On the limits of trust: Characterising automated teller machine fraudsters in southwest Nigeria

Oludayo Tade
Department of Sociology, University of Ibadan, Ibadan, Nigeria, and

Oluwatosin Adeniyi
Department of Economics, University of Ibadan, Ibadan, Nigeria

Abstract
Purpose – This paper aims to investigate automated teller machine (ATM) fraud in southwest Nigeria, as extant studies have not examined the unintended consequences of ATM subscription particularly the effect of the identity of fraudsters and the strategies for defrauding.
Design/methodology/approach – Using sequential exploratory strand of mixed method, data were collected from both ATM users and victims of ATM fraud using multi-stage sampling procedure. This involved purposive selection of Lagos and Oyo states.
Findings – Results showed that fraudsters were typically lovers, friends, relatives and sometimes children of victims. Strategies for defrauding included card cloning, swapping of cards and physical attacks at ATM galleries.
Research limitations/implications – Because of the size of the sample which is small, the research results may lack generalizability. More expansive works are needed across Nigeria in this regard.
Practical implications – The paper includes implications for policy initiative concerning the deployment and use of payment systems such as ATM in Nigeria.
Social implications – The paper reveals the limits of trust in cashless policy. It raises salient policy issues concerning the need for the governance of trust to engender adoption.
Originality/value – The paper characterizes fraudsters and their strategies for defrauding.
Keywords Automated teller machine, Victim, Fraud, Lagos, Oyo
Paper type Research paper

Introduction

On 1 July 2014, the cash-less policy introduced by the Central Bank of Nigeria (CBN) became operational in all 36 states of Nigeria and the federal Capital Territory (Abuja). Hitherto, the cash-less policy was already in operation in about eight locations, distributed around business zones of the country. The cash-less policy in Nigeria aims to engender financial inclusion by limiting the volume of cash transactions. The policy stipulates a "cash handling charge" on daily cash withdrawals or cash deposits that exceed N500,000 (about US$3,030) for individuals and N3,000,000 (approximately US$18,190) for corporate bodies. The new policy on cash-based transactions (both withdrawals and deposits) in banks aims at reducing the amount of physical cash (coins and notes) circulating in the economy and encouraging more electronic-based transactions in the payments for goods, services and transfers, among others.

In designing the policy, the CBN envisions it as a means of curbing negative consequences which arise from heavy usage of cash in the economy. These include the high cost of printing cash, the high risk of using cash (such as robberies and other cash-related crimes), the

circulation of money outside the formal economy, as well as inefficiency and corruption which are more easily facilitated with cash. On the basis of the foregoing, observations about the use of cash, the deployment of electronic banking has been "touted" by the CBN as a veritable way out of the woods. For Nigeria, the setting of daily limits on automated teller machine (ATM) withdrawals is an integral part of the CBN's cashless policy. However, payment systems such as ATMs are also prone to fraud. Despite this, the perspectives of the victims that would allow policy makers make informed decisions and address emerging challenges associated with crime-related problems stemming from the cash-less policy are rarely documented. The problem is phenomenal when considering the number of users on this payment platform.

It is essential to study victims of crime because knowing them will give insight into who they are, their social habits and personality. These will provide ideas as to why they are the targets of criminals. Beyond this, with an in-depth research on victims, more can be known about the actual fraudsters. Findings from such endeavour are therefore vital in providing interventions geared towards checking future occurrences. With other words, it is then possible to unravel the susceptibility factors and the strategies used by ATM fraudsters with a view to deterring future occurrences. On the basis of the foregoing, the main research goals are therefore to characterize ATM fraudsters and probe their strategies for defrauding.

Electronic banking, for a long time the global best practise, is one of the subtleties that have more recently 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, ATMs have emerged to be the most popular service delivery channel worldwide (Centeno, 2003). However, its use is fraught with unintended consequences chief among which is ATM fraud.

Research on ATM fraud is not new in Nigeria. Scholars have examined the relationship between ATM fraud and literacy level (Obiano, 2009), the uncooperative attitude of banks in addressing ATM-related fraud in the banking industry (Ihejiahi, 2009), threat of ATM fraud to e-payment in Nigeria (Omankhanlen, 2009) and infrastructural challenges facing ATM users in Nigeria (Adeloye, 2008). In other studies not restricted to Nigeria, Okafor and Ezeani (2012) identify growth in ATM fraud with more deployment of ATM machines, while Diebold (2002) catalogues ATM fraud types. Michael (2001) looks at ATM robbery, while Furst et al. (2002) investigates ATM robbery patterns. Okafor and Ezeani (2012) were only interested in examining the use of ATM by customers in Ibadan, Nigeria. The kernel of the present study is the characterisation of fraudsters via the prism of the victims of ATM fraud in southwest Nigeria. We key into the suggestion of Jaishankar (2010) who drew the attention of scholars to the need for presenting a more nuanced social science perspective with respect to victimization of technological extraction. And as observed by Davinson and Sillence (2014) and Tade (2013), technology-mediated transactions have provided avenues for legally approved transactions and deviant opportunities and 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 (Davinson and Sillence, 2014).

