to different modes of payment. Likewise, the POS volume attests to the fact that more people are embracing the cashless modes of payment in the country.

Table 2 shows the summary of 2016 transactions by product. Again, from table 2, we can deduce that 55.40% of total transaction volume is NIP while 59.58% of overall transaction value is NIP. It is quite obvious that NIP has been a viable and most used product over the years. In 2016, the volume of POS transactions was impressive, being the second largest transaction by volume in 2016. All products had either tangential or significant change when compared to 2015.

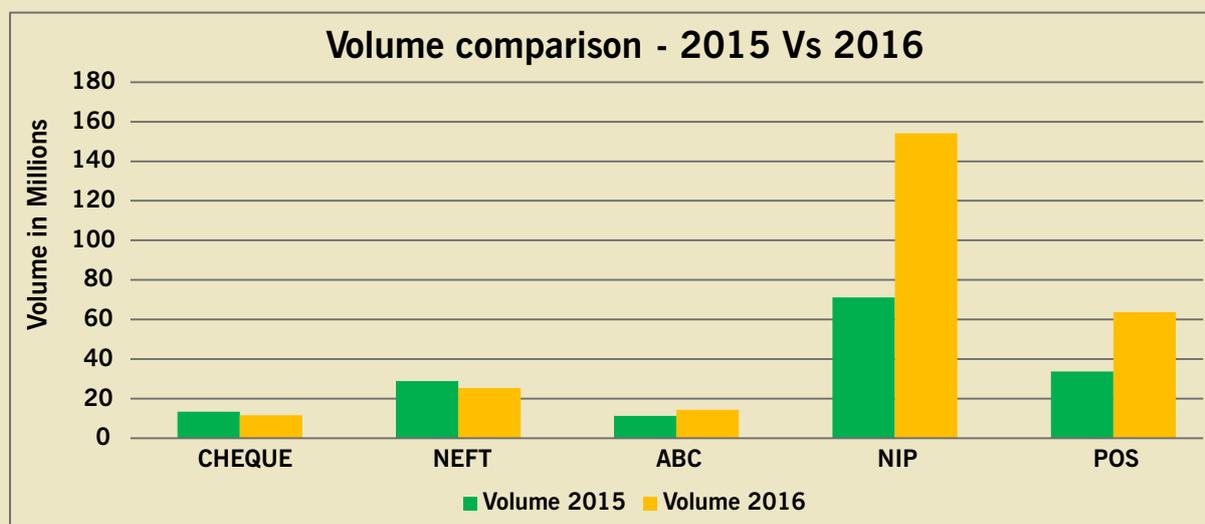


Figure 1: Transaction Volume processed by NCS categorized by payment types

Transactions Monthly

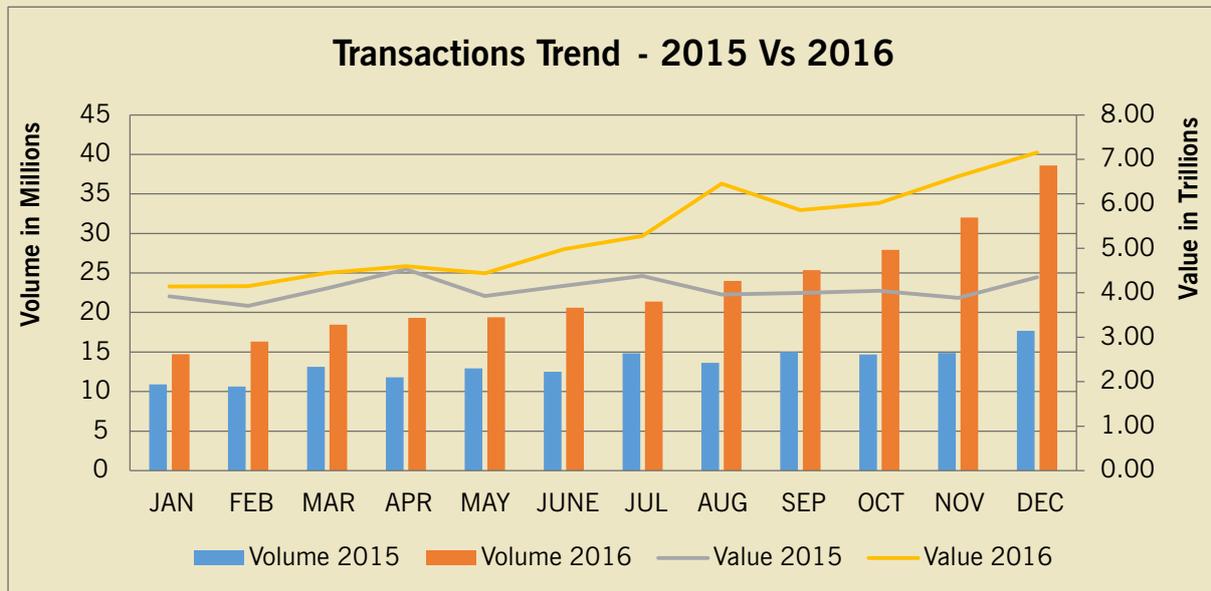


Figure 3: Transaction Growth on Monthly Basis

Figure 3 above shows a graduated growth of transactions from the beginning of 2016 to the end. The consistency in the month-on-month growth reveals a slight shift from 2015 and it shows that more customers are adopting electronic payments on daily basis.

FOREIGN TRANSACTIONS



Foreign Transactions Summary

There was a reduction on the total number of foreign transactions carried out in 2016 when compared to 2015. This reduction spanned across transaction values. It is quite clear that the exchange rates and CBN regulation on foreign exchange affected the velocity of foreign transactions across product channels in 2016.

PRODUCT	VOLUME 2015	VOLUME 2016	VALUE 2015	VALUE 2016
ATM	4,907,069	3,715,319	1,392,275,575.72	474,457,039.74
POS	3,293,852	3,656,895	655,644,377.07	413,101,187.95
OTHERS	1,636,939	359,985	305,249,055.85	30,874,688.08
WEB	1,455,536	2,575,702	98,835,004.24	109,819,535.79
TOTAL	11,293,396.00	10,307,901.00	2,452,004,012.88	1,028,252,451.56

Table 4: Foreign Transactions per Channel

In spite of high exchange rate in 2016, there was an increase of 11.11% in foreign web transaction by value, when compared to 2015. From table 4, with the exception of foreign web transactions, all other product channels decreased significantly by value in 2016 when compared to 2015. More so, across the product channels, there was a drop in foreign transaction volume in 2016, in contrast to 2015.

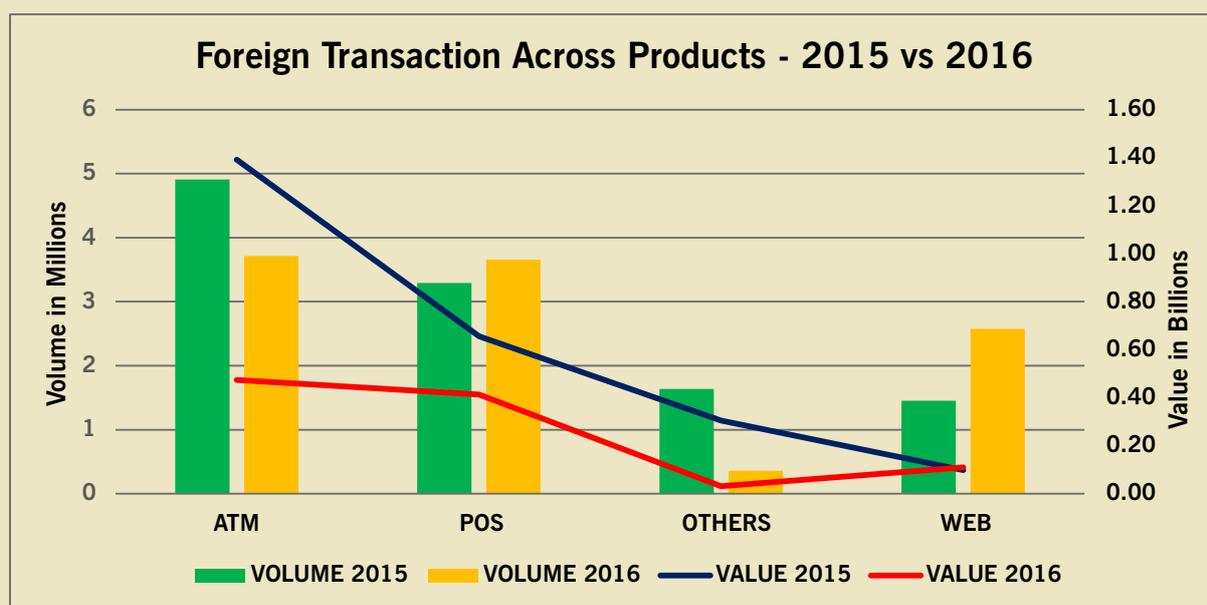
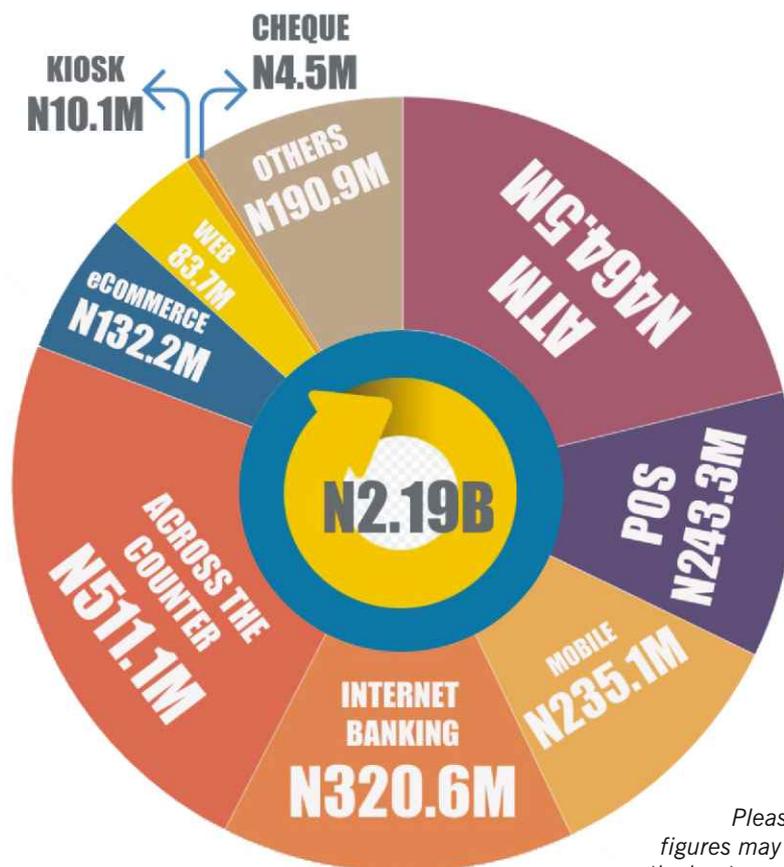


Figure 4: Foreign Transaction across Products

2016 FRAUD AT A GLANCE



The chart below shows the Actual Loss Value as reported on the Anti-Fraud Portal on 2016



Please note that figures may not add up exactly due to approximation

2016 Fraud Summary

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

"The Bad Guys" are constantly finding ways to perpetrate their illicit intentions and take advantage of the system. However, "The Industry" is always deliberating and implementing strategies and policies to negate the acts of these fraudsters. It has been a tough battle but surely, we are winning!

The directive by the Central Bank of Nigeria (CBN) for the establishment of industry fraud desks, sending of all electronic interbank transactions to the Central Anti-Fraud Solution (HEIMDALL), introduction of biometrics to the ecosystem, and most importantly, our collaboration, have contributed to reducing fraud menace in Nigeria's financial space.

The figure below shows that 19,531 fraud cases were reported for Deposit Money Banks in 2016 as against 10,743 in the Year 2015. Although, there was 82% increase in reported fraud cases as compared with 2015, we also witnessed marginal reduction in attempted fraud value and actual loss is **4,368,437,371.64** and **2,196,509,038.78** respectively. Also, there was a decrease of 2.65% in actual loss due to fraud in 2016 when compared with 2015.



N2.19 billion Actual Loss Value with 50.28% Actual Loss Value in Attempted Fraud Value

82% increase in reported fraud cases compared with 2016

2.65% decrease in actual loss value

The attempted fraud value and actual loss value for 2016

... Although more fraud cases were reported in 2016, we had less actual loss value.

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

Table 5: Summary Fraud Report

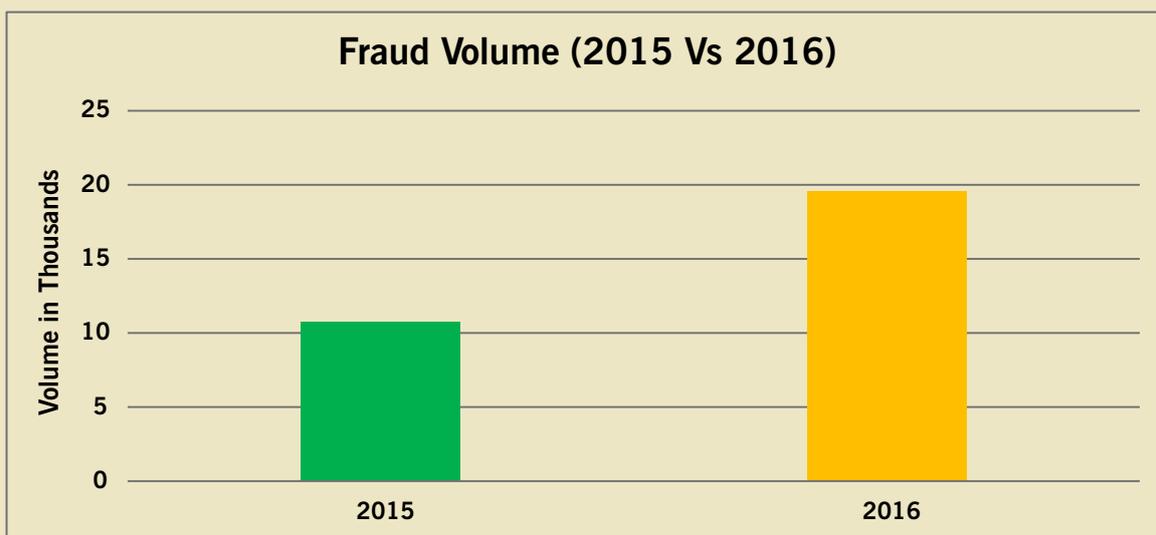


Figure 5: Comparing fraud volume for the years 2015 & 2016

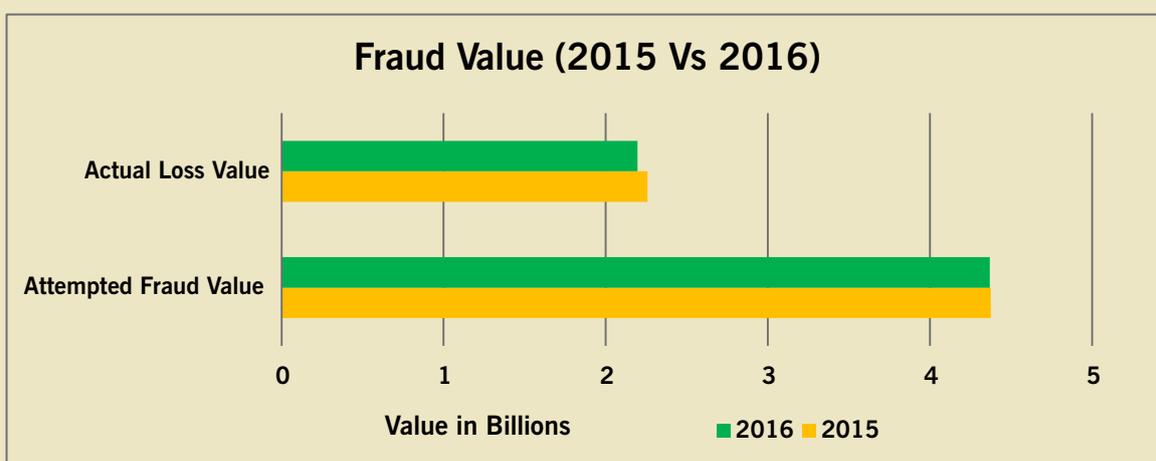


Figure 6: Comparing fraud value for the years 2015 & 2016

Fraud per Channels

Exploring reported fraud events in the year 2016 and categorizing them according to channels, fraud perpetrated through the **Automated Teller Machine (ATM) recorded the highest volume of fraud** followed by Mobile.

