Dimensions of Electronic fraud and Governance of Trust in Nigeria's cashless Ecosystem

Oludayo Tade and Oluwatosin Adeniyi

Abstract

A major downside of the cashless policy introduced in Nigeria since 2014 has been pervasive electronic frauds (e-frauds). Consequently, there is a growing fear of victimization among bank customers interfacing decision to migrate and utilize electronic banking. This raises the importance of trust governance in electronic banking and its centrality to the transition to a cashless economy in Nigeria. This study investigated e-Banking fraud and the role trust governance plays in the adoption or refusal to migrate and use electronic banking in Nigeria. The study was conducted in Lagos, Ogun and Oyo States. Using mixed qualitative methods (In-depth and Key Informants interviews) of data collection, participants were mainly purposively selected and in some instances reached through the snowball methods. Qualitatively, 30 victims of e-banking fraud were interviewed across the research settings. Further, purposive sampling proportionate to research settings was used to select at least 9 (3 in each state) bank officials in e-banking unit. To collect data at the e-banking governance level, we purposively selected participants in Nigerian Deposit Insurance Corporation (NDIC), Economic and Financial Crimes Commission (EFCC), and Committee of Chief Compliance Officers of Banks in Nigeria (CCCOBIN). In these three institutions, we interviewed one Executive member and two officials in fraud and risk management unit. In all, 9 participants were interviewed to provide data on dimensions of fraud, customer complaints and fraud mitigation mechanisms. Furthermore, 600 copies of a questionnaire (200 in each state) were on bank customers using e-banking and who have used any of the e-payment platforms. The questionnaire probed into reasons for adoption, concerns of trust, experiences of trust and perceived susceptibility to fraud. Qualitative instrument explored experiences of victimization and trust in cashless policy. Quantitative data will be subjected to univariate and bivariate analyses while qualitative data will be subjected to content analysis and ethnographic summaries.

Introduction

> *We have got more money now being transferred through electronic channels. Our concern is now how can we put in checks and balances to minimize fraud because as you move huge money via electronic channels efficiently, you run the risk of fraud being more efficient* ***(Sanusi Lamido Sanusi, Former Governor, Central Bank of Nigeria, 2014)***

Since July 1, 2014 when cashless policy became fully operational in Nigeria, a major downside of its introduction has been pervasive electronic Banking fraud (e-fraud). Cashless policy encourages electronic transactions with a view to reducing physical cash in the economy and thereby reduces the risk of cash related crimes. Although the policy is to foster transparency, curb corruption/leakages and drive financial inclusion, the growing perpetration of fraud threatens the cashless ecosystem. This has implications not only for the adoption of e-banking as a secured platform by the banked but is also a major threat to efforts to capture the unbanked populace. Initial investigations show that with the prevalence of fraud and victimization of subscribers, there is a growing fear of migration to and utilization of electronic banking, while those defrauded are opting out of e-banking. The Central Bank of Nigeria attests to the preponderance of electronic fraud (The Punch, June 30, 2014). The Nigeria Deposit Insurance Corporation reported a total of 3,756 fraud cases in 2013 (NDIC, 2013). The amount involved was N21.79billion, which represented 21percent increase compared with the N18.05billion officially documented for 2012. Furthermore, about half of the actual loss occurred within the first three months of 2013. However, looking beneath these aggregate pictures reveals the major channels through which fraudulent practices were executed. NDIC (2013) offers an elaborate list of fourteen sources with automated teller machine (ATM) fraud occupying a prime position. This prominence of ATM fraud is clear on two important fronts. One, a total of N585million was lost to ATM fraud in 2013. This represented approximately ten percent of actual losses over the course of the year. Two, and more importantly, in terms of frequency, almost half (46.3%) of reported cases were ATM-related. Both of these statistics undoubtedly point to the high and heightening incidence of ATM fraud within Nigeria's financial space.

Overall, the fact that the remaining 90 percent of the actual losses arise from thirteen other sources of e-fraud is a pointer to the multifarious nature of electronic fraud in Nigeria. Quite interestingly, as reported in NDIC (2013), a considerable proportion of these fraud cases (ATM related or otherwise) were executed with active collaboration by bank staff. The foregoing state of affairs therefore calls for a more rigorous scrutiny of the trust governance mechanisms within the financial system on the one hand and their effective functioning on the other. Such endeavour unarguably has implications for trust and its centrality to the imminent transition to a cashless ecosystem in Nigeria. With mounting complaints emanating from customers/subscribers on e-banking, a number of questions need probing: What are the dimensions of e-fraud? What strategies are used for perpetrating e-fraud? What role does fear play in adoption of e-banking? What institutional mechanism exists to engender trust governance in Nigeria's cashless ecosystem?

Trust underlies customers-bank relations when the former save their monies in banks. To ensure this trust is not eroded, banks are also expected to make sure that such 'contract of trust' is not breached. However, when bank customers get defrauded, trust is breached. There is therefore the need to understand the dimensions of fraud and the mechanism put in place to govern trust in Nigeria's cashless environment. This will provide insights on how to engender trust in the cashless policy and thereby drive financial inclusion. Building public confidence may be the way out of the woods when sound fraud

governance is put in place. It follows that institutional trust reposed in the banking system implies confidence in its reliable internal functioning. These internal control mechanisms are erected to check system vulnerabilities and douse uncertainties in the minds of bank customers.