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 in the kind of cash-less ecosystem m which Nigeria aspires to. 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 et al., 2006; Tade and Aliyu, 2011; Wada and Odulaja, 2012). The implication of this is that gap exists in knowledge on empirical investigation into the narratives of the victims of ATM fraud who are supposed to be the beneficiaries of these electronic payment platforms. We believe that our study is a timely intervention, as ATM fraud victims are typically left at the mercy of fraudsters in Nigeria. Banks on their part often adopt techniques of neutralization which somewhat suggest denial of responsibility (Bohm et al., 2000; Murdoch et al., 2010). Therefore, the burden bearers are the victims who have not been the focus of many researches. Helpless about unauthorized withdrawals from their account, some bank customers in 2009 sued the CBN, Interswitch and 24 banks at a Lagos Federal High Court on behalf of themselves and other defrauded Nigerians. They demanded 50 billion naira in damages to be paid to all Nigerians who have lost money through the Electronic Payment System (www.atmcommunity.com/news.php?Newsid=105). The crux of the inquiry in this paper is therefore to characterise ATM fraudsters and catalogue their strategies for defrauding based on a careful interrogation of the lived experiences of fraud victims.

Victim precipitation theory

Victim precipitation theory posits that by acting in certain provocative ways, some individuals initiate a chain of events that lead to their victimisation either passively or actively. In victim precipitation, there is an explicit time ordering of events in which victims initiate some type of action that results in their subsequent victimization (Meier and Miethe, 1993). Victim-precipitated robbery involves cases in which the victim has acted without reasonable self-protection in the handling of money, jewellery or other valuables (Normandeau, 1968; Curtis, 1974). It follows therefore that victims of ATM fraud may have initiated some risky behaviours such as disclosure of personal identification number (PIN) to loved ones or friends owing to condition of vulnerabilities (illiteracy, ill-health), non-protection of ATM cards, withdrawal of money in less secured environment, using ATM in the night and non-subscription to e-alert to monitor account which makes them prone to fraud. As Meier and Miethe (1993, p. 462) observe forms of victim involvement would include such acts as getting involved in risky or vulnerable situations, not exercising good judgment when in public places, leaving property unprotected, and interacting on a regular basis with potential offenders. It follows that ATM card holder's exposure to dangerous spaces, people and presence at a dangerous location affect their differential victimization. In other words, routine daily activities of ATM card holders may be useful factors in explaining ATM victimization. This will explain why different defrauding strategies are deployed by fraudsters taking into cognisance the profile of their victims. Likewise, education, age, marital status and gender are factors which may predispose card holders to victimization. This is because these factors explain risk-taking/involving activities.

Method

The study adopts sequential exploratory strand of mixed methods. A mixed method design is useful to capture the best of both quantitative and qualitative approaches (Creswell, 2003). Data were generated via the representation of human phenomenon with numbers (standardized questionnaire and observation) along with methods that gather and represent the phenomenon of e-payment fraud with words (open-ended interviews and unstructured observation). According to Denzin (1978), multiple methodological traditions have an honoured history of enhancing confidence in the validity of findings by viewing a phenomenon from different lenses. This approach has been successfully used by Greene et al. (2005) and Okafor and Ezeani (2012).

The study used multi-stage sampling procedure in selecting research settings and respondents for the study. There are six states in the southwest zone of Nigeria. These are Lagos, Ogun, Osun, Oyo, Ekiti and Ondo states. Of these, Lagos and Oyo states were purposively selected due to the large pool of ATM users they have. While Lagos state is reputed as the commercial engine room of Nigeria, and hence, the location of most bank headquarters, Oyo state is estimated to have the second largest pool of banks in the region owing to its size and population.

