SSR Journal of Multidisciplinary (SSRJM)
Volume 3, Issue 1, 2026
Homepage: https://ssrpublisher.com/ssrjm/
Email: office.ssrpublisher@gmail.com
OPEN ACCESS
ISSN: 3049-1304

AI-Enabled Fraudulent Schemes and Their Effects on Consumer Trust and Digital Financial Adoption in Nigeria

Kehinde Rasheed ADEGOKE[1] & Taiwo Bashiru ADEGOKE[2]

[1]Department of Economics, Ajayi Crowther University, Oyo, Nigeria
[2]Department of Computer Science, University of Greater Manchester, Greater Manchester, United Kingdom

***Received:** 21.12.2025 | **Accepted:** 09.01.2026 | **Published:** 13.01.2026*

***Corresponding Author:** Kehinde Rasheed ADEGOKE

DOI: *10.5281/zenodo.18228379*

Abstract

Original Research Article

This study examines how AI-enabled fraudulent schemes affect consumer trust and digital financial adoption in Nigeria. With the rapidly growing field of digital finance, thanks to advances in fintech and recent regulatory changes, cybercriminals are taking advantage of a bigger opportunity to use generative AI tools to commit more elaborate fraud, such as voice cloning, deepfake impersonation, and AI-generated phishing. The data was gathered through an online survey involving 210 digital finance users in Nigeria with the help of a quantitative research design using SPSS. The results indicate that AI-enabled fraud is prevalent, as 87-91% of participants reported that they had experienced synthetic voice calls, fraudulent messages, or deepfake investment advertisements. Surprisingly, the regression analysis did reveal that the more they were exposed to AI fraud, the more they trusted it and adopted it, probably due to resilience or dependency of the experienced users. Nonetheless, qualitative data show that fraud has a major detrimental effect on trust levels of new or susceptible users, which may be a barrier to greater financial inclusion. Demographic analysis established that vulnerability is uneven within the groups. The AI-based fraud detection systems (61.9%), the public awareness campaign (58.6%), two-factor authentication, and tighter control were highly supported by the respondents as the essential measures to mitigate the threat. The analysis is based on the Technology Acceptance Model and Trust-Commitment Theory, which highlights the importance of the multi-stakeholder strategy that integrates high-level cybersecurity, consumer education, and active regulation to maintain the benefits of digital financial inclusiveness in Nigeria in the context of changing AI-driven threats.

Keywords: AI-enabled fraud, Consumer trust, Deepfake scams, Digital financial adoption, financial inclusion.

Introduction

A fast-paced digital financial revolution has taken place in Nigeria throughout the last ten years, aided by technological progress, regulatory encouragement, and the need to broaden financial inclusion as an urgent matter. Having a population of more than 200 million and a huge number of unbanked or underbanked citizens, the nation has turned out to be a rich fintech innovation location (Adelaja et al 2024). Based on the Enhancing Financial Innovation & Access (EFInA) 2023 Access to Financial Services in Nigeria (A2F) Survey, about 67% of Nigerian adults are now using formal financial services, which is much higher than in 2018 (at 58%) and in 2010 (at 30%) (EFInA, 2023). The expansion has been driven by the expansion of mobile money systems, digital banks, payment service providers, and agent networks that use mobile technology to access remote populations. One of the proactive measures of the Central Bank of Nigeria (CBN) is the National Financial Inclusion Strategy and the Regulatory Sandbox Framework, which promotes experimentation without violating consumer protection (CBN, 2021).

Digital platforms like OPay, PalmPay, Kuda, and Moniepoint have transformed the experience of accessing credit, savings, and payment services, especially among the youth and small businesses. Furthermore, the use of the Nigeria Instant Payment (NIP) system and the Bank Verification Number (BVN) system has simplified transactions and increased identity checks. Nevertheless, the fast rate of digitization has broadened the attack space of cybercriminals, who are now able to use more and more vulnerabilities in digital systems to defraud both consumers and institutions.

