Article

International Journal of
Offender Therapy and
Comparative Criminology
2020, Vol. 64(16) 1717–1740

DOI: 10.1177/0306624X20928028
journals.sagepub.com/home/ijo
SAGE

Dimensions of Electronic Fraud and Governance of Trust in Nigeria's Cashless Ecosystem

Oludayo Tade[1] and
Oluwatosin Adeniyi[1]

Abstract

A negative outcome of the nascent cashless policy in Nigeria has been persistent electronic banking fraud (e-fraud). Fraud occurrence in any financial space indicates insecurity and loopholes being exploited by fraudsters. This underscores the importance of trust governance in electronic banking and its centrality in a transiting cashless economy like Nigeria. Against this background, we investigated e-banking fraud and the role trust governance plays in both the adoption and refusal to migrate and use electronic banking in Nigeria. Using qualitative methods (in-depth and key informant interviews) of data collection, 30 participants were purposively selected and in some instances reached through the snowball and referral methods. Findings showed internal, external, and collaborative dimensions of e-fraud. Experiences of fraud reportedly affected adoption and migration of bank customers to e-banking platforms. Although weak governance mechanism was reported, banks nonetheless are embracing security mechanisms such as sending SCAM alert messages to customers, while shaming and sack of compromised staff were employed as within-bank measures to secure the confidence of customers in the evolving financial ecosystem.

Keywords

financial inclusion, electronic fraud, cashless ecosystem, cybersecurity, Nigeria

[1]University of Ibadan, Nigeria

Corresponding Author:
Oludayo Tade, Department of Sociology, Faculty of Social Sciences, University of Ibadan, Ibadan 200284, Nigeria.
Email: dotad2003@yahoo.com

Introduction

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 the quantum of physical cash in the economy and thereby minimizing 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 nonetheless 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 made to capture the unbanked populace. While banking fraud appears to have heightened in the wake of the introduction of electronic payments, the history of fraud in Nigeria as well as other parts of the world is long. In other words, fraudulent people abound everywhere and Nigeria is not an exception. To underscore the ubiquity of fraud, Cross (2019) extensively reports fraud incidences from the United Kingdom, the United States, Australia, Canada, and Hong Kong with attendant losses in millions of dollars.

Ibrahim (2016) offers a telling sense of the historicity of fraud within the Nigerian context. According to this author, colonial records clearly indicate that "schoolboys" had mastered the art of counterfeiting a broad spectrum of things ranging from official letters to people's signatures (identity theft). These Wayo *trickers*, as they were then referred to, had developed capacities to act as impostors of gold and diamond merchants. The discovery of oil and its commercial exploitation in post-independence Nigeria provided unprecedented impetus for the proliferation of fraudulent practices as the economy was awash with *petrodollars* (Adogame, 2009) which was seen as part of a national cake to be shared. Glut in the global oil markets in the beginning of the 1980s implied sharp reductions in revenues to the government and the entry of the Bretton Woods institutions (particularly the International Monetary Fund [IMF]) into the socio-economic sphere in Nigeria via austerity measures. This reform encapsulated a wide array of interventions in the economic life of the country. It is noted that advance fee fraud ("419") phenomenon emerged strongly in this milieu. The unrealistic expectations during the oil boom years dovetailed into unmet aspirations in the oil bust years producing a large army of disgruntled and jobless citizenry who became vulnerable to becoming fraudulent. In addition to these, Ampratwum (2009) listed a host of other contemporary dimensions of fraud in Nigeria to include credit card fraud, false identity fraud, forgery, and immigration fraud, among others. Therefore, it is doubtless from the foregoing that fraud in Nigeria predates the introduction of electronic payments or internet-enabled transactions which lie at the core of cashless policy. However, the scale of fraud has been accentuated by technological developments and newer vintage fraud typologies are emerging which call for an

explicit focus on the dimensions of electronic fraud within today's cashless ecosystem in Nigeria.

The Central Bank of Nigeria (CBN) also attests to the preponderance of electronic fraud (The Punch, 2014). The fraud anatomy in the Nigerian Banking industry shows that fraudsters continue to evolve new strategies to explore loopholes in the system. For instance, 26,182 attempted frauds and forgeries were made in 2017. This figure is higher than the 16,751 cases recorded in 2016 (Nigeria Deposit Insurance Corporation [NDIC], 2013). Approximately N2.4 billion naira was the value of actual loss to fraud in 2017. This indicates that incidence of frauds within the financial system remains high and in need of empirical probing to understand its varying and evolving dimensions. On a closer scrutiny of the NDIC records, technology-mediated financial platforms show the highest vulnerability to the frauds reported and account for the chunk of associated losses. The foregoing state of affairs calls for a more rigorous scrutiny of the trust governance mechanisms within the financial system on one hand and their effective functioning on the other. Such endeavor unarguably has implications for trust and its centrality to the 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 institutional mechanism exists to engender trust governance in Nigeria's cashless ecosystem?