Review of Related Literature

Electronic banking is one of the global best practices that have visited the Nigerian banking industry. Its launch into the domestic market has however produced dynamic changes in a number of aspects of social relations. On the positive side, Wada and Odulaja (2012) note that e-banking allows customers use of some form of computer to access account-specific information and possibly conduct transactions from a remote location like their home or workplace. According to Liao and Wong (2008), mobile payment such as this allows bank customers the latitude of conducting banking transactions from the comfort and security of their location. Of the e-banking innovations, Automated Teller Machines (ATMs) have emerged to be the most popular service delivery channel worldwide (Centeno, 2003). Other e-payment channels available for use in Nigeria include Point of Sales (POS), Internet banking and mobile banking. However, all these e-platforms are prone to attacks with consequences on customers and distrust in the payment systems.

Davinson and Sillence (2014) aver that fraudulent transactions via the internet or ATMs present a considerable problem for financial institutions and customers. This is because; millions of transactions are mediated by technology usually deployed within a cashless ecosystem like Nigeria. Existing studies conducted in Nigeria reveal that although banks have migrated from cash to automated transactions (Agboola, 2006), they are still confronted with insecurity and inadequate operational facilities, fear of fraudulent practices, and high cost (Chiemeke, Evwiekpaefe and Chete, 2006, Tade and Aliyu, 2011; Wada and Odulaja, 2012). Also, as observed by Davinson and Sillence (2014) and Tade (2013) technology mediated transactions have provided avenues for legally approved transactions as well as created opportunities for deviant behaviours. Despite the development of technological solutions to the problem of internet and ATM fraud, the amount of money lost to the crime remains huge with increasing number of users becoming victims (Davison and Sillence, 2014). Observing this trend, Jaishankar (2010) stresses the need to probe into victimization of technological extraction.

The pervasiveness of fraud in the Nigeria cashless ecosystem is indicative of the inadequacy of existing control mechanisms. This suggests the need for a better understanding of trust governance within the regulatory institutions and service providers. This is because; according to Bijlsma-Frankema and Ana Cristina Costa (2005), trust has now been recognized as a governance mechanism. Trust may undergird the expectations of bank customers when they migrate from cash-based transactions involving face-to-face context to virtual transactions (e-banking/payments). There is the need to fully understand how trust functions as a governance mechanism and how it relates to formal control (Bijlsma-Frankema and Ana Cristina Costa, 2005). Central to this is to investigate how institutional responses to fraud help to build confidence in bank customers? Another problem associated with cashlessness is the virtualization of relations, which in itself, limits the possibilities of monitoring and ensuring other forms of formal control.

The study of trust as a social phenomenon is not new to Sociologists. Classic studies such as Durkheim ([1893] 1960) on solidarity, Simmel (1950) on social ties, Weber (1947) on authority and legitimacy, Blau (1964) on choice in social relations and Gouldner (1960) on reciprocity are indicative of the earlier form of interest in trust. Before taking action towards embracing cashlessness, the banked and unbanked

populations need certain level of assurances, confidence building and trust. These certainly involve risk taking. According to Rousseau et al. (1998: 395), 'trust is a psychological state comprising the intention to accept vulnerability based on positive expectations of the intentions or the behaviour of another'. This implies that trust is associated with the risk that the other party may default which may result in adverse consequences (Bijlsma-Frankema and Cristina Costa, 2005). Bijlsma-Frankema and Cristina Costa (2005) note that studies have addressed control in the study of trust. Yet trust remains vital for human interaction and social relations including financial transactions. It is also of utmost importance in man-to-man and man-to-machine communications. The decision of people to take action towards cashless policy may be due to the cues they take from how the victims of fraud are treated, the fraud-proofness of the e-payment platforms and the governance mechanism which protects people from being victims. All of these may thus boost their trust.

The idea that trust and control might be related has been recently developed after decades of scholarly focus on formal control as a mechanism to govern organizational relations. Formal control is, in short, a regulatory process by which elements of a system are made more predictable through the establishment of standards in pursuit of some desired objective or state (Das and Teng, 2001). Trust operates on both interpersonal and system or institutional bases. While the former is concerned with people, the latter is related to the functionality of organizations and social systems. Zucker (1986) distinguishes three types of trust: (1) character-based trust based on social similarities and shared moral codes; (2) process-based trust, based on experiences of reciprocity; (3) institution-based trust, flowing from institutional arrangements that evoke and sustain trustworthy behaviours. In relation to technology driven payment systems, trust governance may be a vital tool in explaining adoption and its use by customers in the face of growing fraudulent practices. Distrust creates discord, since if others are distrusted, actors will tend to dislike what they like, tend not to share their definitions of relevance and, to the degree that the structure permits them, tend to avoid interaction with them. In the process of developing trust or distrust, beneficial events will tend to be attributed to others that are trusted and detrimental events to those who are distrusted. Trust begets trust, while distrust begets distrust (March and Olsen, 1975). In essence, even in relations among actors in the financial payment system trust may lubricate mutually beneficial partnerships.