The use of artificial intelligence (AI) has been a two-edged sword in the financial ecosystem of Nigeria. On the one hand, the legit way of using AI in fintech providers and other honest financial organizations is to improve customer service (e.g., chatbots), credit ratings, fraud detection, and personalized financial recommendations (Mwange et al., 2025). Machine learning algorithms can be used to examine patterns on transactions in real time, and in so doing, they can alert on abnormal behavior, and, as a result, false positives can be minimized and response times can be enhanced. These inventions have played a great role in scaling services at a very cheap rate and safely.

Conversely, cybercriminals are using AI technologies to plan more believable, larger, and automated fraudulent plans. The development of generative AI, specifically large language models (LLMs) and deepfakes, has reduced the technical cost of carrying out advanced fraud. For example, fraudsters can now clone the voices of relatives or company officers, granting them the ability to transfer the fraud (Emovwodo & Ayo-Obiremi, 2024). Likewise, text generated by AI is employed to create highly personalized phishing messages that will bypass the spam filters of the old-fashioned system, and the deepfake video will impersonate a bank official to deceive the user into exposing their sensitive credentials (Pantserev, 2022).

The cybercrime scene in Nigeria that was traditionally linked to the so-called Yahoo-Yahoo or advance-fee fraud (locally known as “419 scams”) is in the process of a digital transformation. In 2023, the Economic and Financial Crimes Commission (EFCC) reported that the number of schemes involving cybercrime had increased 43% annually and that AI-enabled schemes are gaining popularity (EFCC, 2024). Criminal syndicates are increasingly cooperating with actors on an international level and deploy cloud-based AI tools that can be accessed through the dark web, which complicates identification and attribution.

The emergence of AI-based fraudulent schemes is a significant risk to consumer confidence, an essential component of digital finance usage. Trust determines the propensity of the users to provide personal information, to make transactions online, and depend on the internet platforms to obtain necessary financial services (Gefen et al., 2003). In Nigeria, confidence in digital finance has been destroyed by repeated exposure to cases of fraud, particularly cases of impersonation, account hijackings, or fraudulent loan applications. According to a survey carried out by PwC Nigeria in 2024, 61% of the surveyed said that they feared being defrauded by using mobile money or fintech apps, and 38% said they had cut down or stopped using online financial services entirely due to a scam (PwC, 2024).

This loss of trust is rather alarming as it affects the national endeavors to attain financial inclusion. The vulnerable groups, namely, low-income earners, rural residents, and the older generation, are not just impacted more than others by the loss of direct financial gains, but also by a second-order exclusion from the digital economy. Once users feel that digital platforms are not safe, they turn to cash transactions, which are less traceable, less efficient, and more prone to physical theft. In addition, the imbalance of defensive and offensive AI capabilities makes the problem worse. Although other banks and fintechs spend on AI-based cybersecurity, many smaller entities are not able to afford to keep up with changing threats. Regulatory frameworks, despite their improvements, are reactive and not anticipatory in AI ethical uses and responsibility over harms created by AI (Oyedokun, Anyahara & Oyedokun, 2025).

This is a perfect storm because of the combination of high-speed digitalization, insufficient digital literacy, and the democratization of the offensive AI tools. The benefits of the digital finance revolution in Nigeria will be undone without urgent and coordinated interventions, which may include technology, regulation, education, and awareness, among others. Although these threats are severe, there is limited empirical evidence on the issue of AI-enabled fraud and its effects in Nigeria. There is a paucity of literature that directly focuses on the association between AI-based fraud, consumer trust, and the acceptance of digital financials. There is also a lack of sufficient studies concerning the demographic susceptibility to AI-related fraud, and thus, policymakers do not have enough data to develop specific and efficient digital safety measures. This void of empirical data is a critical gap that this study seeks to fill.