This is analogous to several emerging products and services riding on these channels which fraudsters are taking advantage of, especially mobile channel. The third most used channel to perpetrate fraud is Web.

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

Across the counter
recorded the highest
actual loss value

ATM recorded
the highest fraud
volume

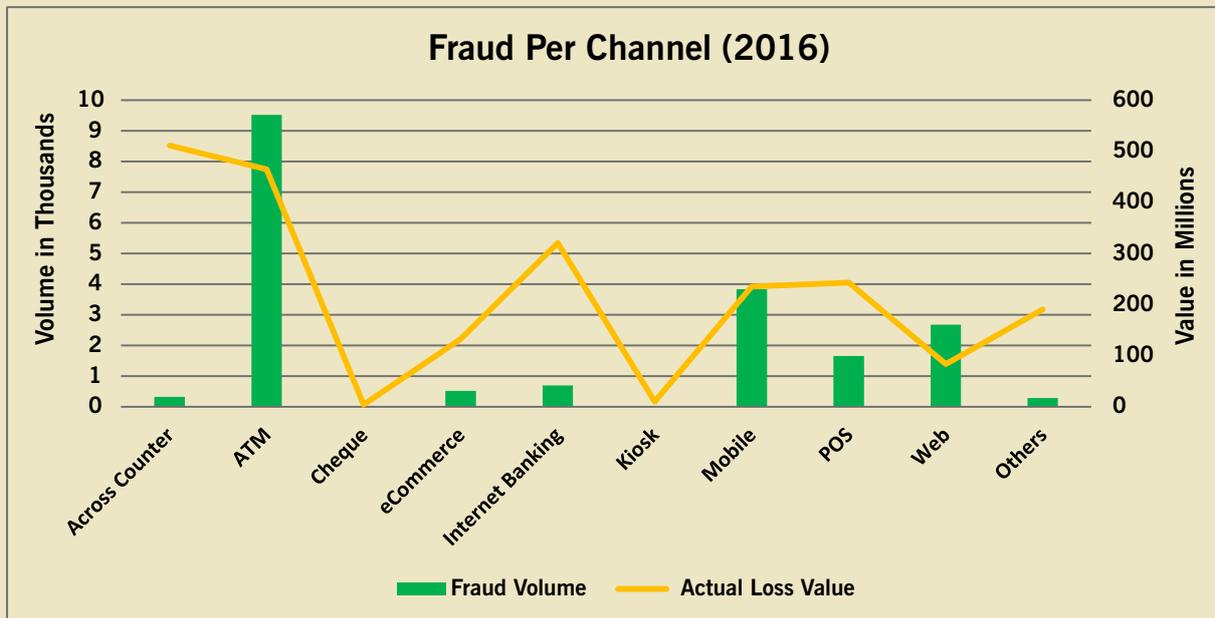


Figure 7: Fraud according to channels in the year 2016: Volume & Value

It is noteworthy to mention that ATM has been the most used channel for fraudulent transactions for the last two consecutive years. We have also seen the increase in Mobile channel fraud. Hence, the need for the Industry to re-evaluate current strategies and policies.

Same with 2015, **“across counter” channel recorded the highest actual loss value for the year 2016** with approximately N511 million. Although, it is less than what we witnessed in 2015 in terms of volume and value. We advise that banks should review their internal processes to curb this, especially with the current status of our economy. ATM and Internet banking occupy the second and third position respectively – same with 2015.

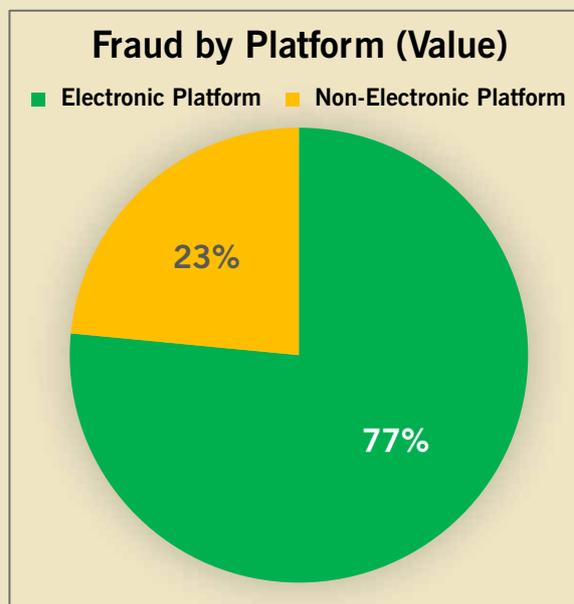


Fraud by Platform

NIBSS categorized various channels stated above into Electronic and Non-Electronic platforms. Tables 7 & 8 below show all payment channels currently captured on the Industry Anti-fraud portal with their corresponding fraud volume and actual loss value for 2016 represented as either electronic or non-electronic platform.

Examining the total fraud volume and value on both platforms, it is evident that fraudsters still leverage more on the electronic platform to carry out their illicit acts.

Consequently, the Non-electronic platform which comprises of “Cheque and Across the Counter” channels represent about 23% of the total actual loss for the year. This shows a lower percentage when compared with 2015, with non-electronic platform representing 43% of the total actual loss for that year.



NON-ELECTRONIC PLATFORM		
Channel	Fraud Volume	Actual Loss Value
Across Counter	325	511,072,861.29
Cheque	12	4,558,897.75
TOTAL	337	515,631,759.04

Table 8: Non-Electronic Channel

ELECTRONIC PLATFORM		
Channel	Fraud Volume	Actual Loss Value
ATM	9,522	464,514,684.27
eCommerce	520	132,252,118.32
Internet Banking	698	320,665,957.87
Kiosk	3	10,198,000.00
Mobile	3,832	235,170,720.40
POS	1,658	243,321,812.67
Web	2,677	83,776,994.11
Others	284	190,976,992.10
TOTAL	19194	1,680,877,279.74

Table 7: Electronic Channel

Fraud per Month

Based on trend and human perception, it is believed that fraud rates increase towards the end of the year due to several festivities observed during this period and the need for people to get more money. But, the truth is, fraud can occur anytime, hence the need for us to always gear up our preventive and detective strategies. Exploring reported fraud cases in 2016, there was a twist when compared with the last two years.

Although, there was increase in the “ember” period, there was less impact in terms of actual loss value – *this will be in detail under “fraud per quarter” segment*. This increase is marginal when compared with last year. In 2016, the month of October recorded the highest fraud volume, followed by March and June respectively. The month of June recorded the highest actual loss value, while February and January took the second and third position respectively.

October recorded the highest fraud Volume while June recorded the highest Actual Loss Value

Month	Fraud Volume	Actual Loss Value
Jan	1,373	227,538,777.49
Feb	961	247,384,495.54
Mar	2,070	188,483,660.93
Apr	1,558	86,164,641.79
May	1,918	104,982,112.35
Jun	1,991	428,160,136.23
Jul	1,448	202,828,418.01
Aug	1,213	157,102,022.47
Sep	1,587	116,094,659.61
Oct	2,128	153,091,198.51
Nov	1,424	138,862,567.58
Dec	1,860	145,816,348.27
TOTAL	19,531	2,196,509,038.78

Table 9: Reported Fraud per Month

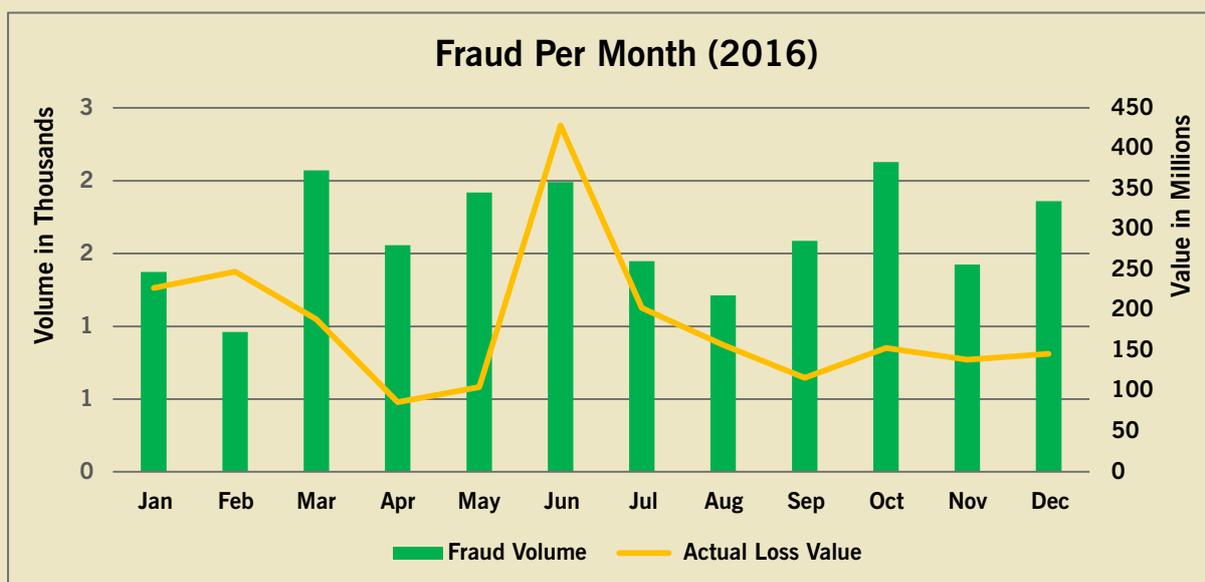


Figure 9: Reported fraud per month

Fraud per Quarter

Quarter	Fraud Volume	Attempted Fraud Value	Actual Loss Value	% Actual Loss Value in Attempted Fraud Value
1st Quarter	4,404	1,136,910,083.39	663,406,933.96	58.35%
2nd Quarter	5,467	1,169,639,671.48	619,306,890.37	52.95%
3rd Quarter	4,248	1,092,332,880.26	476,025,100.09	43.58%
4th Quarter	5,412	969,554,736.51	437,770,114.36	45.15%

Table 10: Reported Fraud per Quarter

Segregating reported fraud cases in the year 2016 into quarters, we experienced constant decrease in the actual loss value. Indeed, this is notable, and shows that our co-operation in the fight against fraud is paying off. For the first time in three years, the fourth quarter of 2016 recorded the lowest actual loss and attempted fraud value.

In 2015, attempted fraud value consistently increased across each quarter. The same goes for actual loss value with just a marginal drop in the second quarter.

...for the first time in 3 years, the 4th quarter recorded the lowest Actual Loss and Attempted Fraud Value.

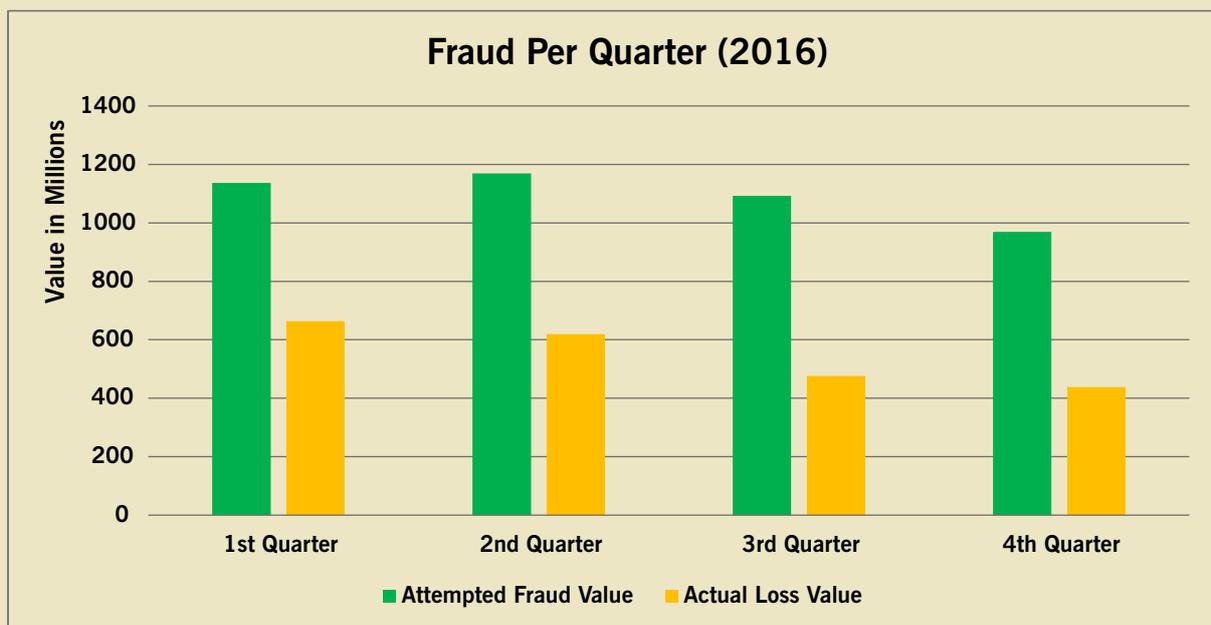


Figure 10: Reported fraud per quarter

Fraud in the Last Three Years...

Figure 11 below depicts reported fraud cases across the channel in the last three years.