Trust underlies customer–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 mechanisms 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 remote locations 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 sale (POS), internet banking, and mobile banking. However, all these e-platforms are prone to attacks with unintended consequences on customers and distrust in the e-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 challenges such as insecurity and inadequate operational facilities, fear of fraudulent practices, and high cost (Chiemeke et al., 2006; Tade & Aliyu, 2011; Wada & 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 behaviors. 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.

It is nonetheless pertinent to point out at this juncture that this seemingly grim picture is not peculiar to Nigeria but evidential of the broader geography of electronic fraud in the global system. While an elaborate description of this ubiquitous and internet-mediated international fraud landscape is not the focus of this study, a few researches done in Latin America and the Pacific, Southeast Asia and India are purposively selected for succinct discussion with the view to demonstrating how the aforementioned observations about fraud in the Nigerian financial ecosystem fit into or potentially may diverge from broader patterns established in other parts of the globe.

Large-scale cyber-attacks and leaks or massive thefts of data are considered among the five most likely risks in the next decade globally (World Economic Forum [WEF], 2018). To this end, the General Secretariat of the Organization of American States (GS/OAS, 2018) undertook a survey-based study on the State of Cybersecurity in the Banking Sector in Latin America and the Caribbean in 2018. The survey instrument was designed to elicit information on multiple aspects of digital security (particularly characterization of banking entities, for example, size distribution and digital security risk management approaches) especially in the banking sector as well as details on the impact of electronic fraud incidents in the region. Overall, the responses showed that there is growing awareness about the evolution of the risk of cyber fraud

incidents with 79.54% of respondents indicating worsening of the situation in the last year. This is in contrast to 10.85% and 9.61% who suggested perceiving that increase or not knowing about it, in that order. In terms of the related issue of the impact of fraud prevalence, 67.08% of respondents considered the existence of risks derived from cyber incidents to be important in affecting their decision to use or not to use digital financial services in this sector.

In India, there is also widespread incidents of financial fraud especially those facilitated via digital platforms (The Associated Chambers of Commerce and Industry of India [ASSOCHAM] and PWC India, 2015). This 2015 joint report, for instance, itemized the dimensions of the fraud as follows: fraudulent documentation, multiple funding/diversion/siphoning of funds, identity theft, internet banking and related frauds, incorrect sanctioning or external vendor-induced fraud, counterfeit cheques, as well as overvaluation or absence of collaterals. The report also provided an incisive summary of global trends in fraud detection and prevention with the eventual notion of the need for financial institutions to look beyond internal controls as sole focus but embrace customer education and other financial literacy initiatives.

Turning to a recent report in the ASEAN Post (2020), Southeast Asia is depicted as the most vulnerable region to fraud compared with the rest of the Asia Pacific. In this region, and of all fraud types, Bot attacks is the leading method in the region with an average of 64.2% across six Southeast Asian countries. In terms of its intra-region severity, the report suggested that it is most prevalent in Vietnam (87.1%), Singapore (66.3%), and Indonesia (58.6%). However, in Thailand and Malaysia, electronic platforms are more prone to click flooding, while finance apps in the Philippines' are more susceptible to install hijacking (50.3%).

In Vietnam, with the most pervasive fraud landscape, security risks such as fraud, customer fraud, network attacks on bank infrastructure, and user data leakage continue to rise and the need for the government to engineer sound regulatory/legal framework for user data security will go a long way in creating and sustaining safe and reliable digital transaction system. This is particularly so as the ongoing adoption of new financial technologies is expected to continue into the future. Financial institutions must therefore stay alert and deal with fraud on a perpetual basis because of its dynamic nature. This should work to deal with real risks such as credibility deficits and loss of trust.

Having highlighted the foregoing cross-national depiction of the global electronic fraud landscape, we again return here to our specific case of interest, Nigeria. The pervasiveness of fraud in the Nigerian 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 & Costa, 2005). Central to this is to investigate how institutional responses to fraud help to build the confidence of bank customers in the credibility of the banking system.

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 forms of interest in trust. Before taking action toward 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), "trust is a psychological state comprising the intention to accept vulnerability based on positive expectations of the intentions or the behaviour of another." (p. 395). This implies that trust is associated with the risk that the other party may default which may result in adverse consequences (Bijlsma-Frankema & Costa, 2005). 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 be favorably disposed toward 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 victimized. All of these may serve as trust boosters.