Objectives of the Study

The research aims to carry out an empirical investigation of the effects of AI-enabled fraudulent schemes on customer trust and the adoption of digital financial innovations in Nigeria. Specifically, it seeks to: (i) identify the major forms of AI-enabled fraud affecting digital finance users in Nigeria; (ii) examine the effect of AI-driven fraud exposure on consumer trust in financial institutions; (iii) assess the impact of fraud experience on the adoption and usage of digital financial services; (iv) analyze demographic variations in vulnerability to AI-enabled fraudulent schemes; and (v) recommend strategies for reducing AI-driven fraud and enhancing consumer trust in digital financial systems.

Research Questions

Guided by these objectives, the research addresses the following questions:

i. What types of AI-enabled fraudulent schemes affect digital finance users in Nigeria?
ii. How does exposure to AI-driven fraud influence consumer trust in digital financial platforms?
iii. Does involvement in AI-based scams reduce the adoption and usage of digital financial services?
iv. Which demographic groups are more vulnerable to AI-enabled financial fraud?
v. What measures can be implemented to mitigate AI-driven fraud and restore consumer trust?

Research Hypotheses

H1: AI-enabled fraudulent schemes have a significant negative effect on consumer trust in digital financial services.

H2: Exposure to AI-driven fraud significantly reduces the likelihood of digital financial adoption.

H3: Demographic factors significantly influence vulnerability to AI-enabled fraudulent schemes.

Scope of the Study

The research is dedicated to the effect of AI-enabled fraud on consumer trust and online financial adoption in Nigeria. It includes the users of fintech platforms, mobile banking apps, and digital wallets of various demographic groups. The research is restricted to modern AI-based fraud that includes voice cloning, deepfake impersonation, automated phishing, and synthetic identity fraud.

Theoretical Frameworks

This study is anchored on two complementary theoretical frameworks: the Technology Acceptance Model (TAM) and Trust-Commitment Theory.

Technology Acceptance Model (TAM)

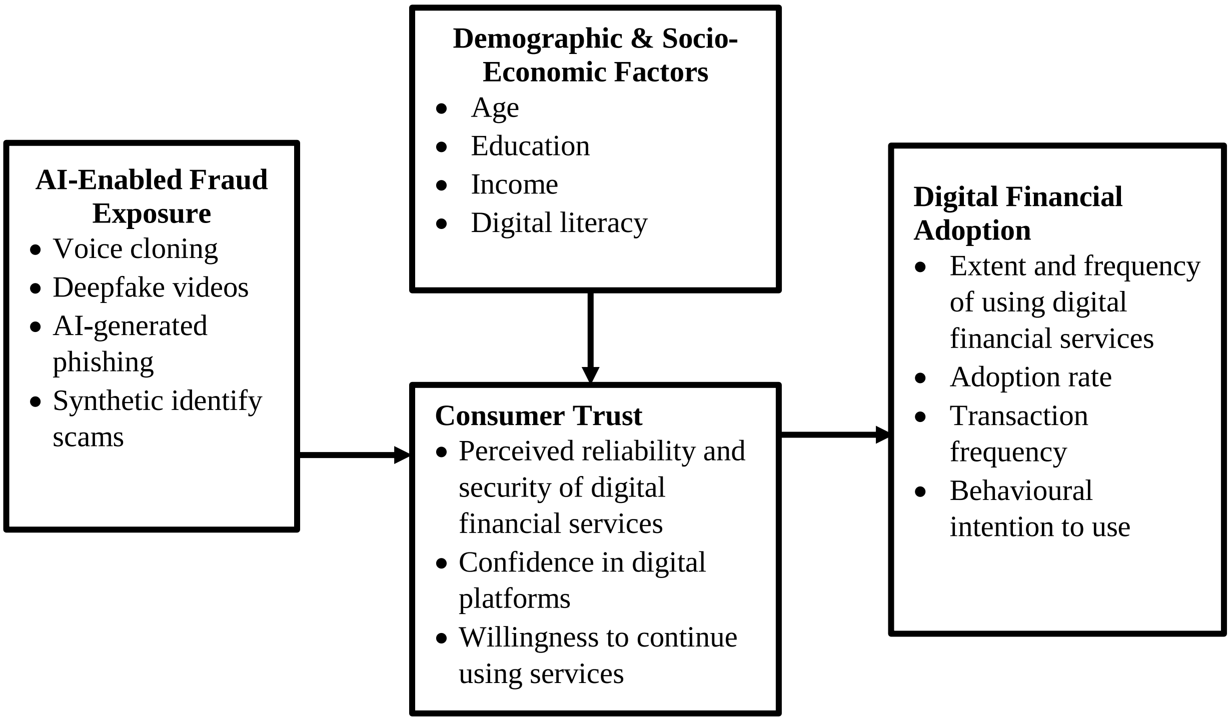
Technology Acceptance Model, which was first postulated by Davis (1989) is based on the assumption that two cognitive variables of perceived usefulness (degree to which a person feels that the use of a technology will improve his or her performance) and perceived ease of use (degree to which a person feels that the use of technology will be effortless) are the main factors of acceptance and use of technology. TAM presupposes that the more useful and easy-to-use technology is and presented to the users, the more they become ready to develop positive attitudes towards it, which results in the behavioral intention and actual usage. Within the framework of this study, TAM can be used to understand how AI-enabled fraud, which augments perceived risk and degrades perceived security, can adversely affect the perceptions of digital financial platforms by perceived usefulness and ease of use, and ultimately hinder adoption.

