

## **“I prefer to remain old school and be safe”: Fear of Fraud and Governance of Risk in Nigeria’s Cashless Ecosystem**

Oludayo Tade and Oluwatosin Adeniyi

### Research Article

#### ABSTRACT

This article provides insight into the prevalence of fraud in Nigeria’s financial cashless ecosystem and how trust is being built in the system to check the growing menace. It is motivated by two overarching questions: Does fear of fraud constitute an impediment to financial inclusion? How does the existence or otherwise of risk governance mechanisms mediate the nexus between electronic fraud and financial inclusion? Using qualitative methods to probe participants in southwestern Nigeria on these issues, the findings show how fear of fraud, indirect experiences of fraud, and fraud governance shape adoption and behaviour in the Nigerian banking system.

**Keywords:** *Electronic Fraud Prevalence, Risk Governance, Cashless Economy, Deposit Money Banks*

#### INTRODUCTION

Does the fear of fraud constitute an impediment to financial inclusion? How does the existence or otherwise of risk governance mechanisms mediate the nexus between electronic fraud and financial inclusion? These two high-level questions are the thrust of the empirical exercise that we pursue in this paper. As a foretaste, this introductory discussion proceeds by initially situating the paper within the broader context of financialisation. We then go further to espouse the financial inclusion drive of the Nigerian government while juxtaposing this with the clear and present danger posed by pervasive electronic fraud. The core research questions (sub-level questions) are highlighted in line with the value-addition proposition of the study.

Financialisation encompasses the processes and frameworks for embedding finance in everyday societal experience. Over the past three decades, it has grown significantly and changed in form, structure, and operationalisation (Pike & Pollard, 2010; Walsh, 2018). The implied notion that finance in itself and access to it are tools for improving development

outcomes, such as poverty alleviation and income redistribution, has received substantial attention in the literature, with the weight of the evidence appearing to tilt in the direction of the dominant view, namely that financial constraints are binding on the poor and hence must be removed to lift those who occupy the bottom portions of the income strata out of their quagmire. This mainstream narrative, to a large extent, underpinned the global embrace of the microfinance mantra of the 1990s and its “evolution” (although some authors argue “replacement” is a more accurate reflection of the observed changes) into the debate on financial inclusion and its ascribed benefits for the poor (Mader, 2017).

As robustly argued by Mader (2017), financial inclusion is propped as central to the development prospects of poorer nations by its proponents, who claim it confers benefits in at least three dimensions. First, it facilitates development outcomes on a broad scale. Second, it is functional for poverty reduction initiatives. Third, it is also, in the end, a good business opportunity. Despite this rather rosy picture, financial inclusion continues to be a contentious subject in the academic literature and policy circles. These contestations are wide-ranging and cover disparate opinions in terms of the definition of the concept, choice of indicators for its calibration, as well as who governs the “enterprise” (external actors or the poor people themselves or both) among others.

However, many developing countries, including Nigeria, still buy into and vigorously pursue the financial inclusion agenda under various institutional arrangements within specific national economies. The remarkable success recorded by the M-PESA revolution in Kenya provided added impetus for the pursuit of the possibility to positively impact the lives of the poor by providing innovative financial services and products. In Nigeria, to be specific, this drive for a transformational mobile money environment within the financial landscape seems to have remained elusive. This is highlighted by the very low mobile money uptake figures recorded for Nigeria (for instance, only 2% of adults accessed mobile money services in 2016 as revealed by the Wave 4 FII Tracker Survey). Therefore, as a complementary route for achieving its financial inclusion aspirations, the monetary authorities, on behalf of the Nigerian government, embarked on the adoption of a cashless policy regime in 2014. The central aims of this move included engendering financial inclusion, albeit indirectly through limits on the volume of cash-based transactions, minimising the huge cost of cash minting, lowering the incidence of cash-related robberies and other crimes, better tracking of currency circulation in the hidden (underground or shadow) economy, and stemming the tide of corruption which is easy to facilitate using cash (Tade & Adeniyi, 2016). While this cashlessness experiment has been extended to all 36 states in Nigeria as well as its federal capital (Abuja), the coincidence of substantial and incrementally magnifying electronic fraud activities stands to reason as a potential drag to the attainment of progress on the government’s ultimate goal of promoting financial inclusion via providing a cashless ecosystem conducive for such purpose. To offer a sense of the scale of the challenge, Tade and Adeniyi (2017a), using statistics obtained from the reports of the Nigeria Deposit Insurance Corporation (NDIC) – the national deposit insurance authorities – for 2013 and 2014, stated that “...a total of 3,756 fraud cases were recorded in 2013. The amount involved was N21.79 billion (\$136.19 million) which represented a 21% increase compared with the N18.05 billion (\$112.81 million) officially documented for 2012. In 2014, the 10,612 reported fraud cases