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 & 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: (a) character-based trust which is hinged on social similarities and shared moral codes; (b) process-based trust, which is related to experiences of reciprocity; and (c) institution-based trust, flowing from institutional arrangements that evoke and sustain trustworthy behaviors. 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. In the process of developing trust or distrust, beneficial events will tend to be attributed to others who are trusted and detrimental events to those who are distrusted. Trust begets trust, whereas distrust begets distrust (March & Olsen, 1975). In essence, even in relations among actors in the financial payment system trust may lubricate mutually beneficial partnerships.

Routine Activity Theory

To explain the dimensions of fraud and governance of fraud in Nigeria's financial ecosystem, we employ routine activity theory (RAT; Cohen & Felson, 1979) as theoretical anchor. The theory explains why crime occurs and under what social situation it is made possible. Specially, RAT contends that crime occurs in time and space. Accordingly, the proponents aver that crime occurrence is the result of the convergence of a motivated offender (poorly paid bank staff, unemployed graduates, greedy spouse, etc.), suitable targets (money in electronic format, banks, information and communication technology [ICT] deficient bank customers, etc.), and lack of capable guardianship (poor cybersecurity system, ineffective governance and sanctions by the CBN on fraud cases, ineffective cybersecurity laws, compromised bank staff, poorly motivated bank staff, poor internal control mechanism on transactions, etc.). In deploying RAT to explain dimensions of electronic fraud and governance of trust in Nigeria's financial space, we argue that the convergence of these three elements explains e-banking fraud. As we would show later in the article, the dimensions of fraud (internal, external, and collaborative) is a function of the exploitation of the loopholes in governance institutions and bank customers by fraudsters. Just as banks and their customers are suitable targets to fraudsters, Cohen and Felson (1979) explained factors that make vulnerable institutions such as banks and their customers attractive to fraudsters. They posited that value, inertia, visibility, and accessibility (VIVA) make offending behaviors possible. Perceived value commanded by the potential victim (financial institutions account, customers account, and transactions with huge financial returns) enables offending behavior to be directed at them. Inertia, the size, and weight of the target are also important. In this case, technology-mediated transaction makes it possible to transfer millions of naira within minutes from one account to another with mastery of the online system. Fraudsters can also make purchases online with the hacked account without having to make withdrawals or carry any heavy physical cash. Third is visibility. This relates to how physically visible the target is to the offender. This is possible once the suitable offender is able to have access to the account of the target (individual or financial institution). While enhanced guardianship (account password, financial literacy education, increased cybersecurity, motivated staff, shaming, etc.) may reduce the incidence of fraud, staff casualization and their deployment to sensitive positions within the industry will promote fraud and undermine trust in the cashless ecosystem. This is another area where RAT becomes useful. Further development into the theory identified what could be done to possibly deter offending behaviors against persons, institutions, or places (see Felson, 1986). Accordingly, *controllers*, as they are called, ensure that persons are prevented from engaging in deviant behaviors while places and

institutions are monitored to prevent or neutralize offending behavior against them. Among the controllers are *Handlers* (parents, teachers in schools) who have personal contacts with potential offenders and are able to monitor them and keep them out of trouble. *Guardians* on their part protect suitable targets from potential harm (Felson & Cohen, 1980). Finally, *managers* ensure that the spaces of suitable targets are fortified to ward-off any potential harm against it. Electronic banking fraud therefore is the result of ineffective *controllers* while fraudsters utilize their mastery of the routine activities of the suitable target and their vulnerabilities to defraud.

Method

We conducted this study in Lagos[1] and Oyo states in southwestern Nigeria. The cashless policy was piloted in Lagos in 2012 while Oyo state became part of the cashless system in 2014. Uniquely, Lagos hosts most bank headquarters in Nigeria. The study design was exploratory and utilized qualitative tools of data collection. This was complemented with secondary sources such as CBN circulars relating to cashless policy, NDIC records, and newspaper publications on fraud.

Data were collected from 20 victims (10 from each state) of e-banking fraud. Five bank customers who did not subscribe to the cashless policy and five fraud detectives at the Economic and Financial Crimes Commission (EFCC) were all reached through the purposive and snowball sampling techniques.

To reach the victims, we utilized individual contacts and institutional referrals. In the case of the former, we got people who linked us with those who had experienced fraud and through them, we snowballed. To unpack the dimensions of fraud, we asked the victims to share their experiences with cashless banking, narrate how they were defrauded, and how they responded or coped with it. The key informants provided responses to questions bordering on fraud landscape, fraud types, governance mechanisms, and how to enhance trust. Furthermore, we obtained observer-status approval to attend the meeting of Committee of Compliance Officers of Banks in Nigeria (CCOBIN)[2] in Lagos. Our non-participant observations at the meeting enriched our understanding about the experiences across the sector and what banks and security agencies are doing to curb fraud menace.