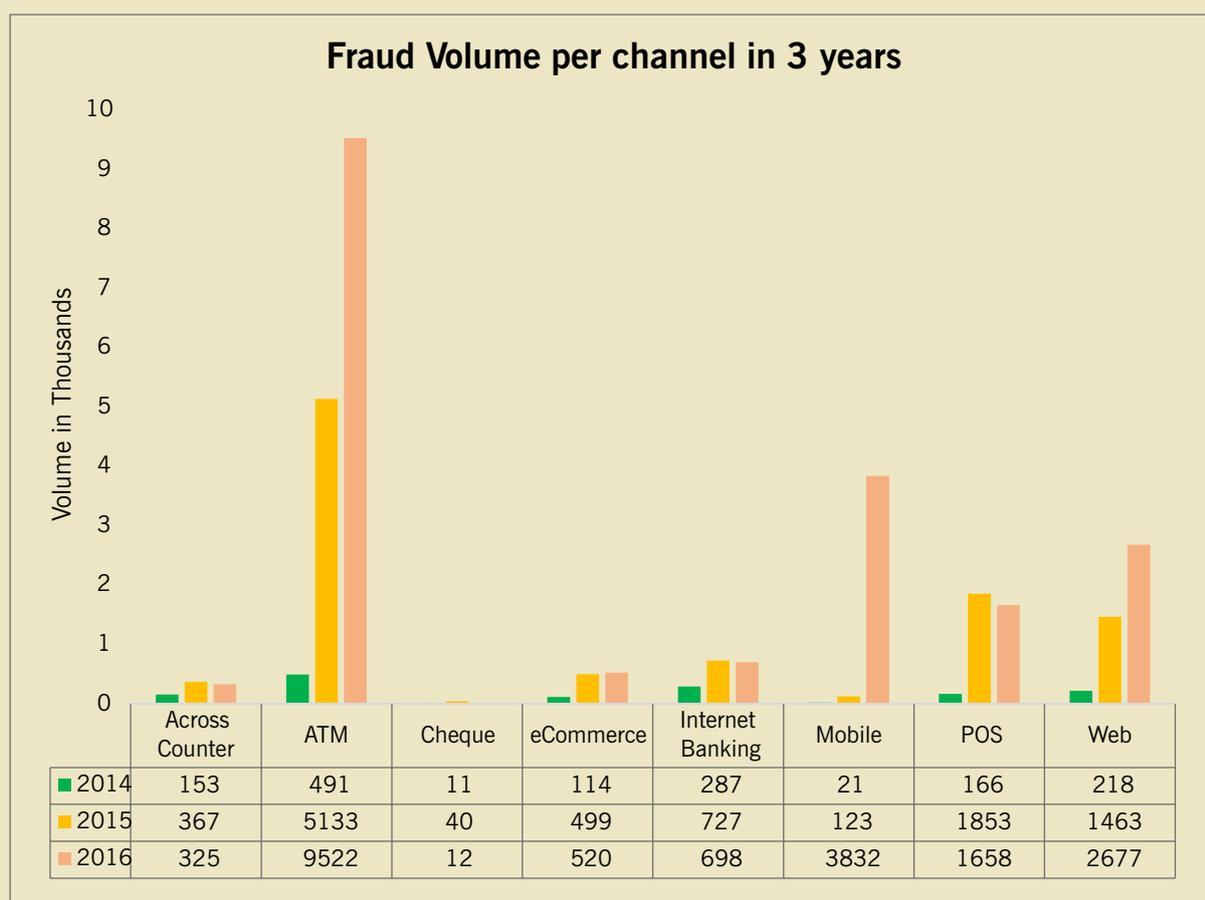


Figure 11: Fraud volume per channel in the last 3 years

In 2014, fraudulent transactions consummated through ATM, Internet banking and Web channels were the top three. In 2015, ATM, POS and Web were the top three most used channels to perpetrate fraudulent transactions. However, in 2016, ATM, Mobile and Web were the three most used. Apparently, ATM and Web channels have consistently appeared in top three channels used to perpetrate fraud for three years running. This is something we have to look at collectively as an Industry.

From figure 11 above, it can be deduced that ATM channel has been the focal point for fraudsters in the last three years. The emergence of Mobile channel in this category cannot be extraneous to the various financial products and services we have these days, which ride on mobile platforms.

As various mobile products and services are being developed, we advise that proper risk assessment and impact analysis be done on these products and services before roll-out or launch.

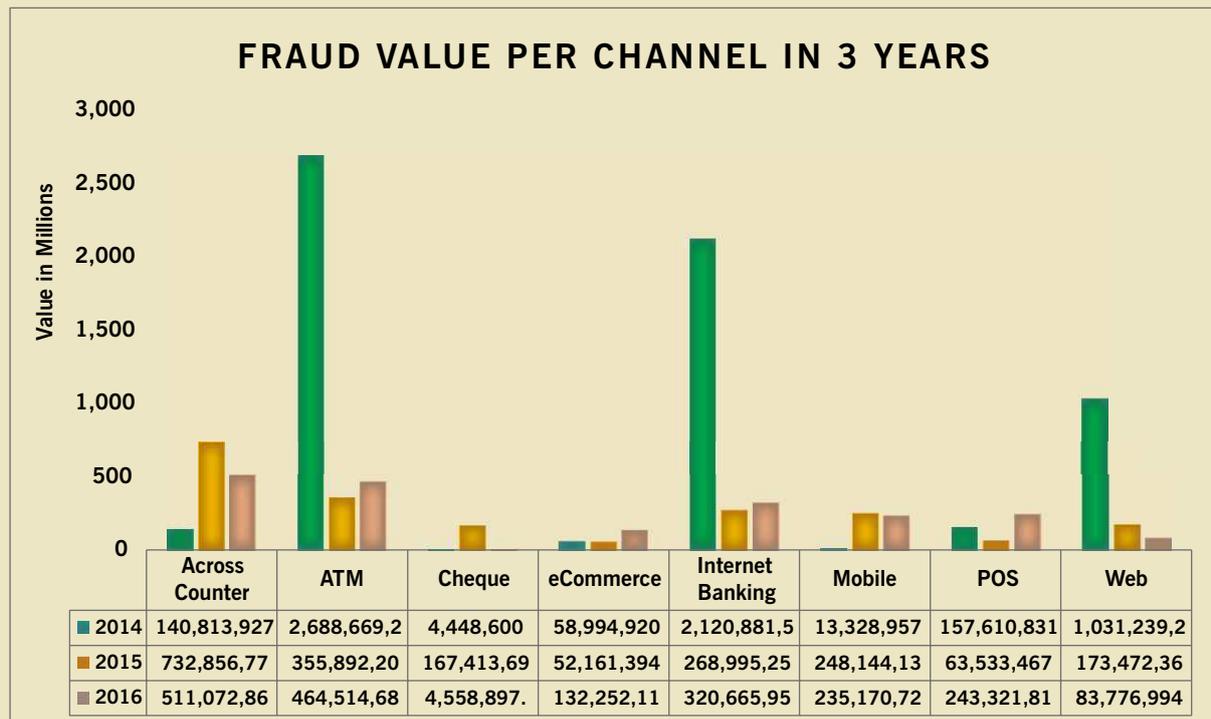


Figure 12: Fraud value per channel in the last 3 years



Unique Individuals who benefitted from fraudulent transactions

Based on reported fraud data for the year 2016, a total number of 1,020 unique individuals were beneficiaries of fraudulent transactions consummated through these channels:– *Across the counter, ATM, Internet Banking, Mobile, Web, eCommerce.*

However, it is quite unfortunate that despite several awareness and tips about BVN watchlist, some institutions still refuse to send BVNs of their customers who have been involved in fraudulent acts for watch-listing, thereby leaving these fraudsters free in our ecosystem and subsequently perpetrating more fraud. Out of the 1,020 unique individuals who were beneficiaries of fraudulent transactions in 2016 across listed channels, only 217 BVNs were sent to NIBSS for watch-listing. Obviously, this is just about 21% of supposed watchlisted BVNs. If we do not cut-off these unscrupulous elements from the financial ecosystem, they will continue to migrate from one institution to another wreaking more havoc.

Table 11 above shows count of unique individuals who benefitted from fraudulent transactions within the year across some channels. The Automated Teller Machine (ATM) which has been the most used channel to perpetrate fraud in the last four years, tops the list. This is followed by the Mobile channel. Apparently, these channels are also the top two used channels to consummate fraudulent transactions for the year 2016.

Channel	Unique Individuals that benefitted
Across Counter	15
ATM	425
Internet Banking	81
Mobile	282

Table 11:
Unique individuals who benefitted from fraudulent transactions for the year 2016.

Only about 21% of individuals who benefitted from fraudulent transactions were sent to NIBSS for watchlisting

Fraud Reported by Other Financial Institutions (OFIs)

The OFIs reported a total number of 88 fraud cases in 2016. This is about 38% reduction in reported fraud volume when compared with 2015. The attempted fraud value is **NGN 50,530,753.30** while actual loss value amounted to **NGN 17,419,283.40**.

Consequently, we have 51% reduction in actual loss value and about 4% increase in attempted fraud value when compared with 2015.

Cheque Summary 2016

The information below represents the overview of Cheque transactions in 2016. When compared to that of the year 2015, reductions are evident in Cheque Presented/Accepted and returned (for value). A reduction is also visible in the volume recorded for Cheques Presented/Accepted and rejected. With the advent of new, and promotion of existing alternatives for making payments, the issuing and usage of Cheques is seemingly declining.

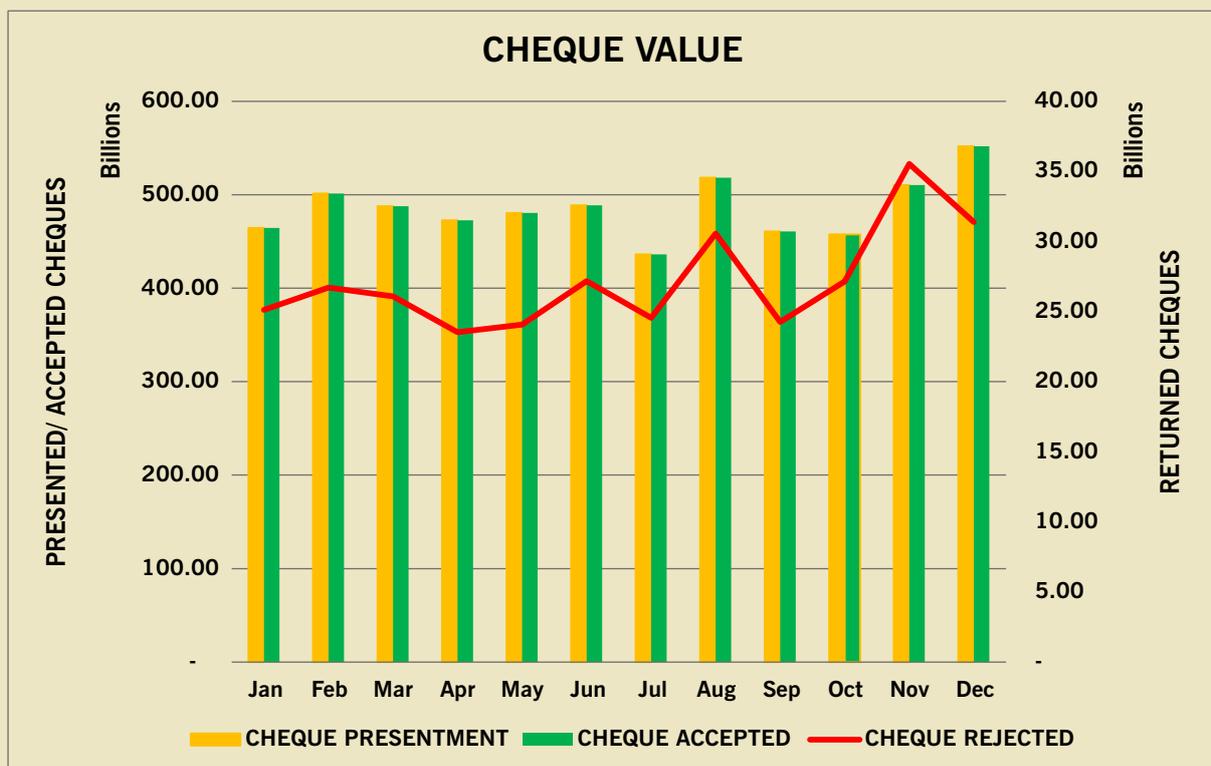


Figure 13: Cheque Value [2016]

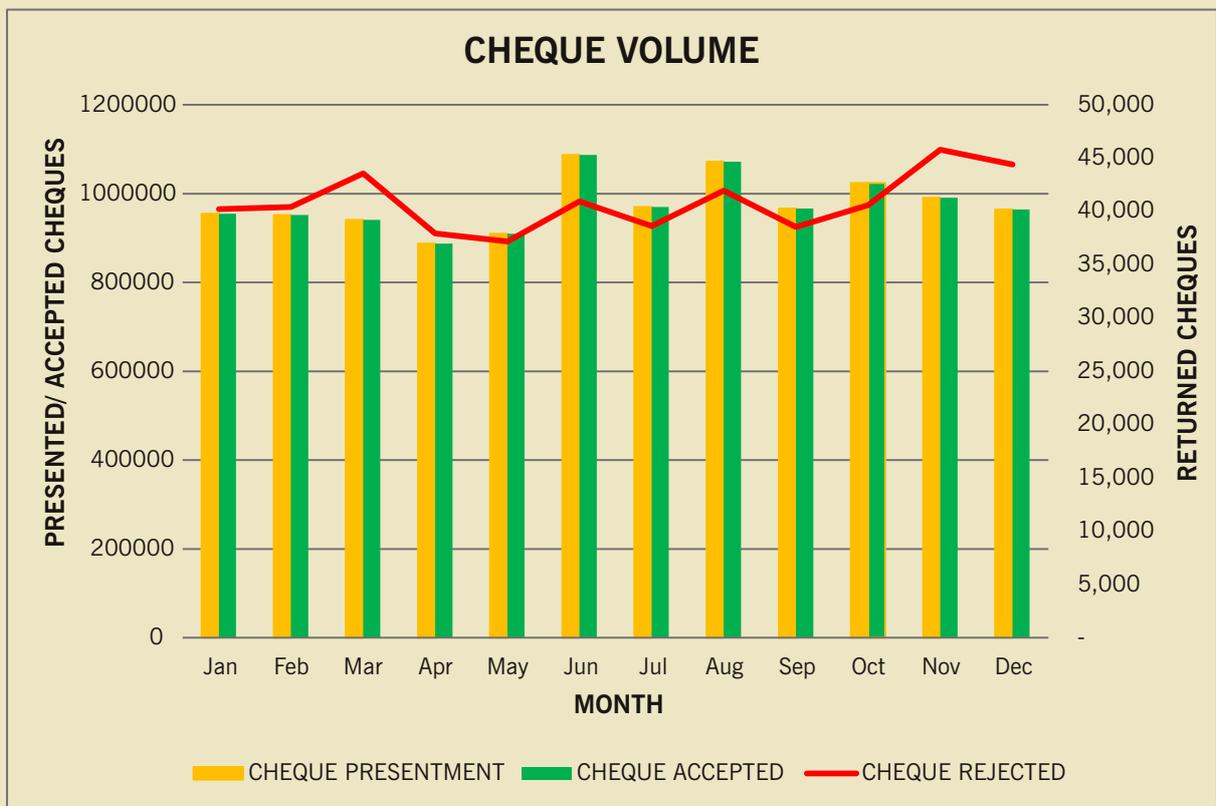


Figure 14: Cheque Volume [2016]

Month	Cheque Presentation Volume	Cheque Accepted Volume	Cheque Returned Volume	% of Returned Cheque (Volume)	Cheque Presentation Value	Cheque Accepted Value	Cheque Returned Value	% of Returned Cheque (Value)
JAN	954,659	954,659	40,211	4.21%	464,552,899,410.41	464,552,899,410.41	25,124,034,473.60	5.41%
FEB	951,824	951,824	40,424	4.25%	501,165,497,863.54	501,165,497,863.54	26,702,107,608.19	5.33%
MAR	940,955	940,955	43,553	4.63%	487,571,913,258.76	487,571,913,258.76	26,089,221,464.36	5.35%
APR	887,721	887,721	37,942	4.27%	472,464,926,944.08	472,464,926,944.08	23,517,519,654.08	4.98%
MAY	909,546	909,546	37,166	4.09%	480,409,004,348.86	480,409,004,348.86	24,066,848,319.24	5.01%
JUN	1,087,100	1,087,100	40,930	3.77%	488,626,752,185.75	488,626,752,185.75	27,161,301,959.91	5.56%
JUL	970,240	970,240	38,624	3.98%	436,046,012,842.98	436,046,012,842.98	24,553,361,803.23	5.63%
AUG	1,071,921	1,071,921	41,951	3.91%	518,116,842,894.17	518,116,842,894.17	30,563,678,621.31	5.90%
SEP	966,480	966,480	38,536	3.99%	460,737,065,090.69	460,737,065,090.69	24,268,616,923.56	5.27%
OCT	1,024,100	1,024,100	40,581	3.96%	457,579,061,969.19	457,579,061,969.19	27,150,199,735.09	5.93%
NOV	990,676	990,676	45,779	4.62%	510,312,940,520.98	510,312,940,520.98	35,520,965,841.53	6.96%
DEC	964,625	964,625	44,411	4.60%	551,966,351,299.05	551,966,351,299.05	31,381,775,844.99	5.69%
Total	11,719,847	11,719,847	490,108	4.18%	5,829,549,268,628.46	5,829,549,268,628.46	326,099,632,249.09	5.59%

Table 12: Overview of Annual cheques

2016 Fraud Trends

2016 closed with slight reductions in value attempts and its losses despite experiencing increase in fraud volume. Actual loss value was about 50 percent less than the attempted fraud value. The year 2016 also experienced a 2.65 percent decrease from 2015 actual loss values. Looking critically over a span of three years, we can see a decline in attempted and actual loss fraud value, but with growing increase in the fraud volume. This trend warns us on the increasing activities of fraudsters, but also suggests that not only was fraud well managed, but the fight against fraud is yielding results.