represented almost a three-fold increase from the previous year. Nonetheless, the configuration of these fraud cases by type showed similar patterns for both years.”

The preceding state of affairs thus raises some pertinent questions about the compatibility of the financial inclusion drive with the concurrence of widespread electronic fraud within the same financial landscape. Specifically, we seek in this paper to inquire into the following: How does the public perceive and frame electronic fraud? Do such framings influence decisions to adopt and use financial innovations? In what clear directions are these influences observed? What do gatekeepers (such as banks and regulatory institutions) do to tackle fraud risk? And what useful lessons for policy can be apprehended from the answers to the preceding questions? The present study attempts to provide insights into all these within the context of southwest Nigeria, which is unarguably the financial nerve centre of the country as well as the hub of commercial activities.

While extant studies have examined diverse aspects of the broader associations between cybercrime and financial sector development in Nigeria – the characterisation of fraudsters (Tade & Adeniyi, 2016), potential victim profiling (Tade & Adeniyi, 2017b), fraud victimisation and victims’ life chances (Tade and Adeniyi, 2017a), and fraud and trust governance (Tade & Adeniyi, forthcoming) – very little attention has been paid to the role of fraud risk and its attendant fear on financial inclusion on one hand as well as the place of the approaches to the governance of such risk on the other hand. This is the gap that the present study fills.

In what follows, we provide a brief documentation of the relevant literature. Also, we detail the methodological aspects of the enquiry and discuss the results. Finally, the conclusion and plausible policy implications are offered in closing the paper.

## BRIEF LITERATURE REVIEW

The literature on financial inclusion, broadly put, is both vast and wide. Hence, this section is not devoted to an exhaustive discussion of the literature. Nonetheless, to highlight aspects relevant to the present study, some space is given to concise renditions of some studies. Beck et al. (2015) focused on the linkages between financial inclusion and innovation in Africa. They reported a concurrence of wider access to financial services (greater financial inclusion in their terms) and marked heterogeneity of this outcome across sub-regions. They suggest that the progress achieved via deeper inclusiveness of the financial space has brought newer dimensions of risk into focus. Arguing from the perspective of the role of external actors, such as the international donor community, Johnson and Williams (2016) beam the spotlight on real and perceived tensions that arise from donor involvement in driving financial inclusion as a reform agenda, especially in developing countries with governments that have a penchant for active participation in reforms. The authors carefully navigate diverse political economy and contextual considerations, which will make donor policy fit for purpose and simultaneously engender buy-in from recipient countries’ governments. Specifically, the authors make a case for ‘pro-market activism’ in pursuing financial inclusion as a policy priority.

Mader (2016), in contrast, offers a nuanced critique of the financial inclusion superstructure. With a focus on digital financial inclusion, he rigorously demonstrates the dearth

of credible and generalisable evidence to support the intrinsic pro-poor attributes of what he calls the three holy grails of financial inclusion. This tripartite grail includes capitalising on the everyday costs of transactions, analysing big data generated by poor people in their basic decision-making processes, and exerting greater governmental control over poor people's money. According to Mader, digital monies also require (just like cash) some back-end physical and institutional infrastructure, which are equally not costless. Furthermore, he argues that the big data obtained from the poor will create big business opportunities for data management companies that service clients such as large financial corporations and interested networks like the economics profession. Together, these will rather leave the poor in more precarious situations than their prior experiences. Implicit in the preceding arrangement is the hierarchical structure of power relations, which typically delivers little or nothing to the vast majority of intended beneficiaries – the poor. Johnson (2016), along this train of thought, examined the power relations suggested by various forms of institutions for attaining financial inclusion in Kenya. More precisely, the author probed into the financial practices of the poor and the kinds of social relations that underline their interactions with mobile payment options. It was found that patronage levels were highest for mobile money operators, followed by informal financial groups, while banks were the least likely to attract the interests of the poor. The author then constructs this evidence as a consequence of poor people's notion of the acceptable "equality" and "negotiability" that epitomise the perceived vertical relationship in the former two modes as against the discouragement characteristic of the hierarchical interactions in the case of the latter mode (deposit money banks). The submission is ultimately that failure to apportion effort to an understanding of the social contexts and social relations that surround decision-making may significantly constrain the intention to extend financial services to the poor in the mould of financial inclusion.