Most of the interviews lasted between 30 min and 1 hr. Through these interviews we developed codes based on shared expressions (experiences). These were collapsed to form themes such as fraud dimensions, fraud strategies, fear of fraud, and trust governance. All of these were then subjected to thematic analysis.

Discussion of Findings

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 from the exploitation of the loopholes in the digital migration embedded in the cashless policy introduced countrywide by the CBN 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 savers, investors, and banking institutions. While Cross (2015) noted that the methods adopted to defraud is endless, a study by same author (Cross, 2012) identified some fraud dimension in the United Kingdom to include money solicitation through transfer of funds or obtaining passwords or personal details. In this study, we uncovered three dimensions of fraud in Nigeria's cashless ecosystem. These fraud dimensions are as follows:

1. *Insider fraud:* By insider, we mean those working with banks or those in any form of affinitive relationship with account holders. Here, the fraud is exclusively executed by members of staff in the banking system. Due to the strategic position they hold in the system and their grasp of the routine working, they breach the trust reposed in them through fraud. In this fraud type, the banking institution and customers are the victims.
2. *Outsider fraud:* This category of fraud is those external to the banking system. The perpetrators usually thrive on their dexterity on the internet and sometimes on the understanding of the victims' routine and identity. This makes them better positioned to plan and execute their fraud.
3. *Collaborative fraud (insider–outsider working together):* The third dimension of fraud 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.

How do these fraud dimensions get executed by fraudsters? In what follows, we share cases which represent each dimension of fraud.

ATM 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 & Adeniyi, 2016, 2017). Their familiarity with the victim makes him vulnerable to the antics of the enemy-within. This is because they understand his routine, and the account holder is more likely to let down the guide when it has to do with those from his or her inner circle. Fraudsters also capitalize on the vulnerability of their victims in relation to e-banking and trust. 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 & Adeniyi, 2014).

In a particular case reported at a new generation Bank in Nigeria,[3] a lady and her fiancée were about to tie the nuptial knot in 3 months. At pre-marriage counseling for intending couples, openness in marital relationship (including finance) is encouraged to engender trust. However, the man took the ATM card of the lady and withdrew N300,000 (US$833). The account owner received "surprise debit alert" and consequently proceeded to her bank to complain. Our research participant who is an ATM custodian informed us that the lady threatened legal action against the bank. However, this fraudulent withdrawal was subjected to internal scrutiny during which it was found, through the mounted *guardian* (Felson & Cohen, 1980), a Close Circuit Camera Television (CCTV), that it was her husband-to-be who was the perpetrator. 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.

Women also breach the trust in their marriages and may also defraud their husbands. This appears to be the case when new technology is introduced and account holders do not seem to know the required security steps to take to protect themselves from fraud. Indeed, it can be argued that characterizing account holders may provide useful insight in offering unique services to customers with similar vulnerabilities to protect them from fraudulent losses. Both illiterate and semi-illiterate customers are vulnerable in technology mediated transactions. We found that it is possible that a wife defraud her husband and vice versa when one has the knowledge that the other does not understand technology-driven transactions. This occurred in a case where a young lady had taken her husband's debit card and made withdrawal. Another bank ATM custodian elaborated thus:

> You see when the man got the alert of withdrawal on his phone, he rushed down to our bank. And because he is one of our big customers, we promptly attended to him. He told us that certain amount was withdrawn from his account while he had his ATM card with him. But you see when we carried out our investigation we found out that it was a compromise. We call it customer compromise because such would not have happened if the customer has not compromised their security numbers. We found that it was his wife who made the withdrawal twice. To save the situation and shame within the banking hall, he told us that he had forgotten that he gave his wife the ATM to make some withdrawals when going to

> school. What the wife did was to transfer money into her account and returned the ATM back to where she took it.

It can be inferred from the two cases that fraudsters could be the unimagined person such as one's lover. This raises question on how social relationships are managed in a technology-mediated financial ecosystem and its implications for human trust in electronic banking.