Year	Fraud volume	Attempted fraud value	Actual loss	%
2015	10,743	4,374,512,776.64	2,256,312,660.00	52
2016	19,532	4,368,437,371.64	2,196,509,038.78	50
% difference	81.80	0.14	2.65	

Table 13: Total fraud values, volume and its percentage difference.

Fraud Trends by Channel

High increase in fraud volume could be linked to the current economic recession, the volume of transactions processed this year,, and most especially, less awareness on the part of customers. ATM, Mobile and Web depict inundate increases when compared with the previous years. The growing use of the electronic payment platforms as the primary means to transact, has definitely attracted and retained fraudsters. POS fraud volume showed slight decrease despite jump in volume in 2015, whilst the value increased marginally. Web fraud values dropped significantly, with mobile fraud maintaining almost the same figures.

Mobile fraud appears to be the most susceptible to fraud and gaining the most interest amongst fraudsters

Trends show “Mobile” as a channel of growing interest for fraudsters' activities, as the adaptation of mobile channels to effect easier and simpler payments. ATMs are the dispatch avenues for stolen funds and thus is highly used by fraudsters to cart away stolen funds.

Focus should be on ATM, Web, Mobile and POS as well as internet banking, as these are suggestive of increasing attacks from fraudsters this year as well as internet banking. Even though the aforementioned channels are attractive and its probability high, other channels are to be guarded equally, as current trends show fraudsters ever changing activities across all channels.

Channel	Volume 2015	Volume 2016	% decrease / increase in volume	Value 2015	Value 2016	%decrease / increase in value
ATM	5133	9522	85.5	355,892,203.30	464,514,684.27	30.5
Cheques	40	12	-70	167,413,696.90	4,558,897.75	-97.27
Across counter	367	325	-11.44	732,856,773.50	511,072,861.29	-30.26
eCommerce	499	520	4.2	52,161,394.14	132,252,118.32	153.5
Internet Banking	727	698	-3.98	268,995,257.70	320,665,957.87	19.2
Mobile	123	3832	3015	248,144,131.00	235,170,720.40	-5.22
POS	1853	1658	-10.5	63,533,467.48	243,321,812.67	282.9
Web	1463	2677	82.98	173,472,360.60	83,776,994.11	-51.7

Table 14: Fraud trend by channels in terms of percentage change between 2015 & 2016

Fraud Rate

Although values of the year 2016 are almost same with those of 2015, the difference in its volume when compared to 2015 suggests more success in curbing fraud. More attempts in volume can be seen over a period of three years, and the rate is expected to increase significantly if the current recession is to be taken into consideration. The current economic recession has, and will always drive persons deeper into fraudulent activities. Also, with the growing adoption of electronic means of payment by individuals and migration to the use of smart phones coupled with the popularity of crypto-currencies in our nation, heightened fraud attempts in volume is almost inevitable. However, though fraud volume in 2016 increased with over 80%, the value in actual loss and attempted was lower than that of 2015. This lends credence to collaborative efforts between the various fraud desks and banks, as well as NIBSS aggregating responsibilities over the various financial institutions.

Year	Attempted fraud value	Actual loss	% difference
2015	4,374,512,776.64	2,256,312,660.00	52
2016	4,368,437,371.64	2,196,509,038.78	50.2

Table 15: Actual loss value as a percentage of attempted fraud value in 2015 and 2016

Year	Transaction Volume	Fraud Volume	Fraud Rate (Vol.)	Transaction value	Fraud Value	Fraud Rate (Val.)
2014	113,421,933	1461	0.001%	43,857,678,478,941	7,750,152,748.00	0.017%
2015	162,598,740	10,743	0.006%	48,932,506,699,512.20	4,374,512,776.64	0.009%
2016	278,744,529	19,532	0.007%	64,186,537,023,217.30	4,368,437,371.64	0.007%

Table 16: Fraud value and volume as a percentage of Transaction value and volume respectively in 2015 and 2016

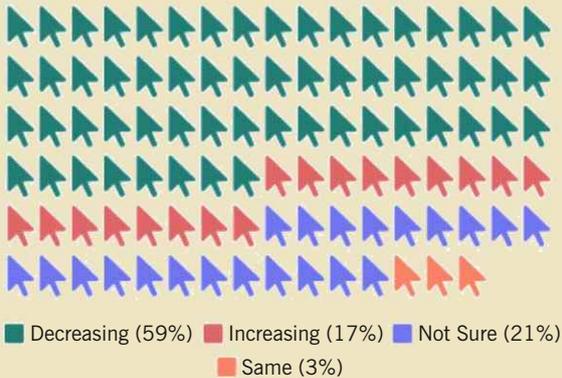


Figure 14: Representation of fraud Rate over the years [2014-2016]

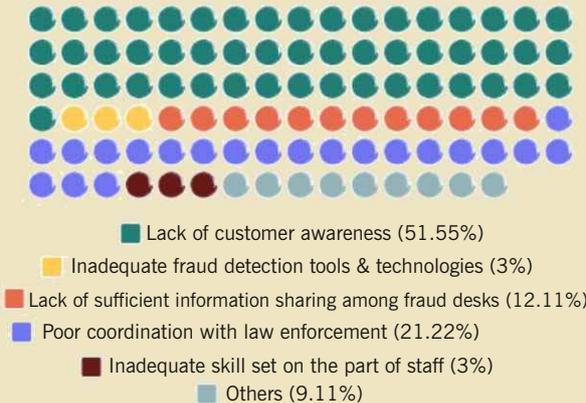


Fraud Desk Survey 2016

What is your experience with cross-border fraud this year?



What is your organization's biggest challenge in the fight against fraud?



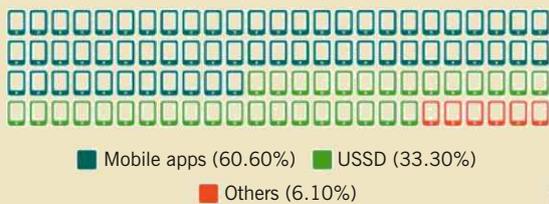
Area of Operations



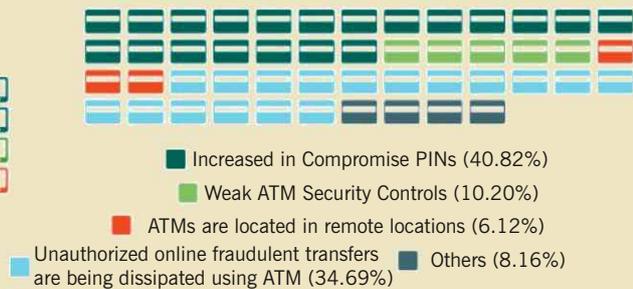
Major contribution to Fraud



The industry is experiencing an increase in mobile frauds, in your opinion, which of these packages is majorly responsible for the increase?



We have seen ATM-related fraud increase within the year, to what do you attribute this increase?

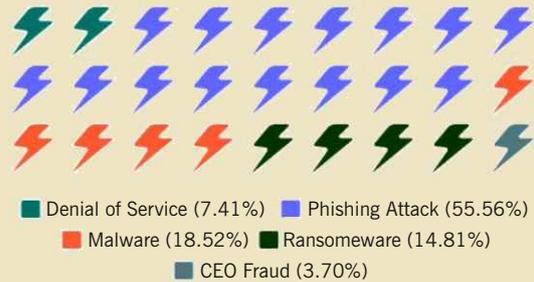


Industry Security Survey 2016

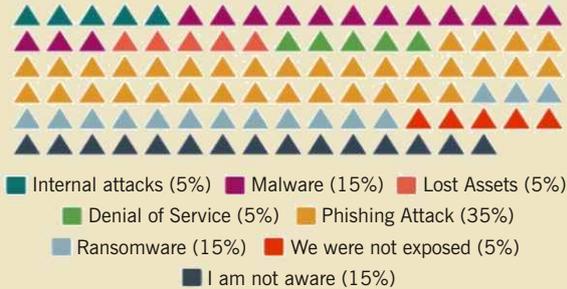
Have you suffered a security breach in your organization in the last 12 months?



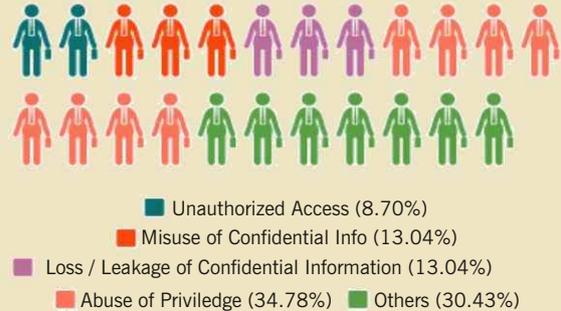
Which of the following attack did your organization experience in the year 2016? (Tick all that applies)



Which was the worst (with greatest impact) security incident faced by your organization in the year 2016?



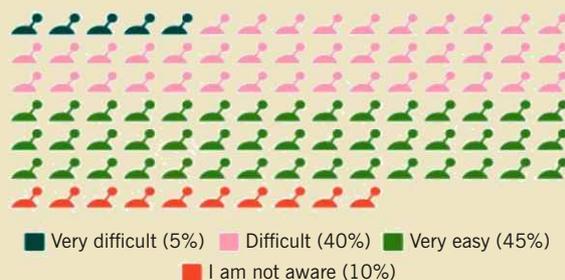
What type of staff related incidents did your organization experience in the year 2016?



In your opinion, what do you think contributed to the breach experienced by your organization in the year 2016?



In your opinion, how difficult do you find it to convince Executive Management to invest in security Control



1ST QUARTER MEETING OF NeFF



FRAUD OUTLOOK 2017



Fraud Outlook 2017

2016 has experienced new dimension in electronic fraud occurrence with 19,531 fraud occurrence. The rising transformation and migration of payment system into the mobile platform channels is expected to lead to consistent increase in mobile fraud. As various mobile products and services are being developed, there is need for proper risk assessment.

Forecasts for 2017

Digital Currencies

With the increasing wave of disruptive technologies within the financial system, the industry must brace up for digital currencies related fraud.

Economic situation:

The current economic situation in Nigeria where job losses and inflation rate are on the increase, more people may be driven into fraudulent acts. Disgruntled and ex-staff may serve as resource for committing fraudulent activities.

Potential Mitigation

Internal palliatives

Mobile phone related fraud vis-a-vis SMiShing, sim swap etc calls for a more drastic solution from the industry. With the regulator's continued engagement, the financial industry must brainstorm on the implementation of some internal palliatives to this pending when the telecom industry will be ready for us.

BVN Watchlist Framework

The industry needs to review the existing BVN framework. The existing framework today allows a fraudster to commit fraud in Bank A and continue normal business with Bank B. Some are even bold enough to commit more than one fraud while still in Bank A. Since the beneficiary bank has not lost money, the bank may or may choose not to watchlist the customer. The revised framework SHOULD allow for the defrauded bank to be able to put such customer on the watchlist irrespective of where he/she banks. Such fraudster should also be denied access to electronic transactions banking services henceforth.

Fraud Desk Framework

There are operational issues surrounding how some specific requests are treated within the fraud desk community. The fraud desk framework will empower individual fraud desks to take necessary actions in certain situations, thereby increasing collaboration in the industry.

Collaboration of the banks' fraud desk and coordination by NIBSS: Since the fraudsters always ensure cooperation and collaboration in the case of coordinated attacks, the only solution is to ensure collaboration among the banks.

The continuous improvement on the Central Anti-Fraud Solution will play a major role in the reduction of fraud. Although, individual banks have their in-house Anti-Fraud monitoring tools, the Central Anti-Fraud System (HEIMDALL) has also played significant role in flagging fraudulent transactions to the tune of N118m in the course of the year 2016. Confirmation of fraud alerts, fine-tuning the system and tweaking the rules to accommodate prevalent fraud trends are expected to improve the system performance and enhance its learning.

Awareness:

The industry should, as a matter of urgency, embark on a massive awareness programme. Many customers easily fall cheap for various social engineering schemes. The industry needs to identify avenues or channels with wider coverage and reach to the populace.

SECURING THE NIGERIAN PAYMENT SYSTEM: CHANGE BEING THE ONLY CONSTANT

By Babatunde Chukwuma Ajiboye

Profile: Babatunde is a Manager with the Shared Services Office in the Central Bank of Nigeria. He also doubles as the Secretary of the Nigeria electronic Fraud Forum (NeFF).

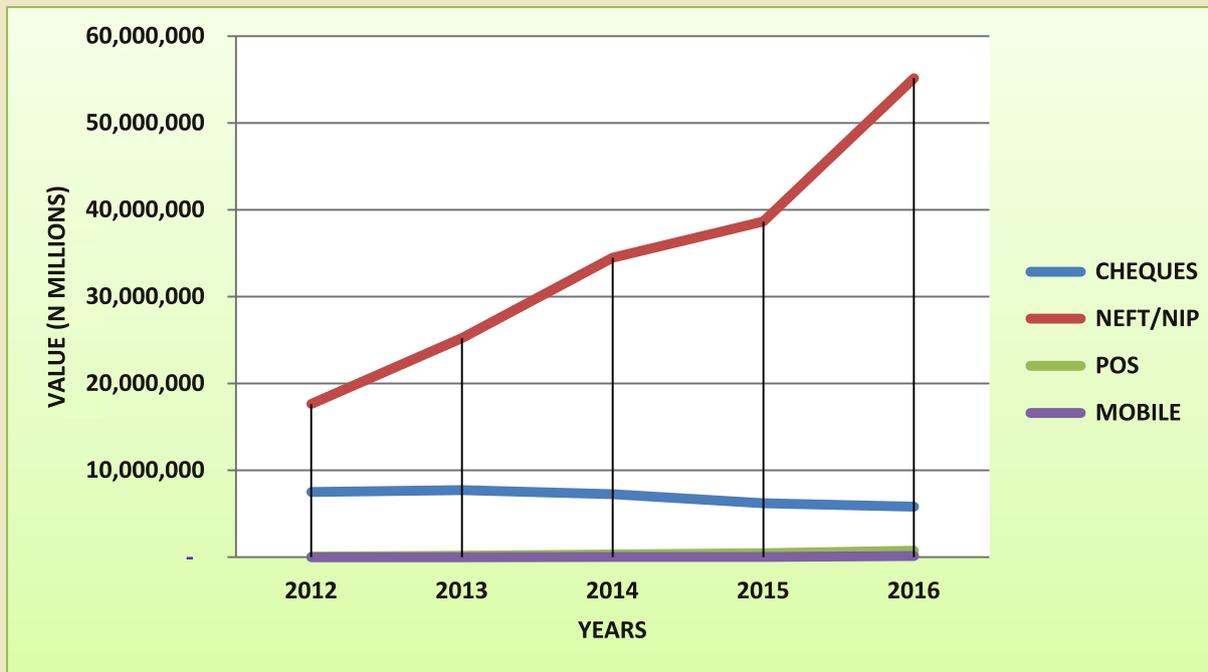


Like every system known to man, the payment system in Nigeria has evolved over the years from basic methods of exchange which barter represents, to a reliance on technology in creating one of the best and most secure payment platforms known to the world today.