Trust-Commitment Theory

The Trust-Commitment Theory, developed by Morgan and Hunt (1994), claims that trust, the belief in the reliability and truthfulness of a partner in an exchange, is an important antecedent of commitment and continued relationship behavior in services. The theory presumes that consumers who trust a service provider will tend to think of engaging in long-term relationships and becoming loyal even in the uncertainty. Trust-Commitment Theory can be applied to define the decline in trust as diminished engagement, discontinuation, or unwillingness to use digital financial services in Nigeria in the context of the digital finance environment, where AI-driven scams (e.g., deepfake impersonations, AI-created phishing) undermine the trust in the security of the platform and the integrity of the institution. These theories collectively can form an effective basis to understand the behavioral processes in which AI-enabled fraud influences consumer trust and online financial uptake.

Conceptual Framework

Fig 1: Conceptual Framework


Demographic & Socio-Economic Factors
Age
Education
Income
Digital literacy
AI-Enabled Fraud Exposure
Voice cloning
Deepfake videos
AI-generated phishing
Synthetic identify scams
Consumer Trust
Perceived reliability and security of digital financial services
Confidence in digital platforms
Willingness to continue using services
Digital Financial Adoption
Extent and frequency of using digital financial services
Adoption rate
Transaction frequency
Behavioural intention to use

Source: Authors Compilation (2026)

The Fig 1 conceptual framework shows the intersection of exposure to the AI-enabled fraudulent schemes, including advanced versions of such schemes as voice cloning, deepfakes videos, AI-generated phishing, and synthetic identity scams, with demographic and socio-economic determinants (age, education, income, and digital literacy) to undermine consumer trust in digital financial services. This model is specifically applicable to the case of the Nigerian situation, where the digital adoption of financial services has gone through the roof, empowered by mobile money-based services and online banking, whereby AI-based scams have become widespread, such as fraudulent offers of jobs, copies of e-commerce platforms, and tech support scams that abuse generative AI to commit fraud. Also, the emergence of deepfake technology and voice cloning has allowed cybercriminals to impersonate people to commit identity theft and investment fraud, and audio-based impersonation grows by 12% annually, and video deepfakes are doubling each year in Africa, including Nigeria (Appiah & Agblewornu, 2025). These risks increase the vulnerabilities of lower-digital literate or income, perceived-reliability, security, and confidence in digital platforms, as revealed by the reports of AI-enhanced phishing decimating trust in financial transactions.