While the previous cases were insider fraud in affinitive relationships, fraud could also be perpetrated by bank staffs to defraud their organization. For this type of fraud to be successful, they recruit or enlist people who are closer to or occupy sensitive positions within the bank such as cleaners or sweepers and those in the ICT unit. This is 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. A fraud detective at the EFCC summarized a case they investigated:

> This fraud was huge. It involved the moving of about N400 million[4] ($2,010,050) 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)

Uncredited lodgment (receiving cash from customer without immediately crediting the account holder) is another type of fraud which is perpetrated by bank staff using their knowledge of banking operations and technicalities. Data show that that a compromised bank cashier may collect cash lodgment but may deliberately fail to credit the account of the customer and will divert the lodgment for personal (quick) business. This fraudulent diversion continues to be utilized until the account owner lodges complaint of not receiving any alert for the payment he or she made. It should be noted that not all account holders subscribe to transaction alert which gives them information about any transaction

on their accounts. This is often the case because people often do not want any deductions to be made on their accounts for subscribing to transaction alert. Hence, fraudsters capitalize on this loophole to defraud. A male doctoral candidate who shared his fraud experience on uncredited lodgment 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 who apparently had 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 after 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 uncredited and used for "arranged" businesses by some compromised staff and their outsider accomplices.

Similar to this, one of our informants and a detective at the EFCC narrated how a N90 million (US$452,261) fraud was perpetrated by an account officer of a major eatery in Lagos state. He stated that,

> As the account officer he would collect money on a daily basis and was expected to credit the company's account. However, he would collect money on Monday and lodge it and collect on Tuesday and not lodge it. He was missing one day out. He did continuously until he was able to rake in N90 million. At this time, when the eatery management raised the alarm on their account, he ran away and could not be found. We however used his sister to arrest him. We were only able to recover N8 million naira from him. He had used part of the money to organize his wedding, had a baby and almost completed a four-bedroom bungalow at another area in Lagos.

This strategy was successful because the Nigeria's cashless ecosystem is still confronted with infrastructure challenges which make people receive delayed alert while many do not even subscribe. The eatery management trusted their account officer but did not know that he had ulterior motive.

Bank officials are also involved in 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. But when the account owner dies, it is difficult for dependants to easily access the account of their benefactor due to many legal obstacles and bureaucratic bottlenecks which may take months or year to scale. More worrisome is the fact that some family members may be oblivious that their deceased relation had such an account. Thus, whenever the account owner dies, such funds become target of insider fraudsters. With their knowledge of the status of the owner of the account, insider fraudsters reactivate the dormant account and start to draw money from the account. They also block possible traces of their actions from ranking management staff in the bank 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.

What this type of fraud shows is a weak internal control on transactions which makes the funds of customers which is saved-in-trust vulnerable to compromised bank staff.

Another type of fraud which is external to bank and its staff is what we have called policy fraud or bank verification number (BVN) fraud. This is tagged as BVN fraud due to the circumstances under which this type of fraud was birthed. The biometric data verification exercise was the policy of the CBN during which all bank account holders were to compulsorily undertake biometric registration. The intention was to ensure security and check fraud. The Federal Government issued a "threat" that whosoever fails to be captured in the BVN registration exercise would not be able to carry out any transaction on his or her account. While the policy could enhance security, many account holders only rushed to banks to carry out the exercise without sufficient financial literacy education. The panic of not been able to access money from unregistered accounts was then feasted upon by fraudsters who began to send fraudulent text messages, phishing mails, and made phone calls to people to supply their BVN details. Due to this, many unconsciously sent their details and became victims. A business man (victim) shared his experience:

> I have not been able to access my account for some days due to non-availability of data on my computer. I needed to make some transactions and I headed for my

> bank. I had called my account officer ahead of time. On getting to the bank, I connected my computer and got a mail from a supposed same bank. I was asked to click on a link and supply my BVN details for update of my account or face service suspension on the account. I just clicked the link and supplied my details and behold, N1 million naira debit alert came on my phone within five minutes! I was shocked and devastated but before we could do anything they had withdrawn everything.

This victimization experience was striking as it happened within the banking hall. The victim, although sat opposite to his account officer, did not bother to ask the bank official about the authenticity of the mail before he got defrauded.

Fake Job Scam

Fraudsters are innovative in thinking, always trying to maneuver security erected along their path. This is where the fake job scam represents a new way of executing electronic bank fraud in Nigeria's cashless ecosystem. Our key informants at the EFCC stated that with the improvement in security features on the ATM and with the BVN, fraudsters have devised this fraud scheme to remain anonymous while those who rather know nothing about the fraud would be arrested as happened in case of a botched deal shared by the detective:

> you will hear from the news these days that one man was arrested with 50 ATM cards and you will be wondering how this is possible. What they do now is fake job scam. They put up fake job opportunity adverts on the road side. When people apply, one of the conditions for getting the job is to open a new bank account. To ensure that you will not run away, they will collect the ATM card from you and give the account owner N5,000 for opening the account. After collecting the card, they will be working to defraud a major account with huge cash. This may take six months to one year to plan but once they hit their target, they will transfer the money into these numerous accounts they presently hold their ATM cards and withdraw it at the same time. This makes it difficult for them to be arrested because they are done at different locations. We only arrest those account holders who know nothing about the fraud.