Speaking of social context, one key element of the financial ecosystem is the fraud and criminal landscape. The structure and operations of this will, of course, differ based on peculiarities in both finance and crime under varying contexts. For example, Cross (2017) provided evidence from Australia showing the prevalence of financial elder abuse through identity crime. In her study, with 29 elderly participants, most had compromised their identity knowingly or unknowingly, partly due to a misplaced understanding of the risk and probability of occurrence of fraud. Hence, it is imperative to retain a strictly focused perspective on specific contexts in gleaning an understanding of the fraud risk-financial inclusivity nexus. In what ensues, the emphasis shifts to an abridged but informative itemisation of related studies on the Nigerian financial ecosystem.

It should be noted that an assortment of studies has examined aspects of the subject matter within the Nigerian space. In no particular order, the existing literature has dealt with the connections between literacy and ATM fraud (a detailed discussion can be accessed in Obiano, 2009), the use of techniques of neutralisation by banks in addressing customer complaints on fraud cases (Ihejiahi, 2009), as well as an analysis of observed patterns of robberies around bank structures, particularly ATM galleries (see Furst et al. 2000 and the references therein). Moreover, Tade and Adeniyi (2016) investigated ATM fraud in Lagos and Oyo States in southwest Nigeria using an exploratory qualitative research approach to uncover the identity of fraudsters and underscore the fraud strategies deployed. The authors showed that fraudsters were

predominantly kit and kin. Also, the main strategies for defrauding included card cloning, card swapping, and more direct offensives at ATM galleries. Tade and Adeniyi (2017a) attempted to track the effects of fraud victimisation on the life chances of victims in southwest Nigeria. The authors used data from in-depth interviews with fraud victims to show that victims suffered post-fraud trauma. It was also found that the banks' responses to their customers' victimisation were not favourable in compensating for their financial losses.

Based on the preceding discussions, it is obvious that the literature on Nigeria is still scant regarding understanding the empirical linkages between concerns about e-fraud and its implications for financial inclusion. Therefore, the present study fills this gap by focusing on the role of fraud risk in determining the extent to which financial inclusion is possible in the Nigerian financial system. The approaches to fraud risk governance are contemplated as an additional contribution to the evolving knowledge on the subject.

## METHODOLOGY

The study was conducted in Lagos and Oyo States. Our reasons for selecting these locations have been well articulated in our previous studies (Tade & Adeniyi, 2014, 2016, 2017a, 2017b). Using mixed qualitative methods (in-depth and key informant interviews) of data collection, participants (20 victims of fraud), four ATM custodians in banks, two bank executives, and governance institutions such as the Economic and Financial Crimes Commission (EFCC) were mainly purposively selected and in some instances reached through snowball methods. For the EFCC staff, we interviewed six agents involved in the commission's Bank Fraud Unit. The units in the EFCC are structured into different fraud cells, each focusing on certain cases.

Unlike other participants, enlisting the EFCC agents into the study involved a bureaucratic process and application to explain the purpose of the study and how the obtained data would be used. The approval was granted by the zonal head of the EFCC's Lagos office. Consequently, we proceeded to the commission's Bank Fraud Unit where agents awaited us, having received correspondence from their superior officer. They volunteered to share cases already decided at the courts with us. During this case review process, questions were asked by the researchers to understand the circumstances under which certain cases were reported and investigated and the challenges encountered in some of the cases. We had four sessions, each of which had at least three agents taking us through the cases, but to protect people's identities, case files were only handled by the agents who shared the facts of each of the cases with us. Since no digital recorders were allowed in this setting, we took field notes and read to the agents what was jotted down to ensure that important points were not omitted.