In the two states, most banks are located in Central Business Districts. Hence, most respondents were recruited near ATM galleries for the quantitative analysis. The main criteria for inclusion were possession of an ATM card and utilization. However, victims were reached through the snowball method after identifying a victim through the help of informants within banks, referrals and relatives of other victims. Data collection proceeded from qualitative to quantitative. The intent was to first explore the problem under study and then follow-up on this exploration with the quantitative data that are amenable to studying a large sample so that results might be inferred to a population. For the qualitative data, 30 in-depth interviews were conducted with victims (15 in each state), while ten key informant interviews were conducted with the ATM custodians in banks. The responses from the qualitative methods were used in developing a more elaborate quantitative instrument. The in-depth interview guide for victims focused on their personal experiences, the identity of fraudsters and the strategies used to defraud. Quantitatively, a total of 1,100 survey questionnaires were administered. Although, all ATM users had equal chances of been included in the study, accessibility, availability and consent guided the administration of instrument. Following non-retrieval and invalid responses, a little less than 700 questionnaires were used for the subsequent analysis.

The interviews for this study were carried out with a digital audio recorder to facilitate the onward download of the recorded conversation onto the computer for editing. The use of digital audio recorder is to have an effective alternative to storing and managing audio data and ensure that the sound quality of the recorded interview is clear, audible and does not deteriorate with repeated use (Maloney and Paolisso, 2001). The audiotaped interviews were transcribed to enhance accuracy, dependability and to enhance the integrity of data analysed. Stop checking of the transcribed tapes was done to ensure the trustworthiness and validity of the interviews. Only texts with analytical contributions to the study were considered. After all the sorting and consequent content analysis, respondents' narratives were then reproduced as accurately as possible. We also use some Yoruba social thoughts as represented by proverbs in analysing trust as a precondition in social relationships.

To analyse the quantitative data which emerged from the questionnaire, descriptive and analytical techniques were used. This is because the intention is to describe systematically the phenomenon of e-payment system use and its challenges from the perspective of actors in general and victims in particular. The major descriptive method adopted is the use of frequency distribution on the basis of percentages.

Findings and discussion

Socio-economic profile of automated teller machine users

With respect to ATM usage, Table I shows that a little more than half (50.3 per cent) of the respondents were in the 21-30 years age bracket, while only 2.3 per cent were aged 50 years and above. The distribution by sex shows that 55 per cent were females, while the remaining 45 per cent were male respondents. The proportion of married people who use ATM services (34.4 per cent) was just a little more than half that of singles (63.9 per cent). In this study, education also appears to correspond with ATM usage, as the larger chunk of respondents (80 per cent) of respondents had higher degrees, namely, HND, BSc, MSc and PhD in that order. ATM users were found to be predominantly Christian, although one-fifth of respondents were Muslims. In terms of length of usage, 12.7 per cent of the respondents had been using their ATM cards for periods less than a year, while an equal number (12.3 per cent) had had their cards for six years or more.

Most of these respondents (Table II below) voluntarily requested for ATM cards from their banks, while a considerable proportion of respondents were coerced by their banks via the imposition of prohibitive charges on over-the-counter withdrawals. Cash withdrawal was the preeminent motif for ATM handling with a strict preference for own bank ATMs (82 per cent) vis-a`-vis the ATMs of other banks (18 per cent). With spending patterns in the spotlight, 43.1 per cent of respondents claimed that ATM use had reduced the way they spend, while on the contrary, 49.6 per cent expressed the view that they had experienced increased spending. This near bifurcation of responses plausibly relates to the lifestyle demands and routine activities of respondents. The available ATM types (Inside Bank ATM, Drive-Through ATM and Through-The-Wall ATM) were unsurprisingly the most frequently used by respondents. Interestingly also, while 65 per cent of respondents reckoned the ATM services offered by banks as average to poor, majority (42 per cent) had never made a formal complaint to their bank.

Table I. Profile of respondents

	Frequency	(%)
Age		
16-20	78	11.8
21-25	179	27.2
26-30	152	23.1
31-35	84	12.7
36-40	64	9.7
41-45	50	7.6
46-50	37	5.6
50+	15	2.3
Total	659	100.0
Sex		
Male	297	45.1
Female	362	54.9
Total	659	100.0
Marital status		
Single	421	63.9
Married	227	34.4
Divorced	4	0.6
Widowed	3	0.5
Separated	4	0.6
Total	659	100.0
Education		
No formal education	2	0.3
Primary school	3	0.3
Secondary school	52	7.9
National Diploma	82	12.4
HND	106	16.1
BSc	326	49.5
MSc	77	11.7
PhD	12	1.8
Total	659	100.0
Religion		
Christianity	530	80.4
Islam	127	19.3
Traditional	2	0.3
Total	659	100.0