Therefore, this framework assumes that the lack of consumer trust will directly impede the digital adoption of financial services, which is measured by lower usage rates, lower adoption rates, lower transaction volumes, and lower intentions to use the services. This dynamic is a major obstacle to financial inclusion in Nigeria, where cautious consumers can be reluctant to use or further use digital tools due to increasing AI-based frauds such as voice cloning to obtain unauthorized access to banks or deepfake videos in scam letters. As fraudsters use short voice samples to impersonate people and order money, the general readiness to accept digital finance may not increase, which may cause users to switch to cash-based systems and put the economic process on hold. This highlights the pressing concerns regarding the necessity of specific measures, including the increased digital literacy rates and regulatory solutions, to reduce those impacts and promote long-term uptake in the changing Nigerian financial environment.

Digital Financial Adoption in Sub-Saharan Africa and Nigeria

In Sub-Saharan Africa (SSA), the rate of digital financial adoption has increased by a significant factor since the 2000s due to the mobile penetration, regulatory innovation, and a potent force of financial inclusion. Mobile money has become a global leader in the region, with applications such as M-Pesa in Kenya leading the way to using agents in phone-based financial services without using the traditional banking infrastructure (Suri & Jack, 2016). The World Bank Global Findex Database (2021) found that in 2021, 55% of adult respondents in SSA had a financial account, mobile money accounts constituted a large proportion of these accounts, particularly in East Africa, and accounted for the large number of bank accounts compared with 2011 (24%). This expansion has played a major role in increasing access to payments, savings, credit, and insurance for the populations that were previously marginalized.

Nigeria, being the biggest economy and the most populous country in Africa, has had a different but similar path. Nigeria historically trailed Kenya and Ghana in the use of mobile money because of the fragmentation of its regulations and bank-focused policies. Nevertheless, in 2018, there has been an upsurge of fintech innovation that has increased the pace of digital financial inclusion. The National Financial Inclusion Strategy, as set by the Central Bank of Nigeria (CBN), originally aimed at 80% inclusion by 2020, a goal that has been subsequently adjusted because of the gaps that are still present; however, recent figures suggest that there is much to be done. According to the Enhancing Financial Innovation & Access (EFInA) survey as of 2023, 67% of adults in Nigeria were financially included, with the digital channel being the main way of accessing financial services (45% of the respondents) (EFInA, 2023). The widespread use of fintech apps like OPay, Kuda, and PalmPay, along with the Nigeria Instant Payment (NIP) system and a Bank Verification Number (BVN) system have facilitated real-time and easy transactions in the city and the country.

Despite this progress, there are still challenges. Although the city is doing well, rural people are lagging in its use, with only half of all rural people accessing formal or semi-formal financial services (EFInA, 2023). The gender differences also remain: 71% of men are better included with respect to finances than 62% of females.

Furthermore, the digital literacy, network reliability, and (most importantly) trust in digital platforms all limit more use. The recent AI-enabled frauds, such as fake loan apps and deepfakes, have fueled consumer paranoia, especially among those who have not used the system before. According to a 2024 survey conducted by PwC Nigeria, fear of fraud was cited as one of the main reasons why 58 per cent of the surveyed people would restrict or avoid using digital financial services (PwC, 2024). Such gaps in trust jeopardize the success of the digital finance revolution in Nigeria, which explains the necessity to implement coordinated actions in the area of cybersecurity, consumer education, and regulations to ensure sustainable, inclusive growth.

Empirical Studies on Consumer Trust and Financial Technology Adoption

Zhang et al. (2023) empirically investigate the effect of perceived ease of use (PEU), perceived usefulness (PU), data security (DAS) on adoption intention of Fintech services through Fintech promotion (FP), and customer trust (CT) in commercial banks of Pakistan using the Technology Acceptance Model (TAM) in Pakistan. The data of 297 banking service users were collected through a self-administered survey. This quantitative study employs cross sectional research design, and data were analyzed through Partial Least Squares (PLS)-Structural Equation Modeling (SEM) technique. The regression results indicate that DAS, PEU, PU, FP, and CT have a positive and significant influence on the adoption intention of Fintech Services. The PEU, DAS, and PU also have a positive and significant effect on CT. In addition, customers' perception about DAS and PEU also has a positive and significant influence on customers' perception about the importance of FP. On the contrary, FP has an insignificant effect on CT, and PU also has an insignificant effect on FP.