This foregrounds it that fraudsters operate in a highly deconcentrated structure which makes them difficult to track. This strategy is, perhaps, made possible by their understanding of the security architecture likely to be deployed in tracking electronic banking fraud(sters). For instance, in the cited case, the security agents were only able to arrest five of the owners of the accounts whose ATM cards were collected when they applied for the job. This is because they had used their home addresses and one of them was arrested when he also tried to withdraw from the account. He had thought it was wise for him to quickly do

over-the-counter withdrawal since he was no longer in possession of his account ATM. By this time, the account had been flagged and he was arrested. The investigators, however, could not go beyond arresting this person as the arrested could not supply any useful information that could lead to the arrest of the "real fraudsters."

Abduction as 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 deploy force. A female victim in Lagos state narrated her experience:

> It happened a few minutes to 6:00 a.m. (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 messages. This loop completes a crime script which makes the fraud successful.

Fear of Fraud and Adoption of Cashless Banking

The spate of insecurity in Nigeria's cashless ecosystem is currently affecting negatively the migration of people from cash-banking to the digital/branchless or cashless banking option. This was the general expression from some of our participants who were asked why they have stuck to the cash-based banking option. Our participants decided not to migrate due to perceived vulnerability of the cashless banking system, the insecurity in the payment option, and the "indirect" experiences which they have had. And due to these reasons, they adopted avoidance behavior by staying away from their branchless banking option. According to Tyler and Lind (1992), while trust is anchored on the intentions to get a fair treatment when involved in a matter, it has the capability of affecting future behavior toward a distrusted organization or system. Defrauded bank customers may withdraw (close account) future association with a bank and migrate to another bank reputed to have security for customers' funds. It follows that, as Wemmers and Manirabona (2014) aver, experiences of victimization have the potential to produce a change in people's outlook of a system.

With respect to perceived vulnerability, participants expressed lack of adequate knowledge of how to behave under the new policy. They seemed to have difficulty understanding the technicalities involved in the cashless banking option and this may predispose them to the antics of fraudsters who are benefiting from this. We found that the avoidance behavior decision was not a function of education. Some senior academics, even in the rank of professor, stated their aversion for the new payment system which they feared would make their hard-earned money accessible to fraudsters. To them, it was easier to track their money through physical visits to the bank for transactions. When banks were limiting the amount that can be transacted in cash and "conscripting" their customers to either use the ATM or other online banking options, this group of people simply threatened to close their accounts. A professor of Political Science opined thus:

> They have described me as "old school" (unyielding to change) but I don't mind the label. I have simply told them if you are not ready to keep my money again just hand my money back to me safely. Sometimes there is a spiritual dimension to the online fraud. This people have committed their fraud by simply dialing the number of some account holders and hypnotizing them to supply their account details and by so doing made away with their money! I can't allow that to happen to me at this age. I would rather be "old school" and be safe.

It thus seemed that the awareness of other people's experiences of victimization might lead to one's adoption of safety behaviors such as this. We also found this expressed by other participants who anchored their reason for not adopting

cashless option to the victimization of their friends, boyfriends, or girlfriends. The diminished trust in the governance of the cashless policy accounted for failure to migrate as stated by another participant:

> I don't want to die by just receiving debit alert on my phone when I have not made any transaction and I will be blamed for compromising my account by the bank. If anything happens to my account I can hold the bank responsible. This fraud thing happened to four of my friends and the experiences were not palatable at all. I should learn from their experiences and not make myself a victim of the same thing.

While these vicarious victims are staying away, those who had been victimized are pulling out of their internet-banking subscription. A student whose money disappeared without transaction on her ATM card stated that,

> Excuse me why will I use the bank again? I closed my account with them and I stopped using the bank. I moved to another bank because I don't want a repeated fraud. It was more of a trust issue. I believed they could have traced the source of the fraud in-house considering the fact that it happened to other people too. They claimed somebody used my ATM and when there was no transaction on my account, they said they would do something to it. I was able to label the bank and stopped some people from banking with them in my school.

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 behavior. This threatens the adoption as well as use and facilitates 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. To understand what banking institutions and allied governance institutions do to engender trust in the policy, we asked participants questions bordering on mechanisms put in place to check fraud.