Table II. Factors underlying the use of ATM cards

	Frequency	(%)
Decision to obtain ATM cards		
I voluntarily asked my bank	561	85.1
My bank forced me through charges	98	14.9
Total	659	100.0
Uses of ATM card		
Check my account balance	378	57.4
Withdraw cash	614	93.2
Recharge my phone	235	35.7
ATM and spending		
It has reduced the way I spend	284	43.1
It has increased the way I spend	327	49.6
No response	48	7.3
Total	659	100.0
ATM use Preference		
I prefer to use ATM of my bank	537	81.5
I like to use ATM of other banks	122	18.5
Total	659	100.0
ATM location and customer use		
Inside the bank	391	59.3
Drive-through ATM	105	15.9
Through-the-wall ATM	204	31.0
Transport Hub ATM	17	2.6
Inside Hotel/Store ATM	39	5.9
Complaints to bank about ATM problems		
Yes	387	58.3
No	272	41.7
Total	659	100.0

Identifying vulnerability factors and characterizing automated teller machine fraudsters

We asked our participants (victims of ATM fraud) what factors they thought predisposed them to fraud. While several factors were listed and explained, the origin of their vulnerability was traced to the introduction of a policy by Deposit Money Banks on the limits of daily withdrawal in line with the directive of the CBN. The CBN introduced a policy on e-banking which has as one of its the cardinal focus to decongest the banking halls and ensure that the banking public embraced the use of ATMs. As adjusting to change usually requires a period of contestation with the new

policy, government handed down a directive to banks to impose a limit on withdrawals from customers using their banking halls. This limit restriction provides that the customer who intends to withdraw below N100, 000[1] (US$625) does so at the machines[2] or pays N100 (US$0.625) for each withdrawal made on the counter. Using cost-benefit analysis of the policy on their savings, bank customers appear to have rationalized by favouring the use of ATMs.

However, since not all customers are literate or educated on how to operate with the ATM card, they become vulnerable. Therefore, illiteracy was identified as one of the vulnerability factors predisposing our participants to fraudsters. The challenge on the use of ATM as reported by participants was inadequate education or enlightenment of the customers on the use of ATM cards. Most card holders, and in particular the illiterates, face challenges at understanding the components of e-banking at the point of withdrawing. In the course of this research, the first author was asked by an aged man to help in withdrawing at a public ATM machine. He asked the aged man about the PIN, and the man "released" it. This provided unlimited access to the content of the account and ample room for opportunistic crime. An ATM custodian indicated that card swapping was a strategy used by ATM fraudsters to defraud illiterate customers, mostly the aged:

> One very old illiterate man came to our bank to report to us that certain amount was debited from his account despite the fact that ATM did not dispense when he used it. But when we requested him to tell us his account and bring his card, he gave us the card belonging to another person. It was there he told us that he asked a boy to assist him in withdrawing but after failed attempts, the boy swapped the cards. He gave his card to the old man and went away with the old man's card apparently because he accessed the account and found that the old man had more money in his account.

Davinson and Sillence (2014, p. 157) note "technology designed without thought to the users' cognitive, social and cultural understandings is likely to fail its objectives and increase the likelihood of users acting insecurely". Indeed, ATM researches have established that insufficient knowledge of ATM operation by users may lead them to embrace insecure behaviour such as improper management of PINs and passwords (Proctor et al., 2002). Fraudsters are opportunistic criminals who key into the vulnerabilities of victims. This may be the case no matter how much they are elevated by the potential victim on the scale of trust. Participants' narratives indicated that fraudsters' key into the condition of vulnerability of victims and downplay or leverage on the position of trust between them to carry out fraudulent transactions on their account and later feign ignorance of the same. E-payment platforms such as ATM shave thrown up challenges of trust in social relations. Trust is a virtue which is not evenly embraced by people in the social world. Indeed, not all persons trust the other due to the complexities in understanding human behaviour. This analogy applies to ATM fraud. Children, relatives, husbands and friends were reported as fraudsters by our participants. The level of trust degeneration in modern societies is alarming. The worldview of the Yoruba people highlights the failure of trust among kin and non-kins with serious implications for social relations. Some maxims in the Yoruba view of trust strengthen our analysis here: *eni a ni ko feni loju fi ata senu* (the person asked to assist in blowing off the dirt in the eyes has pepper in his mouth), and *eni a ni ko kinni leyin fi egun sowo* (the person asked to assist in scrubbing the back has thorns in his hand). The former maxim shows the importance of not entrusting a highly treasured organ such as the eyes to a person whose desire is to impair one's vision. The latter proverb warns about entrusting the task of

watching one's back to a person who will claim to be nice but backstabs. The consequences of not adhering to the implied wisdom in these proverbs may be costly. And this is why the Yoruba believe that an acquaintance thief paves way for the outsiders. Thus, if there is no death within one's household, one cannot be hurt by a death from without (*Bi iku ile o ba pani, ti ode o le pani*). These social thought emphasizes an insider factor to the occurrence of crime in the social world. This insider may in some instances be the domestic servant who was employed to assist an aged parent. Due to weakness or health challenge, the aged may not be strong enough to queue up at the ATM gallery and may therefore opt to send the domestic servant on errand. Doing this means risking two things:

(1) the PIN of the account holder is released to this insider; and
(2) the PIN will provide access to the details of the account which could be used personally or in concert with an outsider to defraud the aged.

While explaining how she was defrauded before detection, an aged woman said:

> I sent my domestic staff to the bank to make withdrawal for me at the ATM. I asked her to withdraw N20, 000 ($125). Before she got back home I got alert of N40, 000 ($250) and waited for her to return. When she got back home, she gave me N20, 000 ($125) and I asked her about the remaining balance, she insisted she withdrew N20, 000. I showed her the alert on my phone but she was still denying. I then dressed up and we went to the bank. It was when the bank staff threatened to arrest and jail whoever did it that she owned up that it was true that she made the withdrawal.

The son of a card holder may be the fraudster as narrated by this respondent. He was defrauded by his son:

> My son was to return to school and asked her mother to give him money but she gave him N1, 000 ($6.25). I then gave him my card to go to the bank and withdraw N5, 000 ($31.25) but you won't believe it that he withdrew N10, 000 ($62.5). He came back and dropped the card. I went to the bank only to discover what he had done. I told the mother. So if my son could do that to me while trying to help him, who else cant he do that to?. It was possible for him to have made the withdrawal because he would have checked my balance while trying to withdraw the money.

The narratives above affirm the limitation of trust in e-transactions. In other words, one's family members may constitute the first threat and hence be suspects in ATM fraud. This is because the position of the card holder in the family determines those considered contextually trustworthy to have access to confidential information such as those concealed in ATM transaction. However, e-transactions raise issues of how a father begins to distrust his son or husband against his wife and vice versa. Although the fraudster and the victim may be of the same moral community, trust may be downplayed when the former is confronted with unequal economic opportunity. Uslaner (2004) argues that economic inequality tears apart the bonds that bind people together in any society. As such, the fraudster may not fritter away an opportunity to enhance personal economic standing when such opportunity materializes.

Ill-health is another vulnerability condition often used by ATM fraudsters to defraud victims. These categories of fraudsters are familiar to the victims. When persons become ill and need money to transact or purchase items, they may seek the assistance of their caregivers because they may be too weak to personally make withdrawals. During the period of illness, the weak is at the mercy of those who show concern, but this may bring unintended consequences of fraud if the "trusted" person has instinct for opportunistic crime. Usually, those close to a sick person are usually family members or very close friends. A male victim narrated thus:

> I was in my house one morning around 7am to 8am sleeping when I got an alert on my phone indicating a withdrawal of N20,000 from my account. I jumped out of my bed and it was the alert that woke me up. I was not settled with the puzzle of debit alert when another alert came indicating the withdrawal of another N20,000. Within some minutes another one came (N20,000) and as I rushed down to the bank I got another one (N10,000) making a total of N70,000. I was depressed and surprised. I asked myself when? How? When I got to the bank, I started shouting and the bank security calmed me down and asked me to speak with the customer care people. I narrated my story and the bank officials were trying to say I was embarrassing their bank. I told them I needed to know the person who defrauded me. I later found out the person […] he was my friend. The bank helped me find the person through the ATM CCTV camera footage which showed him when withdrawing. My card was not missing and I always keep my card in my wallet. And when I was sleeping, I hung it on the wall. He must have picked it from my purse but I remember that there was a time I was ill and needed money to buy drug. I was too weak to stand up and I had no cash on me. So I gave him my ATM card and told him my PIN to withdraw the needed money in order for me to use it to buy the drugs I needed. It was therefore a surprise to me that I saw him in the footage.