Research Design and Method

The study was conducted in Oyo, Ogun and Lagos states in the southwestern part of Nigeria owing to preponderance of banks and customers alike. Another reason is that the cashless policy was piloted in 2012 in Lagos in the first phase while Oyo state became part of the cashless system in 2014 when it became operational nationwide. Uniquely, Lagos is the home of most bank headquarters in Nigeria. The study employed mixed method research design relying on qualitative and quantitative methods of data collection. It also sourced data from secondary sources mainly from organization records; Central Bank of Nigeria (CBN) circulars relating to cashless policy, NDIC records on the incidence of fraud, journal articles and newspaper publications on banking fraud in the research settings. Data was collected from 30 victims of e-banking fraud reached through the snowball and referrals, 10 purposively selected non e-banking subscribers; five investigators at the Economic and Financial Crimes Commission (EFCC), three members of the Committee of Chief Compliance Officers of Banks in Nigeria (CCCOBIN) through the in-depth and key informant interview methods. The interviews were largely carried out with a digital audio recorder to facilitate the onward download of the recorded conversation onto the computer for editing. Each interview lasted between 45 minutes and one hour. The audiotaped interviews were transcribed by the researchers to enhance accuracy, dependability and to enhance the integrity of data analyzed.

Stop checking of the transcribed tapes was done to ensure the trustworthiness and validity of the interviews. The interviews were then sorted along the emerging themes and content analysed. Quantitative data was collected using questionnaire which was administered to 600 respondents (200 in each of the field sites) using e-banking and who have used any of the e-payment platforms. The questionnaire probed into reasons for adoption, concerns of trust, experiences of trust and perceived susceptibility to fraud. Quantitative data will be subjected to univariate and bivariate analyses.

Findings and Discussion

Table 1: Socio-demographic Profile of Respondents

	FREQUENCY	PERCENTAGE(S)
AGE		
16-25	182	30.9
26-35	193	32.8
36-45	130	22.1
46-55	53	9.0
56-65	14	2.4
66-75	7	1.2
Above 75	3	0.5
Total	582	98.8*
EDUCATIONAL ATTAINMENT		
No formal Education	5	0.8
Primary	8	1.4
SSCE	152	25.8
NCE/OND	89	15.1
HND/BSc	255	43.3
MSc	55	9.3
PhD	8	1.4
Total	572	97.1*
MARITAL DESIGNATION		
Single	283	48.0
Marrried	241	40.9
Divorced	30	5.1
Separated	14	2.4
Widowed	16	2.7
Others	2	0.3
Total	586	99.5*
ETHNIC ORIGIN		
Yoruba	428	72.7
Igbo	98	16.6
Hausa	31	5.3
Others	30	5.1
Total	587	99.7*

Notes: These four key headings do not represent the full complement of respondent characteristics for which we obtained data. Hence, their choice as indicators of the features of our respondents is essentially for illustrative purposes. Additionally, rounding errors account for the observed total percentages that are less than 100. It is pertinent to also note that these statistics refer to the respondents in Lagos State. We do not include any tables for the other states since the attributes of interest bear a striking semblance to that of Lagos State.

Table 1 shows the profile of respondents along four core dimensions with respect to socio-demographic attributes. In terms of the age distribution of respondents, the majority are at most 45 years old

(85.8%), while only 0.5% is above 75 years. This is indicative of a plausible youthful bias of the survey which is not surprising owing to the well known affinity of young people for technologies and the specific innovations that they embody. Of all the respondents, less than 1% reported not having any formal education. This is only a little less than the proportion of respondents with a Doctorate degree (1.4%). Thus, the modal educational qualification is the Higher National Diploma (HND)/B.Sc obtained by close to half of the respondents (43.3%). Furthermore, about one-half of the respondents are single (48%) and the bulk of the other half are married (40.9%). This corroborates the aforementioned age distribution. With reference to ethnic grouping, more than 7 out of 10 respondents are Yoruba which is clearly a reflection of the location of the field sites in the predominantly Yoruba southwestern Nigeria. The other major ethnic groups namely Igbo and Hausa constitute 16.6% and 5.3% of our respondents respectively. Overall, our sample comprises of individuals who are majorly of young, educated, single or married and mostly Yoruba.

When the question, "do you use online banking services of any kind?" was posed, out of 572 respondents, 227 answered "No" (skeptics) and 345 said "Yes" (adopters). In what follows we thus present some evidence on a key aspect of the reported behaviour of respondent with focus restricted to the latter group. Table 2, shows the age distribution and its association with the demand for diverse online banking services among the group of respondents who are adopters.