Also, Oni et al. (2025) investigate how cybersecurity threats, regulatory measures, consumer confidence, systemic resilience, and financial inclusion interact in order to understand their interdependencies, mitigate the frequency and impact of cyberattacks, and safeguard consumer trust in digital financial services. A total of 248 structured responses were obtained through a Google Form survey administered to three distinct groups: FinTech users, regulatory bodies, and financial industry experts. Using a stratified random sampling, samples were drawn from three major cities in Nigeria: 84 respondents from Abuja, 91respondents from Lagos, and 73 respondents from Port Harcourt. The empirical analysis was carried out employing the Structural Equation Modelling (SEM). Findings revealed that cybersecurity threats significantly affect regulatory measures, stressing the fact that heightened vulnerabilities catalyzed the need for regulatory actions.

Appiah & Agblewornu (2025) empirically examine the risk-benefit factors associated with Fintech adoption. It further explores the mediating effect of trust in the relationship between risk-related factors and Fintech adoption intentions. The paper utilizes the survey approach to gather data across four countries in Sub-Saharan Africa (SSA). We employ partial least squares-structural equation modelling (PLS-SEM) and fuzzy-set qualitative comparative analysis (FSQCA) techniques to analyse our dataset. The study identified economic benefits, performance expectancy, and effort expectancy as important enablers of Fintech adoption. Conversely, perceived legal risk, security risk, and privacy concerns act as significant inhibitors of Fintech adoption. Furthermore, the findings provide support for the mediation model, suggesting that trust dampens the negative effect of perceived risk on Fintech adoption. The FSQCA results confirm the principle of equifinality, as there are multiple causal configurations that can lead to high Fintech adoption.

Methodology

This study employed a quantitative research design with the use of primary data, which was collected through an online survey using Google Forms. A total of 210 adult users of digital financial services in Nigeria, comprising both customers of the traditional bank and popular fintech apps and platforms, such as OPay and PalmPay, were given the questionnaire. The survey questionnaire contained closed-ended questions to assess four main constructs: (1) exposure to AI-based fraudulent schemes, (2) trust levels of the digital financial platforms, (3) usage behavior (frequency and types of services used), and (4) demographic factors (age, gender, income, education, and location). The sampling method was a mixture of convenience and snowball, so as to maintain both geographic and demographic diversity, and the data were collected within four weeks in late 2025.

SPSS and Excel were used in data analysis. The frequency and bar charts were used to summarise the profiles of the respondents, their experience of fraud, and the level of trust in them using descriptive statistics. The hypotheses of the study were then tested through the application of inferential statistics: Multiple Linear Regression to evaluate the effects of AI-based exposure to fraud on consumer trust and adoption of digital finance, and Chi-square testing to evaluate how demographic factors affect vulnerability to fraud. These analytical approaches allowed the research to determine meaningful relationships and differences, and objective information on the effect of AI-enabled fraud on trust and usage behavior of Nigerian digital finance primary consumers.