Apart from being a close friend, the fraudster understood the routine activity of the card owner and where the card was kept. An acquaintance fraudster may also be a lover or spouse. With such closeness, the potential victim is less suspicious. Also in some relationships, it is a sign of love to be open about everything including the amount earned, the PIN of the account of spouse and other things otherwise held confidential in other social relationships. When a spouse is the fraudster, the bond is threatened and sometimes may be difficult to track. It follows that the fraudster spouse may likely feign playing an active role in the search for the "criminal". This played out in the case of a woman defrauded by her husband as narrated by a bank ATM officer:

> You see, sometimes most of the fraudsters are persons known to the victims. There was a time when one of our big customers came to complain that the sum of N200, 000 was withdrawn from her account and demanded the bank to ensure that the thief was unveiled. We calmed her down and tried to retrieve the CCTV footage on the day of transaction. Fortunately she came to the bank with her husband who was accusing us of incompetence. By the time the footage was played, the woman realized it was her husband that actually withdrew the money. She apologized and she left with her husband in shame.

However, not all ATM frauds are perpetrated by friends and relatives; some are perpetrated via coercion particularly through physical attacks at ATM galleries. By coercion, we mean armed robbery and use of physical violence. It may be argued that the seeming difficulty in breaking some security features introduced into ATM cards has introduced another strategy into ATM frauds in Nigeria. Some participants narrated that they were defrauded while trying to withdraw from the ATM gallery on a weekend. The mastery of the routine activity of people may have made this type of strategy a huge success. This mostly takes place during weekends, in the night or early in the morning when there is a noticeable low traffic in certain neighbourhoods or when security is limited. Banks are unlikely to open for business during the weekend. Hence, it will be difficult to seek help in case of forceful seizure of phone and ATM cards. A victim explains thus:

> It was on a Sunday close to a year ago. I wanted to go out but with limited cash that can take me for the outing. The ATM on my street was not working or should I say it was not dispensing cash. So I had to look for another ATM at another location to make withdrawals. Unfortunately when I got there, I was a victim of an armed robbery gang. I was robbed at gun point. They got my ATM and my PIN and they left and it was on a Sunday so I could not do anything until Monday. But before I could do anything about it my account was drained of N200, 000 ($1,250). They had asked me to insert my ATM, confirmed the PIN number and my balance. This was done at gun point. Someone was shot dead there otherwise I would not have given it to them. This was around 3pm-4pm. It is a normal traffic place but it was a Sunday and people don't patronize that place on Sunday and so less busy. They cashed the money ($1250) twice. They went away with my phone so I could not even get the alert.

In this instance, the confirmation of the PIN was to ascertain that the owner was not lying, while the seizure of phones was to demobilize him in seeking help. The day and time of the operation are also strategic. Sundays are low traffic days in most parts of southwest Nigeria. During this time, economic activities are at low ebb, while people stay mostly in-doors in preparation for work the following day (Monday).

Getting access to the secret code of ATM cards remains largely coded within the network of fraudsters. ATM fraudsters also defraud through cloning of cards. Fraudsters could use the secret numbers peculiar to ATM cards to cloned the card and eventually use it elsewhere to withdraw. They may also have access to some confidential information about the card holder which could be strategic in getting the PIN of the owner. It is not impossible to work with some information on the internet or through an insider. An ATM custodian[3] in a first generation bank said:

> We have received and treated some of those cases before in our bank. I am saying it is possible for your card to be cloaned and used elsewhere to withdraw while you still have your original cards with you.

The narration of the ATM custodian explained why some of our participants found it difficult to fathom why their accounts were debited while they had their cards on them. Although the card may be cloned, compromised bank staffs were reported to be involved in ATM fraud:

> I was just at home and my card was with me and I got an alert that about N50,000 has been withdrawn. I was surprised but I thought the machine was having some problems because it was on a Saturday. So the following Monday I went to bank to report but I was told to go the branch where I opened the account. I could not go there due to the nature of my work. I was told to write a letter and then they started posting me to come back today and tomorrow without any hope of getting my money. Because of that I stopped using the bank. I withdrew all my money and changed to another bank. After some months we heard some news that the staff of the bank were into such scam because of the access they have to account details.

Conclusion

This study examined ATM fraud in Southwest Nigeria from the perspectives of the Victims. As a form of electronic payment, studies have documented that new technologies have the potential of creating opportunities for both legitimate and illegitimate transactions (Tade, 2013). While ATMs remain the most patronized payment platform in Nigeria, it is laden with challenges, particularly fraud. Hence, we investigated the vulnerability factors, characterized fraudsters and outlined their strategies for defrauding victims.

To own ATM cards, bank customers have two options: by voluntary request and by coercion. At the inception of the cash-less policy, banks adopted a radical approach which aimed at decongesting the banking halls by imposing charges on manual withdrawals. Such imposition conscripted customers to obtain ATM cards. It also accounted for subsequent voluntary request of ATM cards by bank customers. As a rational strategy, holders of ATM cards have unhindered access to their money and this saves time. This is because ATMs are largely used for cash withdrawal, checking of account balance and other e-payment services. ATM card holders prefer to use the ATM of their banks to that of other banks. This is to remove the bottlenecks associated with dispense errors and fraud.