Table 2: Use of Different Financial Services by Age Cohort (in %)

	VISITING BRANCH	TELEPHONE	ONLINE BANKING	OTHERS (MAIL, ATM, POS ETC.)
I. BILL PAYMENT				
16-25	48	11	26	42
26-35	60	7	46	21
36-45	36	1	24	16
46-55	20	0	13	4
56-65	5	0	4	1
66-75	1	0	2	0
Above 75	2	0	1	0
Total	172	19	116	84
II. BANK TRANSFER				
16-25	63	10	33	29
26-35	42	16	51	19
36-45	25	7	33	13
46-55	10	2	15	6
56-65	3	0	4	0
66-75	0	0	3	0
Above 75	1	0	1	0
Total	144	35	140	67
III. SPECIAL DEPOSITS/INVESTMENT				
16-25	63	5	14	5
26-35	48	4	7	4
36-45	34	0	1	1
46-55	14	1	3	0
56-65	5	0	1	0
66-75	0	0	0	0
Above 75	0	0	1	0

Total	164	10	27	10

Notes: The three online banking services – bill payment, bank transfers and special deposits – also portray similar behaviour of respondents when educational status rather than age is used as benchmark. We refrain from presenting these results to avoid duplication as the correlation coefficient between age and education attainment is very high in our sample. The qualifications in the notes to Table 1 also apply here.

As seen from Table 2, for bill payment, younger people used alternative platforms to conduct their transactions. For instance, most respondents (172) visited bank branches, while the use of telephone, online banking and other means (especially ATM & POS) are 19,116 and 84 respectively. Clearly, by age distribution, the younger cohorts (below 45 years) used all four platforms the most. More interestingly, however, the largest chunk of these younger respondents still paid visits to bank branches. This is plausibly a reflection of the low degree of substitutability between physical contact and electronic interaction. In terms of making bank transfers, a similar pattern is observed with respect to age dynamics. By contrast, however, the pie is almost equally split between bank branch visits and online transactions especially among the under-45 group. When compared with bill payment, almost double the number use their mobile phones for facilitating bank transfers (See Table 2).

For the case of special deposits/investment, such as fixed/time deposits, younger people appeared to be making plans for their old age partly due to the near absence of a formidable social security regime in the country. In doing so, nonetheless, they showed a marked preference for physical contact with bank officials since 145 out of the 184 respondents under the age of 45 reported that they visited brick-and-mortar banking institutions when it came to investing in order to secure the future.

Dimensions of electronic fraud

The migration of Nigeria from cash-based transactions to branchless banking (also called e-banking) is not without its challenges. These challenges sprouted out of the exploitation of the loopholes in the digital migration embedded in the cashless policy introduced countrywide by the Central Bank of Nigeria on July 1 2014. The gainers of the loopholes are the fraudsters who seem to have mastered the infrastructure lacuna and thus, worked on these lapses to defraud the savers, investors and the banking institution. While Cross (2015) noted that the methods adopted to defraud by fraudsters is endless, a study by same author (Cross, 2012) identified the end of goal of fraud to money solicitation through transfer of funds or obtaining passwords or personal details.

The dimensions of electronic fraud in the Nigeria's cashless ecosystem are of three types: insider fraud; outsider fraud and insider-outsider collaborative fraud. The first type is the fraud dimension that is exclusively executed by members of staff in the banking system. Due to their strategic position within the system and their understanding of how the system works, they defraud their banks thereby breaching the trust reposed in them. In this fraud type, the banking institution is the victim. The second type is a fraud committed by those that are outside the banking system. This category of fraudsters are external to the banking system but due to their dexterity on the internet and sometimes understanding of the victims' routine and identity they are able to carry out their fraud. The third type of fraud dimension found in this study involves the collaboration of bank staff and fraudsters outside the banking system. This collaboration ends up making the bank and individual account holders the victims of fraud. These three dimensions of fraud will now be discussed alongside the different types of fraud strategies in the Nigeria's cashless ecosystem.

E-fraud Strategies

Opportunistic Fraud: Kith and Kin

Automated Teller Machine fraud has continued unabated due to the breach of trust between account holders and the fraudsters. This is because most of the ATM frauds were carried out by those very close to the victim. They include spouses, boyfriend, and friends among others (Tade and Adeniyi, forthcoming). As we would show, fraudsters also capitalized on the vulnerability of their victims in relation to e-banking and trust. This is true as Drew and Cross (2013) note, online fraud becomes successful through selective identification and exploitation of victims' vulnerabilities by a dexterous and savvy offender (see also Tade and Adeniyi, 2014). In a particular case reported at a new generation Bank in Nigeria[1], a lady and her fiancée had up to three months to their wedding. It is usually taught at the marriage counseling preparatory to the wedding that couples must not hide anything from each other to build trust. However, the man took the ATM card of the lady and made a withdrawal of about N300, 000 ($ what exchange rate do we use?). Getting the 'surprise debit alert', the lady proceeded to the bank and lodged complaints. The ATM custodian at the Bank informed us that the lady threatened to sue his bank. However, this fraud alert was subjected to internal scrutiny during which it was found, through the Close Circuit Camera Television (CCTV), that it was her husband-to-be who made the withdrawal without her consent. According to the ATM Custodian; '*she was shocked seeing her man making the withdrawal. Her countenance changed and she felt sorry for raising her voice in the banking hall. She later left the banking hall to reconcile with her fiancée*'.

It can be inferred from the above case that fraudsters could be the unimagined person such as ones lover. This raises question on how social relationships is managed in a technology mediated financial ecosystem and its implications for human trust in electronic banking.