The interviews with victims and ATM custodians were done with a digital voice recorder and were subsequently transcribed and checked for accuracy. The emerging themes tailored along fear of fraud, adoption issues, and governance mechanisms were common among victims to institutional actors. These were then subjected to content analysis with excerpts reproduced verbatim to represent the views of our research participants. In what follows, we discuss the study's findings in line with our earlier stated research objectives.

## RESULTS AND DISCUSSION

### *Fear of Fraud and Adoption of Cashless Banking*

The spate of insecurity in Nigeria's cashless ecosystem is adversely impacting the migration of people from cash banking to the digital/branchless or cashless banking option. Even those who had already migrated to digital online banking were still cautious though optimistic that their monies could be secured from harm and the prying eyes of fraudsters. There was a general attitude of caution by some participants who were asked why they had stuck to the cash-based banking option. These participants decided not to migrate due to the perceived vulnerability of the cashless banking system, the insecurity in the payment options and the 'indirect' experiences they have had. It stands to reason that learning from the misfortune of others is one of the best forms of learning. Studying the processes leading to the victimisation of the reviewed victims' cases and their desire not to fall victim, our participants adopted avoidance behaviour by staying away from the branchless banking option. Therefore, a lack of trust that one's money and savings would be duly secured affected adoption. According to Tyler and Lind (1992), while trust is anchored on the expectation of receiving fair treatment when involved in a matter, it can affect future behaviour towards a distrusted organisation or system. Defrauded bank customers may withdraw their funds (close their account) in a fraud-prone bank and migrate to another bank with a better reputation for security with customers' funds. It follows that, as Wemmers and Manirabona (2014) explain, experiences of victimisation can produce a change in people's outlook of a system.

Concerning perceived vulnerability, participants expressed inadequate knowledge of how to behave under the new cashless policies. They seemed to have difficulty understanding the technicalities of the cashless banking option, which may predispose them to the antics of fraudsters benefitting from this. We found that the avoidance behaviour decision was not a function of education. Some senior academics, even with the rank of professor (of economics), stated their aversion to 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 banks, which allowed for face-to-face transactions. When the policy was implemented, the approach was somewhat autocratic – people were fined for cashier-paid withdrawals to force them to migrate to digital payment platforms. This was followed by limiting the amount that could be transacted in cash and the 'conscripted' of customers to either use the ATM or other online banking options. Many clients who did not yield to this banking policy reacted with a threat to close their accounts if the bank could not pay them in cash. 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. These people have committed their fraud by simply dialling the number of some account holders and hypnotising 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.*

The participant above would rather stick to the older way of doing things than expose himself to a payment system that he has no idea how it works. Going further on the spiritual

dimension of defrauding unveils the bank of knowledge this participant has been exposed to when it comes to contemporary dimensions or strategies of bank fraud. Furthermore, it thus seems that the awareness of other people's experiences of victimisation could influence one's adoption of safety behaviours such as this. We found this expressed by other participants who anchored their reason for not adopting the cashless option to the victimisation of their friends, boyfriends, or girlfriends. The diminished trust in the governance of the cashless policy accounted for the failure to migrate as stated by another participant: *I don't want to die by just receiving a 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 victimised are pulling out of their internet banking subscriptions. A student whose money disappeared without a transaction on her ATM card stated: *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 repeated fraud. It was more of a trust issue. I believe they (the bank) 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. As the narratives indicate, when people feel unsafe about technologically mediated transactions, they are more likely to adopt avoidance behaviours. This threatens the adoption and facilitates the opting out of electronic banking. This is consistent with the findings of Davinson and Sillence (2014) in their study of perceptions 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 using branchless banking options by bank customers in Nigeria have led to doubt or lack of trust or avoidance behaviour and, lately, 'cautious banking'. To understand what banking and allied governance institutions do to engender trust in the policy, we asked participants questions about mechanisms to check fraud. These governance mechanisms depend on the institution, the perceived loopholes in cashless banking, and the fraud dimensions. Tade and Adeniyi (forthcoming) have identified internal, external and collaborative frauds as the dimensions of fraud in Nigeria's cashless ecosystem. Therefore, the mechanism to govern fraud is related to the fraud dimension.