A number of vulnerability factors exposed ATM holders to victimization. These include illiteracy, illness, inadequate enlightenment on the use of ATM cards by banks and failure of card holders to subscribe to account e-mail alert. These factors, jointly or separately, increase the susceptibility of ATM holders to being defrauded. More importantly, cashless policy has thrown up the issue of trust management in electronic payments. This is because perpetrators of ATM frauds are those the victims were most exposed to in their lifestyle. They included friends, lovers, domestic servants and relatives. Arising from the findings, there is the need for the CBN and Deposit Money Banks to enlighten the banking public on the use of ATMs and its components, and ensure that the specific socio-demographic characteristics of the banking public are put into consideration in designing such policies. This will reduce fear in the new payment system, build confidence and engender financial inclusion. As routine activity has become a tool for victimization, it is important for banks to provide better physical security around ATM galleries, locate ATMs in “safe” areas and advise customers on the implications of using ATMs in low traffic situations. Policy makers and executors need to take on board the peculiarities of their markets and block loop-holes which may threaten the utilization of transactions on e-payment platforms. Adopting cashless option in purchases may provide opportunity for ease of transactions but securing the platform will engender trust.

Notes

1. The calculation was done using USS$1 to N160 in the foreign exchange market.
2. In Nigeria, the daily withdrawal limit for most banks at the ATM is N100,000 (US$625).
3. This is the official designation of bank staff in charge of ATM-related services.

References

Adeloye, L.A. (2008), "E-banking as new frontiers for banks", *Sunday Punch*, Vol. 14 No. 1, p. 25.

Agboola, A. (2006), "Information and Communication Technology (ICT) in banking operations In Nigeria: an evaluation of recent experiences", available at: www.iisit.org/Vol6/IISITv6p373-393Olatokun631.pdf (accessed 10 April 2011).

Bohm, N., Brown, I. and Gladman, B. (2000), "Electronic commerce: who carries the risk of fraud?", *Journal of Information Law Tech*, Vol. 3 No. 1.

Centeno, C. (2003), "Adoption of e-services: I-banking in the candidate countries", Report no. 77, IPTS, Sevilla, pp. 14-23.

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.

Creswell, J.W. (2003), *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*, Sage Publications, Thousand Oaks.

Curtis, L. (1974), "Victim-precipitation and violent crimes", *Social Problems*, Vol. 21, pp. 594-605.

Davinson, N. and 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 of Human-Computer Studies*, Vol. 72 No. 2, pp. 154-168.

Denzin, N.K. (1978), *The Research Act: An Introduction to Sociological Methods*, McGraw-Hill, New York, NY.

Diebold, I. (2002), "ATM fraud and security: white paper", New York, NY.

Furst, K., Lang, W. and Nolle, E.D. (2002), "Internet banking development and prospects: Working paper", Center for Information Policy Research, Harvard University, Cambridge.

Greene, J.C., Kreider, H. and Mayer, E. (2005), "Combining qualitative and quantitative methods in social enquiry", in Somekh, B. and Lewin, C. (Eds), *Research Methods in the Social Sciences*, Sage publications, Thousand Oaks, New Delhi.

Ihejiahi, R. (2009), "How to fight ATM fraud online", *Nigeria Daily News*, Oja, 21 June, p. 18.

Jaishankar, K. (2010), "The future of cyber criminology: challenges and opportunities", *International Journal of Cyber Criminology*, Vol. 4 Nos 1/2, pp. 26-31.

Liao, Z. and 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.

Maloney, R.S. and Paolisso, M. (2000), *Field Methods*, Vol. 13 No. 1, pp. 88-96.

Meier, R.F. and Miethe, T.D. (1993), "Understanding theories of criminal victimization", *Crime*