The retail payments system in Nigeria can thus be defined along the following channels which help in facilitating;

1. Purchase of Goods and Services: One-time payment for goods or services using a variety of payment instruments, including cash, cheques, debit cards, credit cards or prepaid cards.
2. Bill Payments: Payments for previously acquired or contracted goods and services for which payment can either be recurring or non-recurring. Examples include utility, telephone, mortgage/rent and medical bill payments.
3. P2P Payments: This involves the transfer of value from one consumer to another. Nigeria has seen an upward increase in the use of electronic person-to-person payment systems.
4. Cash Withdrawals and Advances: The use of retail payment instruments to obtain cash from bank branches and Automated Teller Machines (ATMs). Consumer withdrawals from their bank accounts using the Personal Identification Number (PIN) based payment cards to withdraw cash at an ATM.

The growth in the use and adoption of the above channels are evidenced by the table below, which shows how since 2012, the payments system in Nigeria has deepened;



The impact of security in these retail payments which now leverages on technology, has great consequences on public confidence and acceptance of payment instruments. It therefore was no surprise that, as one of the strategic pillars in securing the Nigerian retail payments system, the Nigeria electronic Fraud Forum (NeFF) was created in December, 2011.

NeFF was set up with the following objectives;

- To educate and inform all banks and other stakeholders on various electronic fraud issues and trends (both locally and globally)
- To facilitate the proactive sharing of fraud data/information amongst banks and service providers, to enable prompt responses to prevent and/or limit fraud losses and;
- To formulate cohesive and effective fraud and risk management strategies, and defining key requirements in relation to e-payment security on behalf of the industry.

The NeFF has of course used its platform to advance fraud mitigating policies like the Two factor authentication for internal banking processes, Regulation of card present fraud in Non-EMV environment and the Creation of fraud desks for effective e-fraud control. However, these measures need to be supported still with additional information security compliance that will tackle the threats that emerge as a result of the ever increasing changes in our payments system.

Securing the payment system in Nigeria has equally evolved from basic signature verification to complex security algorithms. However, the payments industry cannot possibly wave a magic wand to instantly solve all the security challenges we face. The answer would seemingly lie with a detailed analysis of all systems, processes and practices in place.

The question basically is how these new systems will deal with the issues of information security, money laundering and terrorist financing. The belief is that information security will continue to be an area of increasing concern to consumers, merchants, financial institutions and regulators in the coming years. Mark Fajfar et al, in their remarks prepared for The International Monetary Fund (IMF) Institute Seminar on Current Developments in Monetary and Financial Law, defined the basic levels of information security threats to include;

- That an individual will break into an electronic system in order to initiate unauthorized transactions on another individual's legitimate account, thereby stealing money.
- That an individual will steal customers' personal data, enabling the wrongdoer to set up illegitimate credit card accounts, bank accounts and other accounts – this is called identity theft.
- That an individual will attack or corrupt the data in the electronic system, either as vandalism or to extort money from the sponsoring financial institutions.
- That an individual will take advantage of the convenience and speed of the electronic system to mask illegitimate or illegal transactions – i.e., money laundering.
- That an individual will take advantage of the efficiency of the electronic system to facilitate funding of illegal activities, particularly terrorism.

Here the author cannot but agree with Mark Fajfar et al on the information security compliance steps to be taken in order to ensure that security of our payment system always remains resilient against imminent modern day threats. These steps include;

1. Security efforts must be “risk-based,” meaning that the company or financial institution must evaluate the threats to its information assets and concentrate on counteracting those that involve the highest risk.
2. Security efforts must be continuous. Compliance measures must be periodically tested, re-evaluated and modified to maintain their effectiveness. For example, errors may arise when a company or institution hires new employees, opens a new branch or enters a new business without updating its security controls to account for the new activities. Similarly, when employees leave, branches close or businesses wind-up, the information systems devoted to those past activities must be properly

cleansed.

3. Security efforts must cover the entire organization. Specific practices and the compliance culture must be overseen by the Board of Directors and extended to the lowest level of employee with operational responsibility. In particular, the compliance program must take into account that “human error” (whether negligence or willful misconduct) is the greatest threat to information assets. There must be rigorous training of employees.
4. Information systems must permit later auditing in order to detect efforts to alter or compromise information. Just as the “black box” is crucial to the investigation of a plane accident, there must be some means of reviewing how the information systems have actually been used, and what they have been used for. If not, the organization will be unable to determine whether information security breaches have occurred, let alone determine how to prevent them.
5. Third-party service providers must be held to the high standards. Many information system tasks are subcontracted (or “outsourced”) to third party service providers which are able to perform these services more efficiently. However, the responsibility for information security cannot also be subcontracted. On the contrary, these arrangements require close attention to the subcontractor's performance. In particular, the subcontractor should be subjected to a written obligation that it would meet all of the information security compliance standards of the hiring company or financial institution

Another issue of thought is the security of mobile payments. Mobile has become a major channel of expression, particularly in the 21st century. Due to its ubiquitous nature, the mobile phone has pervaded our everyday lives, increasing dependability and reliance. Today, very few (if any at all), can do without this piece of technology as a channel for payments.

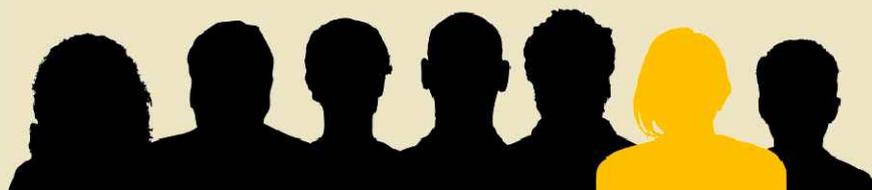
The European Central Bank in its draft document for public consultation (November, 2013) made some recommendations for the security of mobile payments which were based on five guiding principles.

1. Firstly, Mobile Payment Solution Providers (MPSP) should identify, assess and mitigate the specific risks associated with providing mobile payment services.
2. They should give due consideration to, and factor in, risks resulting from reliance on third parties, such as Mobile Network Operators (MNOs), Trusted Service Managers (TSMs) as well as Secure Element and other component manufacturers.
3. Actors involved in the provision of the mobile payment service (e.g. MNOs, TSMs)

should define relevant procedures for collaborating on incident monitoring, handling and follow-up, including security-related customer complaint management.

4. They should also consider the mobile device as inherently vulnerable to security issues in view of the speed of technological advances, the evolution of security threats and fraud mechanisms.
5. Consider the assessment of the relevant risks to be encountered in the introduction of new ways of effecting mobile payments.

Considering the growing trend of adoption of mobile payments in Nigeria and more importantly the role of customer awareness, education and communication, I believe the aforementioned recommendations should be adopted.



The provision of a secure channel for ongoing communication (including reporting of suspected fraudulent transactions, suspicious payment incidents and anomalies in the course of payment transactions) and response has become imperative. This secure channel can be created jointly by the payment industry and utilized as a shared service for optimal cost utilization and effective customer engagement. Alerts on significant emerging risks should also be provided by this secure channel for example, warnings about attempts by potential fraudsters to extract customers' personal financial information.

It is important that customers of e-payment channels are made to understand that at a minimum, they need to protect their passwords, PIN codes, personal details and other confidential data. Customers also need to be constantly informed about updates to security procedures regarding payment channels.

Security in payments will be a never ending challenge in either Nigeria or the rest of the world. Conversations around this therefore, must continue to be encouraged. NeFF as a platform for this engagement has always been available; the Payments Industry is encouraged to continue in its support of the Forum so as to continue to benefit from the results thereof.

References

<https://www.imf.org/external/np/leg/sem/2004/cdmfl/eng/faj.pdf>

<https://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf>

A CHANGING PAYMENTS ECOSYSTEM: THE SECURITY CHALLENGE

By **Olusola Odurinde** Bsc, MBA, ACIB, ACA

Introduction

Payments and Payment Systems have evolved through the history of the human race, starting out at the most primitive level of a simple exchange of goods, or trade by barter. **Over the years**, more ways of paying for goods and services have evolved. Currently, there are more ways to pay for items than at any other time in history. Of course, that is assuming you have the money, credit, or random valuable commodities to back it up.

Disruptive technologies in the form of digital currencies are also emerging in the payment eco-system. Digital currencies such as bitcoin are created and held electronically, and are increasingly being used to consummate transactions. These digital currencies are disruptive in nature because they are not regulated.

According to Wikipedia, a **payment system** is regarded as a “system” because it employs methods to substitute physical money for items such as cheques and letters of credits. In recent years, the electronic information age has led to the development of a vast number of new electronic payment methods that include electronic banking cards, electronic fund transfer systems and direct transfers, and internet/ systems, among others.

Retailers, merchants, financial institutions and payment processors face daunting new challenges and complexity in payments processing across multiple fronts. These fast-changing dynamics include:

- High expectations among omni-channel customers.
- Demands for multiple, relevant payment options.
- Rapid growth in mobile and card-on-file solutions.
- Ever-changing security, privacy and fraud risks.
- Increasing complexity in managing a multi-channel payment ecosystem.
- New chip-enabled card requirements to comply with the EuroPay, MasterCard and Visa (EMV) standard for card-present US transactions

Key challenges in payment processing

Payments are a crucial steps in the customer experience journey. While merchants have made great strides in helping to guide the consumer's path to purchase with personalized marketing and mobile-friendly websites, payments processing presently, is a potential stumbling block that can derail a superior customer experience. Payment processing poses a few challenges to merchants and billers as noted by IBM. These challenges include the following:

1. Satisfy customer demands for payment options.
2. Security, privacy and regulatory requirements.
3. Minimize complexity across the payments ecosystem.

Each of these challenges is further explained below.

1. SATISFY CUSTOMER DEMANDS FOR PAYMENT OPTIONS

Offering customers a wide variety of payment options is a prerequisite for long-term success. Today's demanding omni-channel consumers expect a seamless transaction processing across multiple touch points, including e-commerce transactions over smartphones and tablets, and cashless in-store payments through smartphones. For most retailers, the top objective in all aspects of commerce, including payments, is to deliver a cohesive and rewarding omni-channel experience for the customer. Of the many moving parts in the customer journey, payments is among the most difficult to handle, and its wrong handling is a significant risk to the security and privacy of customer data.

2. SECURITY, PRIVACY AND REGULATORY REQUIREMENTS

Despite heavy investments in Payment Card Industry (PCI) compliance and security systems, the threat to the privacy of customer and payments data continues to increase. High-profile data breaches are now common and pose significant risk to data security and privacy of customer data. The number of fraudster is increasing by the day, that for every harmless legitimate application, there are hundreds of pieces of malware, exploits or viral code. However, internet technology remains neutral in this conflict, as it only helps get both the bad and good guys on the network; therefore, technology is not the problem, but people.

The security of the processes in consummating online transactions can be reviewed from this perspective “how secure is the computer device being used” and “how secure is the channels via which data is being transferred”.

Whenever a new payment technology is introduced, new challenges are sure to emerge as well. In considering the mobile payment system, most of the security concerns associated with it are either identical or very similar to the ones already encountered and managed by the payment industry with the payment security responsibility against threats shared by all stakeholders.

The most important safety concern is the protection of personal data that either are stored in, or flow through a mobile device. These data include – payment account numbers, PINs,

security codes, passwords, etc. The exposure of sensitive customer information over a wireless network can leave the customer vulnerable to theft.

Similar to personal computers, remote payments usually depend on software-based security that is vulnerable to many threats as a result of the open nature of the mobile platforms. The mobile has the capability to execute all types of applications like instant messaging, social media access, games and even online banking and trading. This versatile ability to execute applications extends to viruses and malwares as well. This is potentially a lucrative niche for developing mobile based virus and antivirus respectively, which is gradually evolving.

The key differences and challenges:

- **Software:** The PC-based eCommerce is based almost entirely on standardized Web software on Microsoft Windows, MacOS or Linux operating systems, but different when compared to the mobile, since different platforms are still evolving rapidly with frequent changes to the operating systems and a wide variety of underlying hardware architectures.
- **Internet connection:** PC is limited to the amount of time the computer is switched on and connected to the Internet, but with smartphones, that window of exposure is greatly increased, as the phone is switched on even while sleeping.
- **Scams:** Comparable to the e-mail phishing attacks that trick victims into divulging personal information via a computer, scammers can easily extend these tactics to the mobile channel. In fact, since the mobile device can also communicate via voice, text or data, fraudsters suddenly find that they have even more avenues to the conduct attacks. We are starting to see such PC-style attacks make their way into smishing (SMS text phishing) and vishing (voice phishing).

It is obvious there are major issues that must be addressed to ensure the safety of mobile payments. The industry stakeholders who understand the potential value for merchants and customers, have already taken several steps to remedy these concerns.

All entities under the payments industry that process, transmit or store payment information are being mandated to adhere to the Payment Card Industry Data Security Standards (PCI DSS). Also, the Payment Application Data Security Standards (PA-DSS) applies to software applications used to accept payment data.

In addition, existing fraud mitigation processes and tools are applicable to the mobile channel as well. As more information is made available on mobile devices (e.g., location information), the potential to improve systems monitoring and review improves.

While the industry constantly updates security measures, it is important that merchants and service providers keep their consumers up to date. Staying ahead of possible attacks will be critical in safeguarding personal information.

Tips to Ensure Secure Payment Processes

Education and awareness is a critical element to secure mobile payments. With new payment capabilities, mobile phones will carry more value than the cost of the phone itself, and will need to be treated with extra caution. Put simply, consumers will need to start treating their mobile phones with the same level protection they give to their wallets.

Consumer Mobile/Online Security tips:

- Use some form of password or passcode to access the payment application on the phone.
- Never share confidential or private information, especially if you did not initiate the communication. If you are in doubt, call your Issuer.
- Ensure that any text messages you receive from your financial institution originated from the correct phone number or short code.
- Only download mobile applications from trusted sources.
- Report to the financial institution immediately, if your phone containing your financial information is lost or stolen.

Other security checks for online payment transactions include:

- Always check the keyboard connector for any hardware key loggers.
- Configure the network connection or watch the administrator closely when he is configuring it.
- Ensure all traffic are being routed through secured link SSL/HTTPS (Hyper Text Transfer Protocol Secured) i.e. pad lock should appear on the address bar
- Always login to the merchant you want to bank with, and double check the SSL (Secure Socket Layer) certificates so as not to be feeding an SSL proxy certificate.
- If you want to be very sure, enter the merchant IP address directly, so that you are not fooled with DNS requests.

- Also ensure to delete cookies on the explorer from the OS, if the system is for public use.
- Also set history in explorer to zero so that your previous page transaction will not come up.

What do they do with the stolen information?

Once they have your information, it can be used in the various ways for Bank/Finance/Credit card fraud:

- They may open a new card account in your name and use the card to settle their bills.
- They may change the billing address so you do not get statement.
- They may create counterfeit check using your name or account number.
- They may open a bank account in your name and write a bad check.
- They may clone your card and make electronic withdrawal.
- They may also take loan in your name.

How do you find out if your identity has been stolen?

The best way is to monitor your account and bank statement frequently and your credit report on a regular basis. Hence, you may be able to detect early enough and reduce the damages caused by identity theft.

Preventing Spoofing

- Be extremely skeptical of e-mail received from someone you do not know.
- Keep separate passwords for each online account so that if one is stolen, it will not provide access to the others.
- Do not click on a link embedded within any suspicious e-mail.
- Call your financial institution to verify your account status before divulging information.
- Do not respond to any request for financial information that comes to you via email
- Update your virus software weekly to ward off e-mail borne virus
- Ensure you are working from the most current version of browser and operating system

to prevent possible attack.