This makes more sense when related to our findings, which indicated that a weak governance structure is responsible for electronic fraud in Nigeria's cashless ecosystem. This weak governance is at the level of both banking institutions and regulating agencies such as the Central Bank of Nigeria. Data indicated there was poor supervision at the branch, regional and zonal levels of some banks where fraud is perpetrated. We found that inefficient supervision of

junior bank staff accounted for some banking frauds. A bank staff member 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' accounts. 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 a fraud neutralisation strategy was adopted to cover the tracks of inefficient supervision, which the operations officer and branch manager ought to have been queried about. This in-house fraud neutralisation approach retains compromised personnel 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 been embraced in the Nigerian banking system to the extent that most bank staff are not full-time staff but casualised. This management decision has exposed lowly paid and less-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 frauds committed in banks were perpetrated by contract/casual staff.<sup>1</sup> The Committee of Chief Compliance Officers of Banks in Nigeria (CCCOBIN), at their meeting of 29 October 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 penalising banks for such fraud occurrence"*. This indicates a reactive rather than proactive governance approach. According to a Punch (Monday, 9 November 2015) article entitled "Concerns over rising bank fraud", the magazine 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 the 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 appropriate checks, fraud may occur. The weak governance system, as stated by EFCC investigators, included inefficient supervision, non-performance of oversight by regional heads of banks, and 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 mechanisms that have limited the incidence of fraud. One of these mechanisms is sending information to customers who subscribe to electronic alerts. Through this, banks contact and send anti-fraud messages to their customers. Also, such messages are flashed on the Automated Teller Machines, informing customers to protect their Personal Identification Number (PIN). For instance, during the BVN policy fraud, a message was sent by a bank to its customers tagged "BVN SCAM ALERT". This was sent to the email addresses

---

<sup>1</sup> The current data of NDIC in 2016 indicated a higher percentage of bank staff were involvement in fraud.



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 login 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 emails 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 your account online or requesting your BVN details. Kindly note that BVN enrolment 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](mailto:complaints@gtbank.com) immediately you receive them.

These messages underscore the strategies used and help educate customers about security information. However, we found that not all customers subscribed to email alerts; many customers are illiterate or semi-illiterate. This raises the issue of proper customer characterisation and the need for complimentary financial literacy education.

Banks shy away from the public prosecution of erring staff due to reputational risk. Our research found that banks adopt shaming as a mechanism for instilling discipline while easing out ‘bad eggs’ by flagging their images on computers and across the banking industry. Such system networking will help prevent other banks that are otherwise oblivious of the deviant records of the prospective staff from offering such a person a job. This approach reduces litigation costs if the banks are to engage in legal prosecution. It also protects them from being exposed ‘as incapable of managing their customers’ funds’ and helps them to retain their customers. Through system shaming, fraudulent bank staff are eased out of the banking sector. The informal sanction of shaming has proven to work for mitigating reputational risk. Professional sanctions such as sacking and within-industry shaming are functional to the extent that they are activated to protect the depositing and investing public and the organisation’s image (see Levi, 2002).

## CONCLUSION

This study was motivated by two overarching research questions: Does the fear of fraud constitute an impediment to financial inclusion? How does the existence or otherwise of risk governance mechanisms mediate the nexus between electronic fraud and financial inclusion? In our attempt to answer these two questions, we establish from the literature the merits and

demerits associated with the financialisation of everyday life and how trying to ‘include’ (financial inclusion) in the formal financial ecosystem without taking cognisance of customers’ peculiar features, may trigger the unintended consequence of electronic fraud.

In trying to find answers to the first research question, we interviewed fraud victims and people who are yet to migrate to digital banking about the reasons underlying their actions. A spectrum of responses emerged. At the core of these responses was the fear of being victimised. In other words, account holders are more interested in the security of their money and avoid what can bring untoward experiences to them. They learnt to take the option of either staying away from fraud-prone banks or remaining analogue. More importantly, the negative post-fraud experiences of friends, associates and relatives which we have highlighted elsewhere (see Tade & Adeniyi, 2017a), served to inform others in taking precautions. As such, face-to-face cash transactions were preferred to digital, which some participants felt was more fraud-prone and shifted the burden of protection from banks to account owners. Thus, with a new form of banking emerges a new form of social relations and associated risks. Put differently, a new form of cashless banking has introduced new concerns in money relations and a re-evaluation of the contract between banks and their clients in risk governance for technology-influenced transactions. Therefore, fear of fraud impacts the adoption of new payment systems and, by extension, financial inclusion.