Bank staff can also collaborate with those outside the bank to defraud it. For this type of fraud to be successful, they recruit people who are closer to or occupy sensitive positions within the bank such as sweepers and those in the Information Communication and Technology (ICT) unit. This is mostly achieved by making juicy offers to get people to buy into the idea although not all participants get to know the final purpose for which they were asked to carry out an assignment. Fraud investigator at the EFCC summarized a case they investigated:

This fraud was huge. It involved the moving of about N400million[2] ($2010, 050) naira from the account of the bank. It involved some bank staff in the ICT unit and those in the regular banking hall. They got a woman who sweeps the office of the branch manager and gave her key-logger to insert in the computer to extract necessary data they needed and security information. Through this, they were able to access the banks account and moved the money into about forty different accounts. They were strategic about their fraud. They waited for the day there was public holiday and then moved all the money and almost immediately withdrew from different bank accounts. Before they could be stopped they had used more than three-quarter of the money to buy things online. It was the sweeper that eventually sold them out because as she claimed, she did not know that the things they gave her was to defraud the bank. By the time we tried to trace the computer where the money was wired from, we could not trace it because a particular system we suspected had been disconnected from the connecting wire to the ICT server. (Fraud detective/EFCC)

Un-credited Lodgment

Un-credited lodgment is another type of fraud, which is perpetrated by bank staff using their knowledge of banking operations and technicalities. It was found that the compromised bank staff in the cashier section may collect cash lodgment but may deliberately fail to credit the account of the customer and later divert the money for personal businesses. This becomes successful in most cases until the account owner lodges

[1] We have decided not to mention the name of Banks and Identity of our participants as it was part of the ethical issues raised and were assured of their anonymity before agreeing to participate in the research. In this study, we would be using pseudonyms to represent our participants and institutions.

[2] The official exchange rate in Nigeria at the time of writing is N199 to $1. This is what has been used throughout the paper.

complaint of not receiving any alert for the payment he/she made. It should be noted that not all account holders subscribe to account transaction alert which gives them information about any transaction on their account. This happens because people do not want any deductions to be made on their account for subscribing to this service. Hence, fraudsters predate on this loophole to defraud. A PhD candidate who shared his victimization experience on un-credited lodgement stated that '*I had a nasty experience with this electronic banking. I went to make lodgment of N50,000 (*$251.2*) into my bank account and I went back home. Two days later I did not receive deposit alert. I went back to the Bank and requested for my account balance. Funny enough it was the same amount before I made the lodgement. I went to the Bank Manager to complain and showed him the payment teller. While he wondered why that happened he asked me to come back. Nothing happened two days later, a lady cashier from the bank came to my house apparently traced it through the Know Your Customer form I filled. She told me to come to the bank that I was the one who made mistake in the payment. I was angered by this and I told her what nonsense. She later told me she thought I was working with a business man who they normally would not credit and would use the money to do a business and later credit the account after a week or two. Two hours she left my house, I got the credit alert*.' This experience brings to the fore the issue of customer knowledge about banking operations and how to stop fraud. Those who do not subscribe to account alert may have their monies un-credited and used for 'arranged' businesses by some compromised staff and their outsider accomplices.

Bank officials are also associated with dormant account fraud (DAF). When an account has remained inactive for about 6-months, it is described as dormant and no transaction is allowed on it except the account owner applies for re-activation. Upon this, the account becomes active. In Nigeria, when the account owner dies it is difficult for the dependants to access the account of their benefactor owing to many legal obstacles which may take months or years to surmount. More worrisome is the fact that some family members may be oblivious that the dead person has an account with a bank. As result, whenever the account owner dies, such funds become targets to insider fraudsters. With their knowledge of the status of the owner of the account insider-fraudsters reactivate and begin to withdraw money from the account. They also block possible traces of their actions from ranking management staff in the Branch. This was found to have been carried out by a female bank officer as narrated by a male ATM custodian of a new generation bank. He stated that '*the account belongs to a late Emir in Northern Nigeria. When the man died, some millions of naira were still left in the account. The lady banker found that this account had some good money in it lying fallow and started the process of reactivation, got a debit card on the account from the bank and started withdrawing from the account. It was not even the bank that discovered the fraud. it was her husband, himself a banker who realized she had started living above her normal salary. He carried out secret investigation and later raised the alarm. It was after she was arrested that she opened up.'* If this kind of fraud could occur, it implies a weak system of internal control on transactions which makes the funds of customers which is saved-in-trust vulnerable to compromised bank staff.

Abduction for fraud

Not all fraudsters dupe by using entirely their ICT knowledge. A new strategy in use is the abduction of people in public transportation by some cliques who would pretend to be transporters. They master the routine activities of their victims, call for passengers and once they are in the bus or car, they introduce force. A female victim in Lagos State narrated her experience:

> It happened a few minutes to 6:00am (early morning) while returning from a night vigil, I had boarded a bus supposedly to Oshodi from Obanikoro. No sooner had the bus moved than they sprang into action. The first thing they did was grab my phone; 'what do you do'? 'where are you coming from'? one of them asked. I was hopeful that they would take pity on me having told them that I am a primary school teacher. Why bother ask if it meant nothing to them? After rummaging through my wallet, they found two ATM cards and some cash.