- Check your online account balance regularly.
- Ensure to install and run firewall on your system.
- Do not download unknown attachments, software update or application via an e-mail link.

3. MINIMIZE COMPLEXITY ACROSS THE PAYMENTS ECOSYSTEM

Continuous growth in consumer expectations and complexity of the payments ecosystem have made it more difficult than ever for merchants to manage multiple payment channels. Looking ahead, the uncertainty that surrounds new technologies, payment methods, regulatory requirements and security risks leave many players with an uneasy task of making tactical decisions and projecting strategic direction.

Ensuring PCI and other security obligations become even more costly and challenging as new channels are added, while at the same time, merchants are under increasing pressure than ever before, to ensure that payment-related data are secure and compliant with relevant regulation and standards.

Given the ceaseless complications, many merchants are looking to transition from in-house payments management to a proven cloud based payments platform that can deliver simplicity, security and visibility at levels that are extremely difficult to achieve in today's typical payment systems.

Conclusion:

Technological innovation in the financial services industry as well as trade & commerce, is driving the adoption of electronic payment systems. Electronic payment systems enable us to perform transactions electronically in a fast and easy manner, but also come with their attendant risks, especially security issues. To effectively deal with security issues in the electronic payment systems, it is important for all stakeholders to come together regularly to review and put in place frameworks that will make the system more secured especially in the current trend in the emergence of disruptive technologies such as bitcoin and cloud computing. The Nigeria Electronic Fraud Forum (NeFF) is actively and effectively playing the role of a facilitator by organizing regular meetings of electronic payment stakeholders. This Forum has significantly improved security of the electronic payment systems in Nigeria.

References

- Managing the Risks and Security Threats of Mobile Payments by Bill Gajda February 2011, <http://www.pymnts.com/company-profile/2011/managing-the-risks-and-security-threats-of-mobile-payments/>
- <https://www.sybrin.com/good-idea/>
- <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZM12388USEN>
- Hack No More; Internet Security Attacks and Defence by Aliyu Ahmed Ahmed.
- Ethical hacking and countermeasure by EC-Council
- <http://docplayer.net/11187454-The-payments-ecosystem-security-challenges-in-the-21st-century.html>
- <http://www.experian.com/assets/data-breach/white-papers/experian-data-security-payments-ecosystem-2015.pdf>

UNVEILING OF THE NeFF 2015 ANNUAL REPORT



A CHANGING PAYMENTS ECOSYSTEM: THE SECURITY CHALLENGE

By Ochanya Dan-Ugo

Profile: Ochanya is currently the Chief Risk Officer (CRO) of Unified Payments®. A Visa International trained manager in Risk Management. She has attended several trainings on payment card including American Bankers Association, School of Bank Card Management, Emory University, Atlanta USA. Prior to this period, Ochanya was a Chief Superintendent of Narcotics and a Principal Staff Officer, Records Management (Intelligence), National Drug Law Enforcement Agency. A place she worked for fourteen years where she gathered her investigation and Intelligence experiences.



She is a Certified Protection Officer (CPO), a certification awarded by the International Foundation for Protection Officers (IFPO); a Certified Risk and Compliance Management Professional (CRCMP); certified in Management of Risk (M_O_R) (Foundation and Practitioner levels) and undergoing her certification process for Certified Protection Professional (CPP) by American Society for Industrial Security (ASIS), the highest certification in security profession.

Ochanya holds a Bachelor of Arts Degree from the University of Jos; Post Graduate Diploma, Education: a Post Graduate Degree in Humanitarian and Refugee Law from the University of Lagos; certificate in Bank Card Management and an alumna of the Lagos Business School and the Metropolitan School of Business and Management, United Kingdom. She served as a member of Visa Risk Executive Council for the Sub-Saharan Africa from 2012 – Date. She joined the services of Unified Payment Services Limited in November, 2005.

The way we pay is changing dramatically. How consumers pay, and what they pay with, is changing. The growth of contactless, mobile and other new payment options are forcing the traditional payment paradigm to evolve. For example, people are beginning to use their smartphones for every kind of formal and informal transactions — to shop at stores, buy items online, and carry out fund transfers. The way people pay, are now being driven more by how they live and less by what is in their wallets. This new payment ecosystem will introduce a whole new level of convenience and security for consumers and tremendous benefits for retailers.

Evolution can be slow, but we are closer to a new payment paradigm engineered by disruptive technology. At the heart of these changes in how we pay, are thousands of companies competing and collaborating to facilitate transactions. To understand why the payments industry has faced so much disruption in such a short time, there is just one key thing to understand: Payments is about transferring information from one party to another, and nearly every stakeholder in the industry benefits when that process runs on digital rails.

The number of retailer touch points to engage with consumers is growing, and new experiences are constantly being introduced. The use of deep data science and artificial intelligence (AI) is paving the way for more contextual promotions, virtual reality technologies are becoming more affordable for virtual product demos, and customer

experience expectation is driving the need for a more seamless checkout process.

Most of this disruption is driven by the concept of frictionless payments, which has now transformed into customer engagement and how to unravel the entire consumer experience, well beyond specific payment technologies. Consumers' acceptance and use of multiple devices for commercial activities have grown at a rapid pace. Technology such as voice, buy buttons, home automation and other connected devices led to multiple engagement models without a dominant infrastructure, but rather, an ecosystem driven by consumer data, customer experience and the use of technology.

These evolutions bring new opportunities and new risks. The payment transaction can be more exposed to risk because, several parties are involved in performing the payment service. This may worsen if important services are outsourced to potentially unregulated third parties without clear lines of accountability and oversight, or which are located abroad. This multiparty transaction environment is conducive to exploitation by fraudsters using both technological and sociological attacks, if the appropriate protection mechanisms and accountability controls are not established throughout the payment ecosystem. With careful planning that includes all the stakeholders, processes and technologies involved, the opportunity exists to make security an intrinsic element of all payment systems.

Risk for the participants in the payments ecosystem depends on the role of the entity user, network or communication provider or payment service provider. The table below provides a snapshot of the types of threats and risk that may come into play across the payments environment among its principal players.

Target Type	Vulnerability	Threat	Risk	Counter measures
User	Over the Air (OTA) transmission between phone and Point of Sale(POS) (NFC reader)	Interception of Traffic	Identity Theft, Information disclosure, replay attacks	Trusted Platform Module(TPM), secure protocols, encryption
User	Inadvertent installation of malicious software on mobile phone by user	Downloaded application intercept of authentication data	Fraudulent transactions, provider liabilities	Authentication of both user (PIN) and application (digital signature by trusted third-party), TPM
User	Absence of two-factor authentication	User masquerading	Fraudulent transactions, provider liabilities	Two-Factor authentication

Target Type	Vulnerability	Threat	Risk	Counter measures
User	Changing or replacing mobile phone	Configuration and setup complexity	Reduced adoption of the technology, "security by obscurity"	Simplified user interface, security parameters in TPM set by trusted party
User	Smartphone internet and geolocation capabilities	Malware on mobile device; poor data protection controls at merchant/payment processor	Data disclosure and privacy infringement; profiling of user behaviour	User control of geolocation features, cryptographically supported privacy, trusted platform module, vetted authorization and accounting
Service Provider	POS system accepts OTA transmissions	Malicious party floods POS system with meaningless requests	Denial of Service (DoS)	Request filtering at reader based on mobile device- reader relative geometry
Service Provider	POS devices are installed at merchant premises	Masquerade attacks; tampering with POS	Theft of service, replay, message modification	POS vendor vetting, message authenticators, vetted authorization and accounting
Service Provider	Lack of Digital Rights Management (DRM) on mobile device	Mobile device user illegally distributes content; e.g ringtone, video, games, etc	Theft of Content, Digital piracy, risk to provider for digital rights infringement, loss of revenue to content provider of merchant	DRM incorporated in smartphone Trusted Platform Module (TPM) design, cryptographically supported DRM
Service Provider	Weakness of Global System for mobile communication(GSM) encryption for OTA transmission; SMS data in clear text on mobile network	Message modification, replay of transactions, evasion of fraud controls	Theft of Service or content, loss of revenue, illegal transfer of funds	Strong Cryptographic protocols, SMS message authenticators, encryption

While the overall payment experience have not been transformed into something completely frictionless, contactless payments produce significantly less “friction” at the POS than traditional payment methods. If you have ever felt the ease of stepping out of an Uber car without having to pull out your wallet, or experienced the joy of PayAttitude

at any mall in Nigeria, you will appreciate the paradigm. More mobile and contactless payment options are making the consumer payment experience better and better.

The payments ecosystem is being redefined. In a world where new technology becomes available and commoditized quickly, customer experience and agility will drive the transformation of commerce and brand interaction. It may take time before we say, “goodbye” to our cash and plastic cards, but mobile payments today look a lot like the change we so desire. The snowball has started to roll down the mountain and for those who are willing to step into the payments space; it means a massive opportunity for positive transformation.

References:

<http://www.fit-pay.com/the-changing-payment-ecosystem/>

<http://www.businessinsider.com/the-payments-ecosystem-everything-you-need-to-know-about-the-key-players-and-trends-in-the-payments-industry>

<http://www.pymnts.com/news/payments-innovation/2016/payments-2016-the-year-of-the-ecosystem-redefined/>

<http://seekingalpha.com/article/4003818-complex-payment-ecosystem>

<https://www.isaca.org/Groups/Professional-English/pcicompliance/GroupDocuments/MobilePaymentsWP.pdf>

BLOCKCHAIN TECHNOLOGY: OPPORTUNITY, RISK AND IMPLICATIONS FOR FINANCIAL INSTITUTIONS & REGULATORS

By **Osita Nwanu**, CISA, CISM, CEH, OCP

Head, Systems Control & Business Continuity Management, First City Monument Bank Limited

Profile: Formerly Head, Systems Control & Business Continuity Management, First City Monument Bank Limited



Today, we wholly rely on intermediaries like banks, insurance companies, government agencies, card and switching companies, ecommerce merchants, money transfer operators, and so on to establish economic trust.

Furthermore, imagine some kind of massive, global, decentralized platform supported by millions of computers that could store, transact, exchange and manage every type of assets in digital form; cryptographically secured, devoid of any intermediary and available to everyone.

Blockchain technology—originally developed for Bitcoin—is evolving into several areas—financial services, healthcare, insurance, government, legal, manufacturing and tourism. It promises to make trusted intermediaries either obsolete or transform them.



In the coming years, banking services may begin to run on top of Blockchain technology and it is important we examine the opportunities that Blockchain presents as well as the regulatory, legal, security and technological risks that may inhibit its widespread adoption in Nigeria.

What is Blockchain Technology?

Blockchain technology is a peer-to-peer decentralized ledger initially developed for Bitcoin digital currency. Major features of the technology include no central point of control, high availability, robust data integrity, transparency and network-wide consensus.

Information held on the Blockchain technology is underpinned by millions of computers—that validate and relay transactions—concurrently, thereby, making such information retroactively immutable and accessible to anyone via the internet.

Types of Blockchain Technology

1. Public Blockchain

Public Blockchains are decentralized open source platform that is accessible to everybody. Bitcoin, Ethereum and OpenBazaar run on a public blockchain technology.

2. Private Blockchain

Private Blockchain is a close-ended decentralized platform that is accessible only to approved members of a group or consortium. Ripple Transaction Protocol—which enables banks to move money across borders without the need of correspondent banks—and R3's Corda Banking Blockchain are examples of a private blockchain.

Some leading banks are embracing private Blockchain technology to reengineer and digitalize their operations, by taking advantage of cost savings and process efficiency associated with Blockchain technology.

The Role of Smart Contracts

Smart contract is a computer logic—embedded in a Blockchain—designed to define, self-verify and execute the terms of a contract. It offers a flexible way to exchange money, property, shares, or anything of value in a transparent way, devoid of conflict and without intermediaries.

Real world use of smart contracts is gaining traction in Africa. For instance, Bitland—an African Blockchain technology startup—is using smart contracts to enable individuals and groups in Ghana, to survey land and record title deeds on their Blockchain—providing a permanent and auditable record.

Expanded Cloud Service

Blockchain-as-a-Service (BaaS)

In a BaaS, customers can create smart contract enabled private Blockchain easily, without having any prior experience in Blockchain technology. Microsoft and IBM are some of the big tech companies offering cloud based Blockchain service

Opportunities

Process Efficiency	Blockchain technology ensures standardization, simplification and faster execution of complex banking processes.
Increased Revenue & Cost Optimization	Participating Banks in a Blockchain arrangement can significantly reduce operational costs and increase revenue by eliminating intermediaries.
Autonomy	Consumers of the Blockchain services can own and control the digital assets associated with them.
Availability	On the blockchain, data are duplicated many times and copies maintained across world-wide network of systems. This ensures that data will be available at all times.
Compliance & Audit	AML and KYC practices can be adapted to Blockchain technology increasing monitoring and analysis effectiveness.
Data Accessibility	Regulators and relevant government agencies could have direct online real-time access to Blockchain-based banking transactions, increasing the effectiveness of their supervisory function.
Data Integrity & Security	Data stored in the Blockchain ledger is digitally secured and tamper proof.
New Business Models	Blockchain-based technology is opening entirely new opportunities, including machine-to-machine payments, one click online commerce, and decentralized autonomous organizations.

Potential Risks

Interoperability	Integration could be the biggest hurdle for Blockchain technology adoption as multiple platforms are created by different consortia to address the same business problem.
Vendor Lock-in	Blockchain vendors want customers locked into their platform, thereby, giving the vendors pricing and control power. Additionally, this could lead to high switching costs, should the consumer decide to patronize the services of another Blockchain vendor.
Cyber-Attack & Fraud	Blockchain platforms are constantly attacked and are subject to security exploits. For example, in the third quarter 2016, Ethereum - a blockchain platform - was attacked by cybercriminals resulting in the loss of \$60 million USD. Additionally, Denial of service attacks could threaten the blockchain infrastructure by overwhelming it with excessive data, thus, preventing the normal transaction processing process.
Instability	Most blockchain technologies are experimental and untested.
Regulation & Legal	Policies, legal framework and best practices that will provide safety and stable environment for Blockchain technology, including protecting consumers from unsafe implementations are lagging.
Loss of Agility	In a Private Blockchain arrangement, consensus is needed among members of the consortium to make changes or adjustments. The time spent to reach an agreement could be spent implementing the decision and responding quickly to business exigency.

Conclusion

Blockchain technology is widely touted as the next disruptive innovation that will potentially change the way businesses operate, and as well, provide avenue for entirely new business opportunities. Furthermore, to maximize the benefits of this emerging technology, a principle based regulation will be required to ensure safe and stable implementations.

Regulators will not effectively regulate what they do not know. Consequently, they will need to collaborate with financial institutions, to understand, examine, educate, and promote best practices that will also address regulation, legal and interoperability challenges to enhance Blockchain technology adoption in Nigeria.