On how risk governance mediates electronic fraud and financial inclusion, we used data provided by governance institutions to help address this research agenda. While banks avoid litigation to mitigate reputational risk, they have deployed internal risk control measures such as ‘maker checker’, card hot listing, shaming of compromised staff, sacking of in-house fraud collaborator, and sending electronic fraud alerts to account holders. The ‘know your customer’ is poorly followed up, making it easy for people to give fake addresses. The findings further indicate that fraud cases mostly go unresolved thereby promoting 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. Financial and safety education may be needed to protect these categories of customers. The development of new financial services and payment systems must factor in security, peculiar demographics of customers/users, and the rights of the banking public to engender trust in the cashless ecosystem and drive the anticipated financial inclusion.

In particular, older citizens require deliberate and targeted support by the formal deposit taking and banking institutions if these senior citizens are to be properly inserted into the broader financial ecosystem in the country. To do this more effectively in the Nigerian context, the rural-urban dichotomy in the profiles and access of the elderly to financial services must be considered. In this way, efforts, policies, and actions would be better coordinated and contextually fit for the overriding purpose of expanding access to formal financial services for the vast majority of adult Nigerians.

Finally, and also crucial for designing mechanisms to stem the tide of cybercrimes, especially concerning the elderly, is the need for a robust understanding of how fraud and fraudulent practices are socially organised. Deeper scrutiny of recent and documented fraud perpetration strategies in Nigeria, such as fake job scams, abduction for fraud, collaborative

fraud, and biometric verification fraud is required. This approach may be important, especially with a better appreciation of the emerging roles of institutional insiders in organised cybercrime in Nigeria's cashless ecosystem. Adequately understanding fraud methods, criminal ingenuity, and dynamic sophistication can help identify the organisation of cybercriminality. Once done, the lessons gleaned can be used to improve the design of preventive mechanisms such as the tightening of internal control measures in banks and educating account holders on preventive strategies that can reduce victimisation in the cashless environment, which has come to increasingly characterise the Nigerian financial system.

Overall, while the present study deployed a purely qualitative, specifically interview-based, analytical approach, it is pertinent to note that alternative approaches such as quantitative analysis (using a questionnaire) and case studies may equally offer valuable insights on the core issues at the centre of this study. Further studies may therefore take on the potentially fascinating task of enlisting these options.

*About the author:*

*Oludayo Tade teaches crime, deviance and social problems at Nigeria's Premier University, University of Ibadan. A fellow of the Institute for Money, Technology and Financial Inclusion (IMTFI) at the University of California, Irvine, USA, Tade's scholarly publications on Bokoharam terrorism, cybercrime/fraud, victims of crime, film piracy, child trafficking, transactional sex/prostitution, and rape have appeared in such journals as International Journal of Sociology and Social Policy (IJSSP), International Review of Victimology (IRV), Journal of Financial Crime (JFC), International Journal of Offender Therapy and Comparative Criminology (IJOTCC), Journal of Asian and African Studies (JAAS), Canadian Journal of African Studies (CJAS) and Journal of Aggression, Maltreatment and Trauma (JAMT). Tade is on the Editorial Board of International Journal of Offender Therapy and Comparative Criminology (IJOTCC) Sage as Associate Editor and African criminology section editor. He can be reached at dotad2003@yahoo.com.*

*About the author:*

*Oluwatosin Adeniyi is Senior Lecturer at the Department of Economics, University of Ibadan, Nigeria. His research area of interest includes macroeconomics, development economics, tourism economics, energy economics, and public economics. His publications have appeared in reputable peer reviewed journals. He is also a Research Fellow of the Institute for Money, Technology and Financial Inclusion (IMTFI), University of California, Irvine, USA. He has extensive experience as a reviewer for several journals in Economics and other social science fields. He can be reached at saino78@yahoo.com.*