The question that followed hit me with a bang. "what is your PIN number?" instinctively I hesitated for a while, but a resounding slap on my face soon got me spilling out….these guys were going to do the unimaginable….they were going to clear my account. I saw a guy they called officer with a gun hanging on his neck. He handed over the ATM cards to another member who played the role of a bus conductor. The driver slowed down at my inquisitors' command and the bus conductor jumped off the bus on his way to emptying my account. I silently wished I had paid the money into my friend's account, he had asked me to do so to avoid spending it since I am saving towards paying my rent. As I saw my phone beeped I realized the money had been successfully withdrawn from the account. They went back to the spot to pick the guy. I silently prayed that they drop me off at a safe place

This strategy has become regularly employed at the early hours and wee hours of the day when security is less visible. It is also a time when people rush to get to their destinations leaving little time for choice making and scrutiny of commercial vehicles and their occupants. The robbers cum fraudsters also understood their environment asking about the occupation of their victims in order to check their socio-economic status and make their decision. The use of force was to ensure compliance and naked display of gun as a measure of repression of any untoward resistance. The seizure of the phone was to check any information and stop reception of any call or text message. This loop completes a crime script which made the fraud successful. By this fraud the life chances of the lady, as it concerns paying for her rent, had been shattered. Trust lies beneath customer-bank relations when the former save their monies. As the narratives indicate, when people feel unsafe about technologically mediated transactions, they are more likely to adopt avoidance behaviour. This threatens the adoption, use and facilitates the opting out of electronic banking. This is consistent with the findings of Davinson and Sillence (2014) in their study of perception of being safe and secure in a world of technology-mediated transactions.

Trust Governance in the cashless ecosystem

The prevalence of fraud within the cashless ecosystem and its implications for the use of branchless banking options by bank customers in Nigeria has led to doubt or lack of trust or avoidance behavior. In order to understand what banking institutions and allied governance institutions do to engender trust in the policy, we asked participants questions bothering on mechanisms put in place to check fraud.

We found that weak governance structure is responsible for electronic fraud in Nigeria's cashless ecosystem. This weak governance is at the level of both banking institutions and regulating agencies such as the Central Bank of Nigeria. Our findings are anchored on the dimensions of fraud, which were discussed earlier. Data indicated that there was poor supervision at the branch, regional and zonal levels of some banks where fraud, get perpetrated. We found that inefficient supervision of junior bank staff accounted for banking fraud. A Bank Staff stated: '*there was a fund transfer fraud in which the best man we had for that job was involved in but rather than punishing him and sending the report to the regional head, the Branch manager decided to make it an in-house thing. They forced the man to fill a loan form where they were deducting the money he fraudulently made from customers account. They also moved him to another unit within the bank where he cannot have direct access to money. The matter was resolved internally within the branch*'. Such fraud neutralization strategy was adopted to cover the tracks of inefficient supervision, which the operations officer and the Branch manager ought to have been queried for. Through this compromised personnel are kept within the Banking system.

In line with the above is the exposure of casual staff to sensitive cash-handling positions within the bank. The neo-liberal policies have become embraced in Nigerian banking system to the extent that majority of bank staff are not full staff but casualised. This management decision has exposed lowly paid and motivated casual staff to have fraud opportunity. Giving credence to this assertion, a fraud report by the Nigerian Deposit Insurance Corporation (2014) stated that 64% percent of frauds committed in Banks were

perpetrated by contract/casual staff. The Committee of Chief Compliance officers of Banks in Nigeria (CCCOBIN) at their meeting of October 29, 2015 also noted that *'banks in a bid to cut cost and increase profitability recruit contract staff and assign them to very sensitive areas of the Banks operations and because these categories of employees are poorly remunerated they are susceptible to all sort of vices, including fraud*.' Although the Central Bank's representative at the meeting stated that "*the CBN may consider penalizing Banks for such fraud occurrence"*. This indicates a reactive rather than proactive governance approach. According to the Punch (Monday, November 9, 2015) publication entitled "**Concerns over rising bank fraud**" the paper opined that *whether the fraudsters are casual or permanent staff provides no comfort to the customers who lose their hard-earned savings and fortunes to white collar thieves.* The staff status is beside the point but internal compromise portrays a system in dire need of governance reviews. Loose governance will expose investors or account holders to the whims and caprices of opportunistic fraudsters within its fold. This is why fraud cases perpetrated by Bank staff are huge and mostly successful since they understand how the system works. When bank staffs handle huge transactions in banks without checks, fraud occurs. Weak governance system as stated by EFCC investigators included inefficient supervision; non-performance of oversight by regional heads of banks as well as poor follow-up on customers' addresses (Know Your Customer).

Despite this weak governance architecture, which is still not fraud proof, Bank executives reported having in place mechanism, which has limited the incidence of fraud. One of the mechanisms put in place is sending out information to customers who subscribed to electronic alerts. Through this, banks contact and send anti-fraud messages to their customers. Also, such messages are flashed on the Automated Teller Machines informing customers to protect their Personal Identification Number (PIN). For instance, during the BVN policy fraud, a message was sent by a Bank to her customers' tagged "BVN SCAM ALERT". This was sent to e-mail addresses of customers and displayed on the website).