We found that weak governance structure is in part 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 CBN. 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 retained 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 fraud opportunities. Giving credence to this assertion, a fraud report by the Nigerian Deposit Insurance Corporation (2014) stated that 64% of the frauds committed in banks were perpetrated by contract/casual staff. The Committee of Chief Compliance Officers of Banks in Nigeria (CCCOBIN) at their meeting on 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 titled "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 staff 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 ATMs 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 as "BVN SCAM ALERT." This was sent to the email 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)

Another message reads:

> Our attention has been drawn to recent phishing emails sent to our customers prompting them to click on a link to update their BVN. Please disregard and delete all such emails requiring you to update account you account online or requesting your BVN details. Kindly note that BVN enrollment can only be carried out physically at any GTbank branch. GTbank, its staff or agents will never call or send you an email requesting for you to update your information via a link or over a phone. Kindly report such calls to any of the GTconnect numbers below and forward the emails to complaints@gtbank.com immediately you receive them.

These messages 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 try to refrain from public prosecution of erring staff. Our research found that bank adopts shaming as a mechanism for instilling discipline within the bank while attempting to ease 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." 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 the depositing and investing publics and the image of the organization (see Levi, 2002).

Conclusion

The study examined the 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 ICT units of banks and casual and permanent employees in fraud episodes raises question about recruitment policies and internal governance within the banking system in Nigeria. Data show 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 uncredited lodgment, fake job scam, ATM card swapping, and compromise my lovers and son, fund transfer fraud, phishing emails/BVN fraud, and DAF, 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 CBN. The "Know Your Customer" is poorly followed up making it easy for fraudulent persons to give fake addresses without being 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. 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 behavior.

Acknowledgments

The authors wish to thank Bill Maurer, Kate McKee, Ursula Dalinghaus, Mrinalini Tankha, and other participants during the session "In —— We Trust: The Contingencies of Social and Financial Protection" at the IMTFI Researchers Conference at Irvine, California, in April 2016. All omissions and errors, of course, remain the responsibility of the authors.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The article is based on a project grant (2015-3258) titled "Dimensions of Electronic Fraud and Governance of Trust in Nigeria's Cashless Ecosystem," supported by the Regents of the University of California, Institute for Money, Technology and Financial Inclusion (IMTFI), Irvine, USA.

ORCID iD

Oludayo Tade https://orcid.org/0000-0002-5997-1819

Notes

1. Lagos state has a population of about 21 million inhabitants while Oyo state has about 7.8 million.

2. Committee of Compliance Officers of Banks in Nigeria (CCOBIN) is made up of compliance officers of banks and security agencies. At this meeting, compliance officers share experiences on incidence of fraud and its dimensions. This allows security agencies to have information and guide banks on how to deal with fraud. It is also attended by regulatory bodies like the Central Bank of Nigeria.
3. 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 they were assured of their anonymity before agreeing to participate in the research. In this study, we have used pseudonyms to represent our participants and institutions.
4. The official exchange rate in Nigeria was N199 to US$1 at the time the fieldwork for this article was conducted. This is what has been used throughout the article.

References

Adogame, A. (2009). The 419 code as business unusual: Youth and the unfolding of the advance fee fraud online discourse. *Asian Journal of Social Science*, *37*, 551–573.

Agboola, A. A. (2006). Electronic Payment Systems and Tele-banking Services in Nigeria. J*ournal of Internet Banking and Commerce, 11*(3). http://www.arraydev.com/commerce/jibc

Ampratwum, E. F. (2009). Advance fee fraud "419" and investor confidence in the economies of Sub-Saharan Africa (SSA). *Journal of Financial Crime*, *16*(1), 67–79.

The ASEAN Post. (2020). Digital fraud on the rise in ASEAN. https://theaseanpost.com/article/digital-fraud-rise-asean

The Associated Chambers of Commerce and Industry of India and PWC India. (2015). *Current fraud trends in the financial sector* (28 pp.).

Bijlsma-Frankema, K., & Costa, A. C. (2005). Understanding the trust-control nexus. *International Sociology*, *20*(3), 259–282.

Blau, P. M. (1964). *Exchange and power in social life*. John Wiley & Sons, Inc.

Centeno, C. (2003). *Adoption of Internet Services in the enlarged European Union: Lessons from the Internet Banking case*. Report EUR 20822 EN. European Commission Joint Research Center.

Chiemeke, S. C., Evwiekpaefe, A. E., & Chete, F. O. (2006). The adoption of internet banking in Nigeria: An empirical investigation. *Journal of Internet Banking and Commerce*, *11*(3). http://www.icommercecentral.com/open-access/the-adoption-of-internet-banking-in-nigeria-an-empirical-investigation-1-9.php?aid=38546

Cohen, L., & Felson, M. (1979). Social Change and Crime rate trends: A routine activity Approach. *American Sociological Review, 44*, 588–688.

Cross, C. (2012). *The Donald Mackay Churchill Fellowship to study methods of preventing and supporting victims on online fraud*. Report. http://eprints.qut.edu.au/view/person/Cross,_Cassandra.html

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology, 21*(1), 187–204.