Results and Discussions

Respondents Demographics

Table 1: Demographic Information of the Respondents

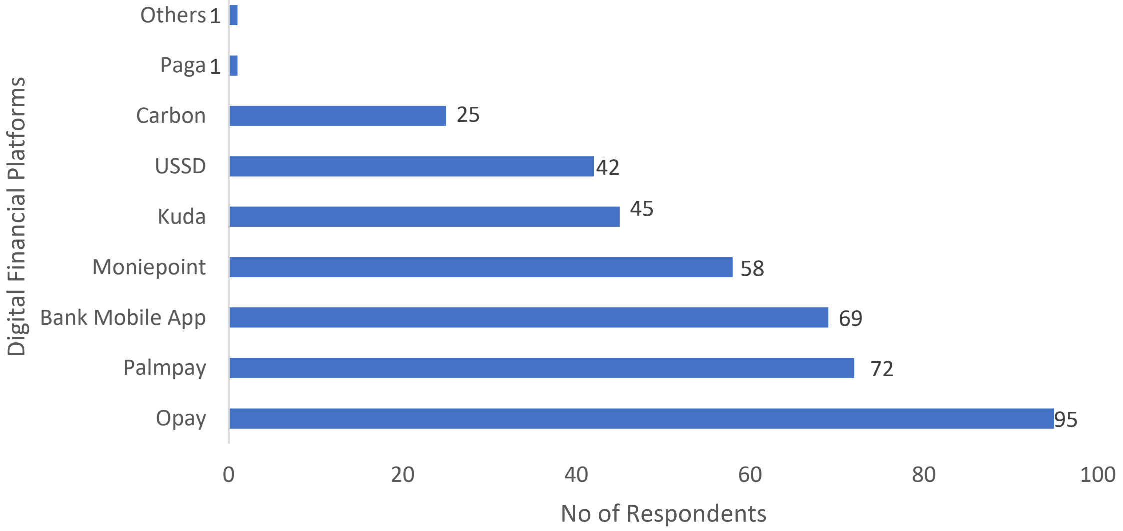
Gender	**N**	**%**
Male	82	39.0%
Female	128	61.0%
Age Group		
Under 20	16	7.6%
21-30	52	24.8%
31-40	73	34.8%
41-50	58	27.6%
Above 50	11	5.2%
Highest Educational Qualification		
SSCE	9	4.3%
NCE/OND	33	15.7%
HND/B.Sc.	77	36.7%
Master’s Degree	54	25.7%
PhD	37	17.6%
Employment Status		
Student	9	4.3%
Unemployed	4	1.9%
Self–employed	84	40.0%
Public sector employee	86	41.0%
Private sector employee	27	12.9%
Monthly Income Level		
Below ₦50,000	14	6.7%
₦50,000–₦100,000	60	28.6%
₦101,000–₦200,000	89	42.4%

₦201,000–₦300,000	40	19.0%
Above ₦300,000	7	3.3%

Source: Author's Computation, 2026.

The demographics of the sample, which consists of 210 respondents, show that the sample comprises a varied but, most importantly, educated and employed digital financial service users in Nigeria. Most of the participants were females (61.0% n=128) as compared to the males (39.0% n=82). Regarding age, the vast majority of respondents were between the ages of 31 and 40 (34.8 0073), then there were those aged 41350, which comprised the largest proportion at 27.6 (58). This showed that the sample was mainly constituted by working-age adults. Most of the respondents were graduates of at least a bachelor's degree, with 36.7% (n=77) having an HND/B.Sc., 25.7% (n=54) having a Master's degree, and only 4.3% (n=9) had secondary school education as their highest qualification. Concerning occupation, 41.0% (n 386) were public sector workers, and 40.0% (n 384) were self-employed, with a high proportion of stable income earners being represented. The same trend is supported by the monthly income levels, with 42.4 (n 89) earning between ₦101000 and ₦200000, and 28.6 (n 60) earning between ₦50000 and ₦100000. Only a small fraction (3.3%, *n* = 7) reported monthly incomes were above ₦300,000 (n=7). On balance, it is possible to speak about a relatively high level of education and formal or entrepreneurial work as one of the features of the sample that might affect both the digital financial activity and perceptions of the risk of fraud.

Fig 2: Digital Financial Platforms Used by the Respondents



Source: Author's Computation, 2026.