A message on the website reads 'safeguard your account' Nobody knows your account better than you. That's why you should never share your card details, internet banking log in and token with anyone over the phone, SMS or email. GTBank is continuously developing and implementing security enhancements to ensure the integrity of our Online Banking platform. Our goal is to protect your online safety, the confidentiality of our customer account and personal data. Learn more about protecting yourself online, how to spot fraudulent e-mails and Web sites (http://www.gtbank.com/securitycentre#your-responsibility)

Messages such as this underscore the strategies used and educate customers about security information. However, we found that not all customers are subscribed to email alerts and many of these customers are either illiterate or semi-illiterate. This raises the issue of proper customer characterization and the need for complimentary financial literacy education. Owing to reputational risk, Banks run away of public prosecution of erring staff. Our research found that bank adopts shaming as a mechanism for instilling discipline with the bank while sending easing out 'bad eggs' through flagging of their images on computers and across the banking industry. Such system networking will not make other banks that are oblivious of the deviant records of the prospective staff offer such a person job. This approach reduces costs of litigation were the banks to engage in legal prosecution and protects them from being exposed 'as incapable of managing their customers' funds'. Such individuals are excluded from the banking sector. The informal sanction of shaming has proven to work for mitigating reputational risk. Professional sanctions such as sack and within-industry shaming are functional to the extent that they are activated with a view to protecting depositing and investing publics and the image of the organization (see Levi, 2002)

Conclusion

The study examined dimensions of electronic fraud and governance of trust in Nigeria's cashless ecosystem. As an underside of the cashless policy introduced in Nigeria in July 2014, pervasive electronic fraud

threatens the total embrace of this policy by banked and unbanked customers over safety of their funds under the new financial ecosystem. Trust governance becomes a central issue to engender trust and facilitate financial inclusion. The study found three dimensions of fraud to include insider fraud, outsider fraud and insider-outsider collaboration fraud. In majority of these dimensions, the banking institution is either a victim or the customers holding the account. The compromise of the Information Communication and Technology Units of Banks, casual and permanent employees in fraud episodes raises question about recruitment policies and internal governance within the banking system in Nigeria. Data shows that Banks do not fully prosecute fraudulent employees or any outsider found to have engaged in fraud to save cost of legal prosecution on one hand and to show customers that they are capable of keeping their monies safe on the other hand. The strategies used in perpetrating fraud, such as un-credited lodgment, fake job scam, ATM card swapping and compromise my lovers and son, fund transfer fraud, phishing emails/BVN fraud, and dormant account fraud among others, indicated that fraudsters are exploiting the loopholes of the cashless ecosystem. More importantly, it shows the need to check fraud outset through customer awareness and financial literacy education when a major policy has been introduced. There is need for policies in the financial space to target peculiar characteristics of customers to reduce fraud in developing countries particularly Nigeria.

At the governance level, the study found inefficient governance within the Banks and among governance institutions such as Central Bank of Nigeria. The 'Know Your Customer' is poorly followed up making it easy for fraudulent persons to give fake addresses without been discovered before getting account opened in their names. Although circulars for compliance to new rules and treatment of fraud cases within stipulated time are issued, many fraud cases go unresolved until customers become frustrated. Such unmet needs among victimized customers promote distrust in the financial system. Although scam alert messages are sometimes sent to customers, this does not get to all customers since very few are educated to know the importance of tracking their accounts through email alerts. Our findings also indicated that the illiterate and semi-illiterate do not get to know these hints thereby making them susceptible to fraud. Financial and safety education may be needed to protect these categories of customers. While Banks have erected mechanisms to impede fraud perpetration within their system such as 'maker-checker' which guarantees that no-one can initiate and complete a transaction without approval by another superior officer, card-hotlisting, the creation of 'Hall of Shame' where images of fraudulent staff already sacked are flagged across the banking industry to ensure that they do not get employed at another bank. While fraudsters continue to design more innovative ways of working on customers' vulnerabilities, there is need for Nigerian Banks to utilize the new Cybercrime Act to prosecute offenders/fraudsters to boost confidence and deter future offending behaviours.

References

Bijlsma-Frankema and Costa, AC (2005). Understanding the Trust-Control Nexus. *International Sociology* 20(3): 259-282

Blau, P. M. (1964) *Exchange and Power in Social Life*. New York: John Wiley.

Chiemeke, S. C., Evwiekpaefe, A. And Chete, F.(2006) The Adoption of Internet Banking in Nigeria: An Empirical Investigation, *Journal of Internet Banking and Commerce,* Vol. 11, No.3,

Das, T. K. and Teng, B. S. (2001) 'Trust, Control and Risk in Strategic Alliances: An Integrated Framework', *Organization Studies* 22(2): 251–83.

Durkheim, E. (1960) *The Division of Labor in Society*. Glencoe, IL: Free Press. (Orig. pub. 1893.)

Emeka A. (2007). Fraud Alert - Banks Raise Fresh Alarm on ATMs, Vanguard Newspaper Lagos

Emeka, E.E and Ezeani, F. (2012) Empirical Study of the Use of Automated Teller Machine (ATM) Among Bank Customers in Ibadan Metropolis, South Western Nigeria. *European Journal of Business and Management* Vol 4 (7):18-34.