Cross, C. (2019). Is online fraud just fraud? Examining the efficacy of the digital divide. *Journal of Criminological Research, Policy and Practice*, *5*(2), 120–131. https://doi.org/10.1108/JCRPP-01-2019-0008

Das, T. K., & Teng, B. S. (2001). Trust, control and risk in strategic alliances: An integrated framework. *Organization Studies*, *22*(2), 251–283.

Davinson, N., & Sillence, E. (2014). Using the health belief model to explore users' perceptions of 'being safe and secure' in the world of technology mediated financial transactions. *International Journal Human-Computer Studies, 72*(2014), 154–168.

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

Durkheim, E. (1960). *The division of labor in society*. Free Press. (Original work published 1893)

Felson, M. (1986). Routine Activities, Social Controls, Rational Decisions, and Criminal Outcomes. In D. Cornish & R. V. G. Clarke (Eds.), *The Reasoning Criminal*. Springer-Verlag.

Felson, M. & Cohen, M. (1980). Human ecology and crime: A routine activity approach. *Human Ecology, 8*, 389–406.

General Secretariat of the Organization of American States. (2018). *State of cybersecurity in the banking sector in Latin America and the Caribbean* (181 pp.). https://www.oas.org/es/sms/cicte/sectorbancarioeng.pdf

Gouldner, A. W. (1960). The norm of reciprocity: A preliminary statement. *American Sociological Review*, *25*, 161–178. http://www.arraydev.com/commerce/jibc/2005

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, *47*, 44–57. http://dx.doi.org/10.1016/j.ijlcj.2016.07.002

Jaishankar, K. (2010). The future of cyber criminology: Challenges and opportunities. *International Journal of Cyber Criminology*, *4*(1–2), 26–31.

Levi, M. (2002). Suite justice or sweet charity? Some explorations of shaming and incapacitating business fraudsters. *Punishment and Society*, *4*(2), 147–163.

Liao, Z., & Wong, W. K. (2008). The determinants of customer interactions with internet-enabled e-banking services. *The Journal of the Operational Research Society*, *59*(9), 1201–1210.

March, J. G., & Olsen, J. (1975). The uncertainty of the past: Organizational learning under ambiguity. *European Journal of Political Research*, *3*, 149–171.

Nigeria Deposit Insurance Corporation. (2013, December). *Annual reports and statement of accounts*. www.ndic.org.ng

Nigerian Deposit Insurance Corporation. (2014). *Annual report and statement of accounts*. https://ndic.gov.ng/wp-content/uploads/2015/07/NDIC%20Report%202014.html

The Punch. (2014, June 30). *Tortuous journey to cashless economy* (pp. 39–42).

The Punch. (2015, November 9). *Concerns over rising Bank fraud*.

Rousseau, M. T., Stikin, S. B., Burt, S. B., & 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*. Free Press.

Tade, O. (2013). A spiritual dimension to cybercrime in Nigeria: The yahoo-plus phenomenon. *Human Affairs*, *23*, 689–705.

Tade, O., & 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

Tade, O., & Adeniyi, O. A. (2016). On the limits of trust: Characterising automated teller machine fraudsters in southwest Nigeria. *Journal of Financial Crime*, *23*(4), 1112–1125. https://doi.org/10.1108/JFC-04-2015-0023

Tade, O., & Adeniyi, O. A. (2017). 'They withdrew all I was worth': Automated teller machine fraud and victims' life chances in Nigeria. *International Review of Victimology*, *23*, 313–324. https://doi.org/10.1177/0269758017704330

Tade, O., & Aliyu, I. (2011). Social organisation of cybercrime among university undergraduates in Nigeria. *International Journal of Cyber Criminology*, *5*(2), 860–875.

Tyler, T., & Lind, E. A. (1992). A relational model of authority in groups. In M. P. Zanna (Ed.), *Advances in experimental social psychology* (Vol. 25, pp. 115–191). Academic Press.

Wada, F., & Odulaja, G. O. (2012). Assessing cyber crime and its impact on E-banking in Nigeria using social theories. *African Journal of Computer and ICT*, *43*(3), 69–82.

Weber, M. (1947). *The theory of social and economic organization*. Free Press.

Wemmers, J.-A., & Manirabona, A. (2014). Regaining trust: The importance of justice for victims of crimes against humanity. *International Review of Victimology*, *20*(1), 101–109.

World Economic Forum. (2018). *Global risk report*.

Zucker, L. G. (1986). Production of trust: Institutional sources of economic structure. In B. M. Staw & L. L. Cummings (Eds.), *Research in organizational behavior* (Vol. 8, pp. 53–112). JAI Press.