## REFERENCES

- Beck, T., Senbet, L., & Simbanegavi, W. (2015). Financial Innovation and Innovation in Africa: An Overview. *Journal of African Economies*, 24(AERC Supplement1), i3–i11.
- Cross, C. (2017). 'But I've never sent them any personal details apart from my driver's licence number...': Exploring seniors' attitudes towards identity crime. *Security Journal*, 30(1), 74–88.
- 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 of Human-Computer Studies*, 72(2), 154-168.
- FII Tracker Survey. (2017). Available at [http://finclusion.org/uploads/file/reports/Nigeria%20Wave%204%20Report\\_23-Jun-2017.pdf](http://finclusion.org/uploads/file/reports/Nigeria%20Wave%204%20Report_23-Jun-2017.pdf)
- Furst, K., Lang, W., & Nolle, E. D. (2000). Internet Banking Development and Prospects. Office of the Comptroller of the Currency Economic and Policy Analysis Working Paper no. 2000-9. Boston: Harvard University.
- Ihejiahi, R. (2009). How to fight ATM fraud online. *Nigeria Daily News*, June 21, p. 18.
- Johnson, S. (2016). Competing Visions of Financial Inclusion in Kenya: The Rift Revealed by Mobile Money Transfer. *Canadian Journal of Development Studies*, 37(1), 83–100.
- Johnson, S., & Williams, R. (2016). The Political Economy of Financial Inclusion: Tailoring Donor Policy to Fit. *Development Policy Review*, 34(5), 721–743.
- Levi, M. (2002). Suite Justice or Sweet Charity? Some Explorations on Shaming and Incapacitating Business Fraudsters. *Punishment and Society*, 4(2), 147-163.
- Mader, P. (2016). Card Crusaders, Cash Infidels and the Holy Grails of Digital Financial Inclusion. *BEHEMOTH: A Journal of Civilisation*, 9(2), 60–81.
- Mader, P. (2017). Contesting Financial Inclusion. *Development and Change*. <https://doi.org/10.1111/dech.12368>
- NEFF. (2016). A Changing Payment System: The Security Challenge. Annual Report. <https://www.cbn.gov.ng/Out/2017/CCD/A%20CHANGING%20PAYMENTS%20ECOSYSTEM%20NEFF%202016%20Annual%20Report.pdf> (accessed 6 March 2018).
- Nigeria Deposit Insurance Corporation. (2013). Annual report and statement of accounts. Available at: <http://ndic.gov.ng/wp-content/uploads/2015/01/NDIC%20Report%202013.html> (accessed 26 February 2017).
- Nigeria Deposit Insurance Corporation. (2014). Annual report and statement of accounts. Available at: <http://ndic.gov.ng/wp-content/uploads/2015/07/NDIC%20Report%202014.html> (accessed 26 February 2017).
- Obiano, W. (2009). How to fight ATM fraud. *Nigeria Daily News*, 21 June, p. 18.

Pike, A., & Pollard, J. (2010). Economic Geographies of Financialization. *Economic Geography*, 86(1), 29–51.

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](http://www.imtfi.uci.edu/files/docs/2014/tade_and_adeniyi_final_2014_1.pdf).

Tade, O., & Adeniyi, O. (2016). On the Limits of Trust: Characterising automated teller machine fraudsters in Southwest Nigeria. *Journal of Financial Crime*, 23(4).

Tade, O., & Adeniyi, O. (2017a). 'They withdrew all I was worth': Automated teller machine Fraud and Victims' Life Chances in Nigeria. *International Review of Victimology*.

<https://doi.org/10.1177/0269758017704330>.

Tade, O., & Adeniyi, O. (2017b). Automated teller machine fraud in south-west Nigeria: Victim typologies, victimisation strategies and fraud prevention. *Journal of Payment Strategy and Systems*, 11(1), 86–92.

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

Tyler, T.R. & Lind, E.A. (1992). A Relational Model of Authority in Groups. *Advances in Experimental Social Psychology*, 25, 115-191.

Walsh, K. P. (2018). Transforming Usury into Finance: Financialization and the Ethic of Debt. *Finance and Society*, 4(1), 41–59.

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.