Ezeoha, A. E. (2005). Regulating Internet Banking in Nigeria, Problem and Challenges-

Furst, K, .Lang, W. and Nolle, E. D. (2002) , Internet Banking Development and Prospects: Working Paper, Center for Information Policy Research, Harvard
Gouldner, A. W. (1960) 'The Norm of Reciprocity: A Preliminary Statement', *American Sociological Review* 25: 161–78. http://www.arraydev.com/commerce/jibc/2005

http://www.sharpedgenews.com/index.php/news/recent-news/139-357-nigerian-bank-employees-caught-in-atm-fraud-in-2010-ndic-report

Ihejiahi R 2009. How to fight ATM fraud online. *Nigeria Daily News,* June 21, P. 18.

Jaishankar, K (2010) The Future of Cyber Criminology: Challenges and Opportunities. *International Journal of Cyber Criminology* Vol 4 (1&2):26-31

Joe Agbro Jr., Rita Ohai, and Bukola Afolabi (2012). Living in the Shadow of hackers http://thenationonlineng.net/new/insight/living-in-the-shadow-of-hackers/ The Nation Newspapers (October 21, 2012)

Kerkhof, P., Vahstal-Lapaix, N. and Caljé, H. (2005) 'Store and Advertiser Reputation Effects on Consumer Trust in an Internet Store: Results of an Experimental Study', in K. M. Bijlsma-

Frankema and R. J. A. Klein Woolthuis (eds) *Trust under Pressure: Empirical Investigations of the Functioning of Trust and Trust Building in Uncertain Circumstances*. Cheltenham: Edward Elgar.

Liao Z. & Wong W. K., (2008).The Determinants of Customer Interactions with Internet-Enabled e-Banking Services. *The Journal of the Operational Research Society*, Vol. 59, No. 9, pp. 1201-1210

March, J. G. and Olsen, J. (1975) 'The Uncertainty of the Past: Organizational Learning under Ambiguity', *European Journal of Political Research* 3: 149–71.

Michael S.S. (2001).Robbery at ATM: Problem-Oriented Guides for Police Series

NDIC (2013). Annual Reports and Statement of Accounts. December 2013. www.ndic.org.ng

Nuth, M.S (2008). Taking advantage of New Technologies: For and against crime. *Computer law and Security Report*, Vol 25 (5):437-446

Nweze, C (2012) Banks raise Daily ATM withdrawal limit
http://thenationonlineng.net/new/business/money/banks-raise-daily-atm-withdrawal-limit/ posted on October 10, 2012

Obiano W (2009). How to fight ATM fraud. online Nigeria *Daily News,* June 21, P. 18

Ogunsemor AO (1992). Banking services: The emergence and impact of electronic banking. *The Nigerian Banker*, January – March, 1992
Part1, Journal of Internet Banking and Commerce 10(3), retrieved from
Problem-Specific uides Series No. 8. New York

Rousseau, M. T., Stikin, S. B., Burt, S. B. and Camerer, C. (1998) 'Not So Different After All: Across-Discipline View of Trust', *Academy of Management Review* 23(3): 393–404.

Simmel, G. (1950) *The Sociology of George Simmel.* New York: Free Press.

Tade, O (2013). A Spiritual Dimension to Cybercrime in Nigeria: The Yahoo-plus Phenomenon. *Human Affairs*, Vol 23:689-705.

Tade, O and Aliyu, I (2011). Social Organisation of Cybercrime among University undergraduates in Nigeria. *International Journal of Cyber Criminology* Vol 5(2): 860-875

The Punch, June 30, 2014. Tortuous journey to cashless economy. Pages 39-42
University
Uslaner, E.M (2004) Trust and Social Bonds: Faith in Others and Policy Outcomes Reconsidered. *Political Research Quarterly*, Vol. 57, No. 3, pp. 501-507

Wada, F and Odulaja, G.O (2012). Assessing Cyber crime and its impact on E-Banking in Nigeria Using Social Theories. *African Journal of Computer and ICT Vol* 4. No.3 (2): 69-82.

Weber, M. (1947) *The Theory of Social and Economic Organization.* New York: Free Press.

Zucker, L. G. (1986) 'Production of Trust: Institutional Sources of Economic Structure', in B. M. Staw and L. L. Cummings (eds) *Research in Organizational Behavior*, Vol. 8, pp. 53–112. Greenwich, CT: JAI Press

Levi, M (2002) Suite Justice or sweet Charity? Some explorations of shaming and incapacitating business fraudsters. *Punishment and Society* 4(2):147-163

Drew, J and Cross, C (2013) Fraud and its PREY: Conceptualizing social engineering tactics and its impact on financial literacy outcomes. *Journal of Financial Services Marketing*, Vol 18: 188-198.

Tade, O and Adeniyi O.A (2014). Automated Teller Machine Fraud in Southwest Nigeria: The shoe wearers' perspectives. http://www.imtfi.uci.edu/files/docs/2014/tade_and_adeniyi_final_2014_1.pdf.

Tyler, T ad Lind E.A (1992). A relational model of authority in groups. In Zanna MP (ed.). *Advances in Experimental Social Psychology* 34:1-59

Wemmers, Jo-Anne and Manirabona, Amissi (2014). Regaining trust: The Importance of justice for victims of crimes against humanity. *International Review of Victimology*, Vol 20 (1):101-109.