References

1. Vasanth Raval; "Information Ethics in the Mid-21st Century," ISACA Journal Vol. 6, 2016
2. Lester Coleman; "What Role Does Government Play in Blockchain Technology's future?," 12 February, 2017, <https://www.cryptocoinsnews.com/what-role-does-government-play-in-blockchain-technologys-future/>
3. Vitalik Buterin; "On Public and Private Blockchains," 7 August 2015, <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>
4. Jamie Redman; "Bitland: Blockchain Land Registry Against 'Corrupt Government,'" May 26, 2016, <https://news.bitcoin.com/bitland-blockchain-land-registry/>
5. *Jacob Parks, J.D.*; "Tracking The Intangible: How Fraud Examiners Are Busting Bitcoin Fraud," <http://www.acfe.com/fraud-examiner.aspx?id=4294980488>
6. Andrew Quentson; "What is Ethereum?" 19 February, 2017, <https://www.cryptocoinsnews.com/what-is-ethereum/>
7. Rob Marvin; "Blockchain: The Invincible Technology That's Changing the World," February 6, 2017,

NeFF END OF THE YEAR RETREAT

Transcorp Hotel Calabar, November 2016



MMM PONZI

ANALYSIS OF FINANCIAL IMPLICATIONS IN THE NIGERIAN BANKING SYSTEM



PREAMBLE

The Nigerian version of Mavrodi Mundial Moneybox Ponzi scheme, popularly called MMM-Nigeria was launched in November 2015 through a hosted website (<https://mmmoffice.com/>). It was a scheme that promised a return of 30% per month on investment made in the scheme. The MMM scheme had a remarkably different modus operandi from previous schemes that had operated in the country in times past. For the MMM scheme, instead of having a central pool where investors put in their money, a peer-to-peer methodology was employed where investors (Helpers) actually pay money directly (Pledge Help – PH) to another member of the scheme who has requested to Get Help – GH. After 30 days, the Helper who PH-ed would be entitled to GH (Get Help) of the amount he had previously given out, along with a 30% extra. As at December 2016 (one year after the scheme started in Nigeria), it is estimated that MMM had over 2.5 million registered Nigerians in its scheme.

This Report is aimed at presenting the financial facts of MMM Ponzi Scheme as it relates to the banking industry in Nigeria from the point of view of the Central switch.

The Nigeria Inter-Bank Settlement System (NIBSS) PLC is the Central switch for the financial sector in the country. Majority of the account-based inter-bank transactions either pass through NIBSS for processing, or NIBSS has visibility of the transactions through its industry Anti-fraud System – HEIMDALL.

The figures rendered in this report are strictly based on the inter-bank transactions of the 14 commercial banks that are currently live on HEIMDALL, and all other Commercial Banks and OFIs (Other Financial Institutions) that are on the NIBSS account-to-account platform called NIP (NIBSS Instant Payment).

LIMITATIONS

Due to the fact that NIBSS can only see transactions that are of Inter-Bank nature, this report does not capture the intra-bank MMM transactions. For a full and complete analysis (that includes Intra-Bank transactions) to be made, there is a need to have all transactions (both intra-bank and inter-bank transactions) aggregated to a central point. The usefulness of such a move goes beyond this particular analysis. It would form the bedrock for many more industry-level analysis. Such ability would afford the CBN the opportunity to get accurate, full and complete information about the industry. Such reports can be relied upon to make far reaching decisions to assist the nation.

This report also does not take into account those who invested in the MMM Ponzi scheme using the Bitcoins option (investing through the Bitcoins attracted a premium of 50% ROI).

Lastly, this report analysed only the last six months of the scheme. i.e June 2016 to December 2016

THE FREEZE

On December 13th 2016, Nigerians woke up to the news that the MMM website had frozen the ability to “GH” (Get Help). This meant that those who had put in money, were not able to take out neither their promised interest nor their invested capital. Promoters of the scheme promised that investors would be able to get their money by January 14th 2017. The said date has since passed without people being able to get their investment funds back. The MMM Ponzi scheme is now officially considered crashed!

THE FACTS

Between June 2016 and December 13th 2016 which forms our review time frame, over 460,000 (four hundred and sixty thousand) MMM transactions of Inter-bank nature were carried out to a tune **28.7 billion Naira**.

To put this amount into perspective, the 2017 budget for the Defense headquarters is 4.7 Billion Naira. This implies that the amount transferred by Nigerians within the MMM Ponzi scheme would have funded the Nigerian Defence HQ almost six times over.

NGN 28.7b
INVESTED IN
MMM NIGERIA IN
6 MONTHS

THE CHANNELS:

Majority of the transfers made by customers of banks that participated in the MMM Ponzi scheme was made through the account-to-account transfer platform. This was followed by the Mobile Channel, and lastly, through the web channels of other transfer platforms in the Industry.

Channels of Transfer by value		
Stream	Value	Volume
MOBILE	188,501,512	2,920
NIP	28,494,406,383	456,652
WEB	66,584,448	1,351
Grand Total	28,749,492,343	460,923

THE BANKS

Customers of Thirty four financial institutions paid out money for investments into the MMM-Nigeria Ponzi scheme. The customers include customers of commercial banks, customers of Mobile Payment Operators and even customers of mortgage banks. By the side are the amounts, in terms of volume and value for each financial institution that money was paid out from:

Less number of banks received inflows of MMM transactions than the number of banks from which outflows occurred.



Value of MMM transactions in 6 months greater than Ministry of Education's Budget by 61%



Amount received by each destination bank			
S/N	Bank	Volume	Value
1	ACCESS BANK PLC	42,018	2,642,339,439
2	ASO SAVINGS AND LOANS	3	90,000
3	CITI BANK	3	357,000
4	DIAMOND BANK PLC	52,911	3,405,960,504
5	ECOBANK NIGERIA PLC	27,976	1,688,089,455
6	FIDELITY BANK PLC	23,987	1,350,813,042
7	FIRST BANK OF NIGERIA PLC	67,813	4,447,387,715
8	FIRST CITY MONUMENT BANK PLC	19,014	1,288,865,211
9	GUARANTY TRUST BANK PLC	90,431	5,395,504,759
10	HERITAGE BANK	3,334	182,963,899
11	JAIZ BANK	97	4,416,700
12	KEYSTONE BANK PLC	5,111	318,385,204
13	SKYE BANK PLC	16,677	993,707,693
14	STANBIC IBTC BANK PLC	8,444	575,365,488
15	STANDARD CHARTERED BANK PLC	1,052	79,373,853
16	STERLING BANK PLC	6,126	392,686,604
17	SUNTRUST BANK	1	28,000
18	UNION BANK OF NIGERIA PLC	9,707	598,427,025
19	UNITED BANK FOR AFRICA PLC	45,007	2,673,438,335
20	UNITY BANK PLC	2,414	157,247,171
21	UNKNOWN	1,167	52,397,448
22	WEMA BANK PLC	5,744	312,250,185
23	ZENITH INTERNATIONAL BANK PLC	31,886	2,189,397,613
	Grand Count	460,923	28,749,492,343

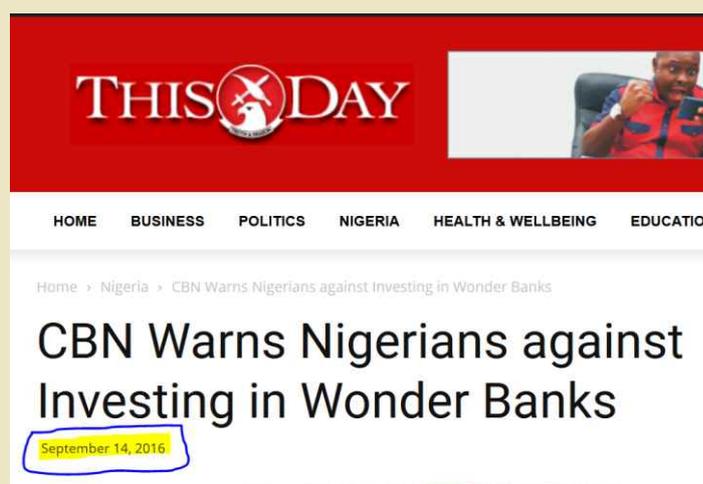
Unknown** Some web transactions were reported without destination bank codes.

MONTHLY CONSIDERATIONS:

MMM followed the usual pattern of PONZI schemes. They continue to build momentum and crash when the maximum amounts are already invested in the scheme. The peak of the MMM investment was in November 2016 where over 13 billion Naira was transferred amongst participants.

MMM Volume and Value by Month		
Month	Value	Volume
June	557,847,291	8,115
July	646,509,555	15,260
August	2,966,390,527	35,753
September	6,176,593,577	79,313
October	1,669,800	26
November	13,596,999,069	227,959
December	4,803,482,525	94,497
Grand Total	28,749,492,343	460,923

In the middle of September 2016, CBN officially warned about the dangers of the MMM Ponzi scheme. The pronouncement of the CBN greatly affected the confidence of participants in October, after the September ending cash-out. There was a vigorous campaign by the promoters of the scheme on social media in October. The resultant effect was seen in November activities of MMM



MOTHER OF ALL LOSSES

By the time the scheme “crashed” (the word the owners prefer to use is “froze”) on December 13th 2016, the amount lost was over **NGN 11.9 bn**. Since the MMM Ponzi scheme is a 30 day cycle before ROI is realized, it means all people who put in money after November 12th 2016, did not get their money out. The system crashed on December 13th 2016.



The amount put into the scheme between November 13th and December 15th 2016 (through interbank transactions) totals over NGN 11.9 bn. This amount was largely not recovered. By the time the system was re-opened again on January 14th, 2017, everyone wanted to cash out and no one wanted to invest. As at the time of this report (March 2017), no one has been able to recoup his/her money.

METHODOLOGY

A staff registered as a participant of the MMM community to understand the modus operandi. One major directive on the MMM platform is the one which tells participants that when they want to Pledge Help (PH), the narration to be used in the transaction is either “help” or “Donation”.

In getting the data, all transactions with the narration “Help”, “Donation” or “MMM” were spooled and analyzed. The spooled records were filtered line by line to reduce the chances of unrelated transactions being considered as one of the MMM Ponzi scheme transactions. Only the resultant records after filtering were processed for the analysis.

We leave a room of 2% statistical error margin.

LIMITATIONS OF METHODOLOGY

There are some limitations to this analysis. As stated earlier, this analysis covers only the last six months of the MMM Ponzi scheme. Also, because the financial industry only has a central point for inter-bank transactions (NIBSS), but does not have a central point for converging all intra-bank transactions, the analysis can only be done on interbank transactions. The figures in this report reflect ONLY the interbank transactions. It is estimated that at least another thirty percent of the above figures of MMM transactions might have taken place at intra-bank levels.

CONCLUSION

Although MMM has crashed, many other variants have spun off from it, and Nigerians

INTERNET OF PAYMENT THINGS (IoPT): THE SECURITY CONCERNS

By **Olusola O. Olodude**

Profile: Mr. Olusola Olodude is a staff of Nigeria InterBank Settlement System Plc (NIBSS). He holds a B.Tech degree in Computer Engineering from Ladoke Akintola University of Technology, Ogbomosho and a Masters in Computer Systems from the University of Ibadan, Nigeria. He is currently running Masters in Business Administration (with MIS Option) from the University College of Plymouth, United Kingdom.



Olusola joined the service of NIBSS in March, 2008. He has worked in various departments of NIBSS which includes Switching Operations, Nigeria Automated Clearing System (NACS) and Support Services. He was the team lead, Operation Support Unit of NIBSS before his redeployment to Fraud Management. He is currently the Head of Fraud Management Unit. He has facilitated in several training on Electronic Fraud and has served as guest speaker in several fora within the industry.

Olusola is highly experienced in Electronic Payment Operations, Cyber-Security, Fraud Detection & Prevention and Investigation. His certifications include Certified Fraud Examiner (CFE), Certified Ethical Hacking (CEH) and Computer Hacking and Forensic Investigation (CHFII). He is an associate member of Association of Certified Fraud Examiners (ACFE). He is also a member of Nigeria Electronic Fraud Forum (NeFF) and Nigeria Computer Society (NCS).

ABSTRACT

Change is the only constant phenomenon in the whole wide world. About two decades ago, when the internet came to Nigeria, it seems to be the height of technological innovation. I remembered how excited I was seeing “Dear Olodude, Welcome to yahoo mail”. The internet to us then was the climax of all invention. The advent of the email services disrupted the old traditional letter writing and postage system. The internet continues to grow not just faster, but at the speed of light. The internet became a platform where every business leveraged on for the provision of convenient and affordable services to their customers. The internet platform became a great tool for various industries ranging from automobile, military, government, education, and even religious associations.



*The financial industry did not lag behind in harnessing the strength of the internet. The internet brought about ease of doing business, seamless communication with consumers and thereby leading to customer's satisfaction. The internet gradually metamorphosed into Internet of things (IoT) by moving from our PCs at home to our mobile phones and now to everything you can think about. **"Yes, it is Internet of everyThing"**. Leveraging on various connected devices, the world is gradually moving away from just internet of everything into Internet of Payment Things (IoPT).*

INTRODUCTION

The financial industry is highly dynamic and constantly leveraging on available technology to provide convenient services to its customers. The consumers always prefer a channel of comfort in making payments without feeling any discomfort whatsoever. Today, mobile platform has already disrupted what was seemingly destructive payment system some years ago. With my mobile phone I can consummate almost all forms of banking services without having to visit the banking hall.

The advent of the internet caused a major change in every sphere of life. The payment space was not left out. However, wearable devices as a means of payments are going to be the next evolution, and in the future, most of the devices that are going to be connected will also be able to make payment. At this stage, we would be moving beyond IoT to IoPT. Major manufacturer of branded smart watches today are embedding the latest payment technology that will enable such devices to make payment. Imagine your smart-watch tracking all items picked at the shopping mall and initiating payments without you having to wait in line – what an easy life!!!

IoT: The Emerging Technology

The Internet of Things (IoT) is the inter-networking of physical devices, buildings, household equipment and other items embedded with software, sensors, chips and network connectivity that enable those objects to collect and exchange data. IoT is the concept of simply connecting any device with a power button to the



Internet and to each other. This includes everything from mobile phones, refrigerators, washing machines, headphones, lamps, wearable devices, cars and lots more.

The emergence of IoT is changing the way we interact, the way we drive, how we make purchases and even how we seek medical attention. Sophisticated sensors and chips are embedded into physical things that surround us and each transmitting valuable data. The Internet of Things (IoT) is growing faster in our advanced technological world and providing a paradigm shift in the interaction of people. The world is about to experience a digital payment revolution which will be driven by these connected objects. There will be increased efficiency through connected objects and this will lead to the establishment of new business opportunities. Objects connectivity will lead to provision of new services and thereby opening up new payment models. Our planet is about to witness a new payment era, it shall be called the “Internet of Payment Things”.

(IoPT): The future payment

This concept is called different types of names in various quarters. To some, it is IOT-enabled Payment, some call it Payments of Things while others call it Internet of Commerce and “Internet of Payment Things”(IoPT). Regardless of the various names, the most important factor is that it leverages on connected objects for payment.

With the development and on-boarding of various devices to make payment on behalf of their owner, the world awaits the emergence of new business models. The new rule for the future is going to be “Anything that can be connected, will be connected” according to Jacob Morgan. This will definitely lead to the complete digitalization and transformation of the financial system. It will also change the consumer's interaction within the payment space.

Bank customers will key into the digital payment and there will be a shift in spending pattern. Payment of things will create a new layer of an economy driven by the usage of recurring bills, pay-as-you-go subscription model and would also increase online transactions. Consumers will make payment with minimal stress and friction. We would



see introductions of different devices with different payment schemes.

Device can place order for replenishing services when in need of some items. Imagine your refrigerator in the living room stocks up items that is running out. Connected car will be able to pay toll fee, parking fees or perhaps pay for fuel refill at filling stations. Smart tag on your luggage could pay for baggage fees at the airport. You have exhausted your electricity credits but your prepaid meter is able to make credit purchase for your flat. Smart devices would maintain and service their own contract by themselves. Would you like to have a smart car that would pay its insurance premium as at when due?

Assuming you have a smart printer with replenishment services, you can push a button on the device to order for a new ink or toner. The payment is consummated using your online payment method, hence you do not need to log on to your internet banking, mobile platform or even place an order via online shopping portal. However, the printer can also contain on-boarding sensors that flag when the device is running out of ink. Using the available or preset data, the device could, by itself, place an order for another ink. Here, it is the device that initiates the transactions autonomously. This could be applied to different household devices. Your IoT-powered decoder can independently initiate your subscription payment before the due date, hence you do not need to bother yourself about when the subscription will expire. The IOT is expected to improve customer service experience and provide competitive advantage with convenient banking systems.