And Justice, Vol. 17, pp. 459-499.
Michael, S.S. (2001), "Robbery at ATM: problem-oriented guides for police series problem-Specific Uides Series No. 8", New York, NY.
Murdoch, S., Drimmer, S., Anderson, R. and Bond, M. (2010), "Chip and PIN is broken", *2010 IEEE Symposium on Security and Privacy*, doi: 10.1109/SP.2010.33.
Normandeau, A. (1968), "Trends and patterns in crimes of robbery", Doctoral dissertation, University of Pennsylvania, Philadelphia.
Obiano, W. (2009), "How to fight ATM fraud", Nigeria Daily News, Oja, 21 June, p. 18.
Okafor, 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 No. 7, pp. 18-34.
Omankhanlen, O. (2009), "ATM fraud rises: Nigerians groan in Nigeria", *Daily News*, London, 21 June, pp. 8-10.
Proctor, R.W., Lien, M.C., Vu, K.P.L., Schultz, E.E. and Salvendy, G. (2002), "Improving Computer security for authentication of users: influence of proactive password restrictions", *Behavior Research Methods*, Vol. 34 No. 2, pp. 163-169.
Tade, O. (2013), "A spiritual dimension to cybercrime in Nigeria: the yahoo-plus phenomenon", *Human Affairs*, Vol. 23 No. 4, pp. 689-705.
Tade, O. and Aliyu, I. (2011), "Social organisation of cybercrime among university undergraduates in Nigeria", *International Journal of Cybercriminology*, Vol. 5 No. 2, pp. 860-875.
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. 2, pp. 69-82.

Further reading

Agbro, J. Jr., Ohai, R. and Afolabi, B. (2012), "Living in the shadow of hackers", *The Nation Newspapers*, available at: http://thenationonlineng.net/new/insight/living-in-the-shadowof-hackers/ (accessed 21 October 2012).
Emeka, A. (2007), "Fraud alert - banks raise fresh alarm on ATMs", *Vanguard Newspaper*, Lagos.
Ezeoha, A.E. (2005), "Regulating internet banking in Nigeria, problem and challenges- part1", *Journal of Internet Banking and Commerce*, Vol. 10 No. 3, available at: www.arraydev.com/commerce/jibc/2005
Mimiola, O. (2012), "Plight of 70-year-old ATM user", *The Nigeria Tribune*, available at: www.tribune.com.ng/sun/wakabout/7881-plight-of-70-year-old-atm-user (accessed 15 July 2012).
Nuth, M.S. (2008), "Taking advantage of new technologies: for and against crime", *Computer Law and Security Report*, Vol. 25 No. 5, pp. 437-446, available at: www.sharpedgenews.com/index.php/news/recent-news/139-357-nigerian-bank-employees-caught-in-atm-fraud-in-2010-ndic-report

Nweze, C. (2012), "Banks raise Daily ATM withdrawal limit", available at: http://thenationonlineng.net/new/business/money/banks-raise-daily-atm-withdrawal-limit/ (accessed 10 October 2012).
Ogunsemor, A.O. (1992), "Banking services: the emergence and impact of electronic banking", *The Nigerian Banker*, Abuja, January – March.
PM News (2012), "Banker jailed over ATM fraud", available at: http://pmnewsnigeria.com/2012/03/31/banker-jailed-over-atm-fraud/

About the authors

Dr Oludayo Tade obtained his Doctor of Philosophy from the department of Sociology, University of Ibadan. He specializes in social problems and criminology. Dr Tade is also a media expert. His experience spans over a decade in reporting in the southwestern part of Nigeria. A number of his scholarly publications on cybercrime, piracy, child trafficking, family issues, transactional sex/prostitution and juvenile delinquency, among others, have appeared in learned international journals. Dr Tade is an Associate member of the Nigerian Institute of Public Relations (NIPR) and a Member of the Nigerian Union of Journalists (NUJ). He is also a Member of the Nigerian Anthropological and Sociological Association (NASA). He is a fellow of the Institute for Money, Technology and Financial Inclusion at the University of California, Irvine, USA, and the Council for the Development of Social Science Research in Africa (CODESRIA), Dakar. He has won several travel and research grants. Oludayo Tade is the corresponding author and can be contacted at: dotad2003@yahoo.com

Oluwatosin Adeniyi teaches at the Department of Economics, University of Ibadan, Ibadan. His research interests are in the areas of criminology, development economics and socio-economics. More recently, he has expanded his interest especially into some aspects of African economic history and economic anthropology. He is also a Fellow of the Institute for Money, Technology and Financial Inclusion (IMTFI) at the University of California, Irvine, USA. He has published on a broad range of economic issues in reputable scholarly journals.

The authors appreciate the financial support of the Institute for Money Technology and Financial Inclusion (IMTFI) at the University of California, Irvine, USA, on the project titled "Automated Teller Machine Fraud in Southwest Nigeria: The Shoe Wearer's Perspectives". The authors equally thank Bill Maurer, Jan Chipchase and other participants at the IMTFI Fifth Conference for Funded Researchers held at IMTFI, University of California, Irvine, USA, from 4 to 6 December 2013, for their insightful comments. Nonetheless, all errors remain the sole responsibility of the authors.