Securing the “Payment” in (IoT)

Every technological revolution comes with its own challenges. There are serious security implications on the use of IoT. Security becomes critical since we shall be entrusting our bank accounts to our connected smart objects with the ability to make payments on our behalf. Today, most devices are vulnerable to different threats with sophisticated breaches occurring in cyber-attacks.



loPT will definitely open a new phenomenon in the space of cyber security. Unprotected device on this platform will be attacked. Attackers would take control, steal information and disrupt connected services.

There will be identity issues here, hence there is need for not just the authentication of connected devices but also for the authentication of the user/owner too. Consumers must establish limits on the transactions the device can initiate, in terms of volume, frequency, or amount. The manufacturer of these devices must also ensure high-level embedded security as any serious security breaches could lead to reputational loss.

Besides, some of these devices are likely to be biometric enabled and the industry would need to start planning on how to solve device identity issue and reduced new arrays of fraud models due to loPT. The digital identity security is crucial here. The authentication, validation and access control of these devices will be made possible with the introduction of biometric features such as fingerprints, facial, iris or voice recognition. Perhaps, we might be authenticating payment instructions with the scan of our iris. Today, the financial industry has done very well by ensuring accurate identity of human customers with the implementation of Bank Verification Number (BVN). However, we may be heading for another phase of that project but this time for connected devices. Companies and organizations will experience more and new form of security threat. The issue of privacy and data sharing will be key discussion. Organizations are going to be faced with huge volume of data generated as a result of these connected devices. Organizations must ensure compliance with standards in storing, tracking, analyzing massive data that will be generated.

This future payment scheme will also change the face of electronic fraud pattern. Fraud will migrate to IoT in its full capacity. The implication of this is that fraud desks across the industry must scale up by connecting together – maybe we may have Internet of Frauddesks (IoF) – *just thinking*. Anti-fraud monitoring infrastructure must take into consideration IoT and integrate digital payment into its operations. Human identity with relation to device identify will be the new order for fraud desks in the industry.

Conclusion

The security of any payment infrastructure is very critical no matter how small or insignificant. To avoid **“Internet of Insecure Things”**, the financial industry must however, be prepared to ensure the security of these connected devices.

References

<http://www.wexinc.com/wex-corporate/the-internet-of-things-is-turning-into-the-internet-of-payments/>

<http://themworld.oberthur.com/payment-of-things/>

<https://usa.visa.com/dam/VCOM/download/visa-everywhere/innovation/bringing-secure-payments-to-the-internet-of-things.pdf>

<https://www.cognizant.com/services-resources/Gearing-Up-for-the-Internet-of-Payments-codex1549.pdf>

<http://internetofthingsagenda.techtarget.com/essentialguide/Prevent-enterprise-IoT-security-challenges-with-preparation>

A CHANGING PAYMENTS ECOSYSTEM: THE SECURITY CHALLENGE

By **Joash Omole** - Information Security Risk Mgt. – Access Bank Plc.

Profile: Joash Omole is a seasoned Information Systems Security professional with over (14) years banking experience spanning Information Systems Security, Application Support, Conduct and Compliance, and Risk Management. He is currently Head, Information Systems Security in Access Bank Plc.

He has a Bachelor's degree in Computer Science from University of Ilorin, Kwara State.

Joash is a Certified Information Systems Auditor (CISA), Lead Cybersecurity Manager (ISO27032), Certified in Management of Risk (MoR), an Oracle Certified Associate (OCA), and ISO27001 Information Security Management System - Lead Implementer and Auditor.



A century ago, a merchant's top payments concern was having an adequate supply of the right coins and bills in the till to make change for the customer. Rapidly changing technology, customer requirements and regulations are transforming payment systems, especially the e-payments, at a very fast rate globally.

Traditionally, the channels below, always resonate when we think of payment ecosystem:

- Automated Teller Machine (ATM)
- Point of Sale Terminal (POS)
- Electronic Funds Transfer
- Mobile Commerce
- Internet Banking

How consumers pay, what they pay with, and how they will like to pay, as well as the emergence of new participants competing with existing key players is a constant change driver in the ecosystem. The way in which people pay is now being driven more by how they live, and less by what is in their wallets. This change or evolution in the payment ecosystem comes with new levels of convenience and security needs/challenges for consumers, retailers and key players.

The need to meet the endless hunger for convenience and advancements in technology has led to the emergence of new payment methods such as contactless cards and Near Field Communication (NFC), IoT (Internet of Things), use of block chain technology, virtual/crypto currencies and a plethora of mobile payment options, forcing the traditional payment paradigm to evolve. Payments across borders, made seamless by interconnectivity, are now easier than ever before.

Challenges in the Payment Ecosystem

The stakeholders in the payment ecosystem, namely, Retailers, Merchants, Financial Institutions, Payment processors, Regulators and other participants now face new challenges and complexity in payments processing across multiple fronts. These fast-changing dynamics include:

- ✓ High customers' expectations on multi/omni-channels
- ✓ Demands for multiple, relevant payment options
- ✓ Rapid growth in mobile and card-on-file solutions
- ✓ Ever-changing security, privacy and fraud risks
- ✓ Increasing complexity in managing a multi-channel payment ecosystem

The changing payment ecosystem has its own security implications. These require adequate controls and proper fraud management processes, adopted across the e-commerce landscape. These changes in new technologies such as smartphones and digital wallets, shifts in buying habits, demands by individuals to accept card payments, and growing interest in peer-to-peer payments have created a fierce battle within the industry.

Digital revolution is driving business innovation and growth while exposing us to new and emerging threats. The top key security challenges in the payment ecosystem that confront merchants and financial institutions include, achieving security, privacy and regulatory requirements.

The changing payment ecosystem has witnessed increase in system attacks and breaches worldwide, which, if proper security controls are not implemented, will continue to grow. It is important to note that:

- The attacks are becoming more sophisticated in mode and methods
- More breaches are targeted at system components
- Criminals target the easiest opportunities
- Phishing, Smishing, Ransom ware, DDOS attacks, rogue mobile apps, man-in-the-middle vulnerability exploitation are samples of attacks that were witnessed in high volumes last year.

Despite the stipulated regulatory requirements and heavy investments in Payment Card Industry (PCI) compliance and security systems, the “black hat” threat to the privacy of customer and payments data continues to escalate. As technology certifications, such as PCI DSS, ISO27001, etc, are mandated with the widening scope of regulation, the compliance costs could increase. Conversely, the cost of a fraud is much higher, if the

security standards are not applied.

Strong assurance from independent trusted third parties as well as the development of, and adherence to, best business practices within the mobile payments ecosystem will be required to encourage widespread consumer adoption. Deployment of effective heuristic/behavioural monitoring system has also become inevitable as there is currently no “fool proof” security/fraud prevention system.

Collaboration among stakeholders is low, the need for collaboration among stakeholders to achieve a high level of security in the emerging payment ecosystem is essential and very important.

Constant training and research for security skill upgrade, technology, antifraud, compliance & internal control skills will effectively check the increasing new forms of attacks with complete visibility and granular control of the security system.

Continuous security awareness/sensitization to users and customers, training and re-training of staff on security of the payment ecosystem cannot be overemphasized.

Conclusion

The ongoing evolution in the payment ecosystem portends great benefits and ease of doing business. However, the inherent risks and security issues need to be adequately managed and harnessed by stakeholders. All hands must be on deck to ensure that we minimize the risks and maximize the benefits.

NeFF END OF THE YEAR DINNER

Colonades Hotel, Ikoyi



CREDIBLE, RELIABLE AND EFFICIENT PAYMENTS SYSTEM AS A PANACEA FOR CURTAILING MONEY LAUNDERING/TERRORISM FINANCING (ML/TF) RISKS IN NIGERIA FINANCIAL SYSTEM

By **Ibrahim Atukpa**, Financial Policy & Regulation Department, Central Bank of Nigeria.

Profile: Ibraheem Adeka Atukpa, Esq. is a Principal Policy Analyst with AML/CFT Division of Financial Policy and Regulation Department, Central Bank of Nigeria, Abuja.



1.0 Introduction

The increasing innovations in the payments system space call for strong and effective laws and regulatory frameworks to proactively deal with *actus reus* (activities) and *mens rea* (the mind) of fraudsters who would like to take advantage of the system. In the world today, the ease with which financial transactions are conducted using the available payment platforms requires a legal regime that is not only effective, but strong enough to prevent, detect and correct abnormalities. The role of the regulator is, therefore, to identify issues around the payment systems, analyse them, and formulate the appropriate policies to address the issues so identified, so as to gain the confidence of the participants in the financial system (depositors, shareholders, regulators, operators, etc). It is for the financial institutions or the platform providers to implement the laws and regulations to the letter, to protect the financial assets and data of the users of the platforms. It is a collaborative effort (regulators and operators) to safeguard the soundness, stability and safety of the financial system.

2.0 Credible, Reliable and Efficient Payment System

Payment system refers to “a set of instruments, procedures, and rules for the transfer of funds between, or among participants; the system includes the participants and the entity operating the arrangement” (Bank for International Settlement). <https://www.bis.org/publ>.

Another definition of payment system by Wikipedia says:

*A **payment system** is any system used to settle financial transactions through the transfer of monetary value, and includes the institutions, instruments, people, rules, procedures, standards, and technologies that make such an exchange possible. A common type of payment system is the operational network that links bank accounts and provides for monetary exchange using bank deposits.*

The definition of payment system is not limited to the use of ATM, PoS, NIBSS, Interswitch, Remita, Mobile banking, etc, but includes laws, rules, regulations, circulars and guidelines issued for effective management and operations of various platforms, intended to safeguard the financial assets of the depositors and shareholders.

Therefore, credible, reliable and efficient payment system is a *sine quo non* for fighting

money laundering/terrorism financing. For instance, withdrawal limit at the ATM, the Three Tiered Know Your Customer policy (segregation of accounts into Tier 1, 2 and 3) with minimum and maximum amounts of deposits and withdrawals, the 2factor authentication, use of token in internet banking, limit on cash deposits and withdrawals in line with cashless policy, the suspicious transactions report (STR), Foreign Currency Transaction Report, among others, are intended to safeguard the payment system from all forms of criminalities (e.g, fraud and forgeries).

3.0 Money Laundering/Terrorism Financing (ML/TF)

3.0.1 Money Laundering

Money Laundering is defined as the process of concealing and disguising the true origin, movement, ownership and purpose of illegal wealth (Shehu: 2015). The illegality of the wealth is the main reason why money is laundered so that me and you will believe that the money is not proceeds of crime such as fraud, illicit drug trafficking, bribery, kidnapping, etc.

Section 15 (6) of MLPA specifically lists predicate offences of money laundering as: *participation in an organized criminal group and racketeering; terrorism, including terrorist financing; Trafficking in human beings and migrant smuggling; sexual exploitation, including sexual exploitation of children; Illicit trafficking in narcotic drugs and psychotropic substances; Illicit arms trafficking; illicit trafficking in stolen and other goods; Corruption and bribery; fraud; Counterfeiting currency; counterfeiting and piracy of products; environmental crime; murder, grievous bodily injury; kidnapping, illegal restraint and hostage-taking; robbery or theft; smuggling; (including in relation to customs and excise duties and taxes); tax crimes (related to direct taxes and indirect taxes); extortion; forgery; piracy; and insider trading and market manipulation.*

In effect, proceeds of these predicate offences are illegal, and are therefore, considered crime when committed; and because they are illegal, they must be laundered to make them look clean.

3.0.2 How illegal money are laundered

There are three known stages of laundering money: **Placement, Layering and Integration.** *Placement* is the first step in laundering money. It refers to the process of depositing proceeds of crime (illegal funds) into a bank account. The second step is the *layering* which is the process of transferring by splitting/smurfing the money into two or more accounts in the same bank or in different accounts in different banks with the sole aim of disguising the

source of the fund. The intention is to make it difficult, if not impossible, to trace the movement of the money. The third and last step is the *integration* of the “washed money” into the formal financial system so as to make it look as if it is “legal money”. At this stage, the seemingly clean money will be used to acquire legal assets, invest in genuine businesses, thus integrated into the formal financial system that may not be traceable to the original illegal source.

3.0.3 Terrorism Financing

Without using technical definition, terrorism financing is the act of providing financial assistance to a terrorist, directly or indirectly, and with the knowledge that such money will be used to commit an act of terrorism. The import of this definition here is that terrorists are financed using the banking payment platforms to move money around to facilitate their heinous activities. This underscores the importance of financial institutions, particularly, banks in the struggle to keep our payment system safe from criminalities. The regulator provides the enabling laws and regulations, while the operators are expected to strictly comply.

Section 19 (3) of Cybersecurity Act, 2015 states: “Financial institutions must as a duty to their customers put in place *effective counter-fraud measures* to safeguard their sensitive information, where a security breach occurs the proof of negligence lies on the customer to prove the financial institution in question could have done more to safeguard its information integrity”.

The phrase “effective counter-fraud measures” simply means, ensuring that payment system should be such that it will be difficult for fraudulent mind to attempt to steal or tamper with funds of the depositors without being detected and prevented. Similarly, safeguarding “sensitive information” means that all records especially, financial records of the depositors must not be disclosed to an unauthorized user without his consent.

3.0.4 The Nigeria Electronic Fraud Forum (NeFF)

It will not be out of place to mention that the Forum has contributed immensely to credible, reliable and efficient payment system in Nigeria within its years of existence. Some of these contributions are contained in the previous Annual Reports of the Forum.

4.0 The relationship between payment system and Money Laundering/Terrorism Financing

Financial transactions are usually carried out at financial institutions (banks) thereby

making the institutions key in facilitating movement of funds from one account to another or from one bank to another or even across the Nigerian border. It is this critical role of movement of funds from one account to another within the banks and amongst the banks; and eventually into the hands of owners in an economy that it becomes imperative on the part of both regulators and operators to ensure that illicit funds are isolated from the financial system. Banks have been directed by the Central Bank of Nigeria via its instruments of supervision, to ensure that their payment platforms and systems are strong, reliable and effective enough to detect and deter the inflows and outflows of illegal funds respectively. With adequate control measures in place, it will be very difficult for money launderers and terrorism financiers to find a platform to perpetrate their illegalities. The fraudsters will not be able to penetrate the financial system without being detected, arrested and made to face the consequences of their actions if banks apply due diligence and commitments in complying with all laws, regulations, circulars, guidelines from the regulator in addition to complying with their internal control procedures, processes and putting in place appropriate mitigants. In other words, a credible, reliable, strong, effective and efficient payments system is a disincentive for fraudulent and illegal financial practices.

5.0 Conclusion

I want to conclude this paper by stating that the consequences of money laundering/terrorism financing in a developing country like Nigeria are better imagined than experienced. The lack of essential infrastructure to grow the economy was as a result of people stealing money meant for development, and stashing them in their houses when they could not “place” the stolen money in the bank; but where they could place the money, that is, deposit into a bank, they would, and start laundering process until it got co-mingled and lost the audit trail in the financial system. The way out is to ensure that both the regulators and the operators collaborate to fight the monstrous “vampire” through credible, reliable and efficient payment system.

Reference

Shehu, A.Y: Nigeria: The Way Through Corruption To The Well-Being of A People, National Open University of Nigeria, 14/16 Ahmadu Bello Way, Victoria Island, Lagos.

Bank for international settlement: <https://www.bis.org/publ>.

Money Laundering (Prohibition) Act, 2011 (as Amended)

Cybersecurity (Prohibition, Prevention) Act, 2015

Wikipedia, a free online dictionary

NeFF END OF THE YEAR DINNER

Colonades Hotel, Ikoyi