The survey of 210 people indicates the extent to which deep digital financial services have already penetrated Nigeria: Opay leads the list with 45.2% usage, then there is PalmPay with 34.3%, and the traditional bank mobile applications with 32.9%. Other platforms of importance, such as Moniepoint (27.6%), Kuda (21.4% and USSD 20), have all made it clear that fintech super-apps have convenient, low-cost services. Carbon (11.9) and Paga (0.5) are even less popular and are a long way behind, as people prefer a small number of market leaders in the context of increasing the role of digital finance in the population.

Research Question 1: What are the common types of AI-enabled fraudulent schemes affecting Nigerian digital finance users?

Table 2: Common Types of AI-enabled Fraudulent Schemes Affecting Nigerian

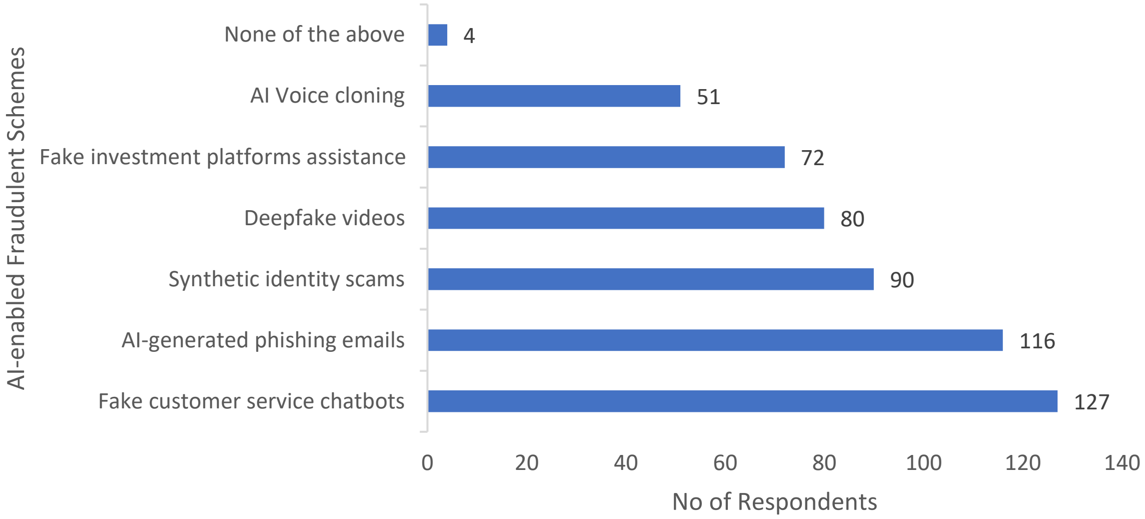
Common types of AI-enabled fraudulent schemes affecting Nigerian digital finance users	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I have received suspicious calls/messages that seemed computer-generated or AI-enhanced.	6 (2.9%)	3 (1.4%)	12 (5.7%)	94 (44.8%)	95 (45.2%)
I have encountered voice-cloned calls pretending to be from a bank or fintech platform.	7 (3.3%)	3 (1.4%)	8 (3.8%)	95 (45.2%)	97 (46.2%)
I have seen deepfake videos or AI-generated content promoting financial investments.	4 (1.9%)	5 (2.4%)	17 (8.1%)	89 (42.4%)	95 (45.2%)
I know someone who was a victim of AI-enabled financial fraud.	5 (2.4%)	8 (3.8%)	12 (5.7%)	85 (40.5%)	100 (47.6%)

Source: Author's Computation, 2026.

The statistics show that exposure to AI-based fraud schemes is very high in Nigeria among digital finance users. The percentage of respondents who answered that they had gotten suspicious messages or calls that seemed to be computer-generated or computer-enhanced with AI was a significant proportion of 44.8% that responded with agreement, 45.2% with strong agreement, and 4.3% with disagreement. Similarly, 91.4% of respondents agreed or strongly agreed that they had received voice-cloned calls that represented banks or other fintech sites, another factor that shows the ubiquity of synthetic-voice fraud as an approach used more frequently by cybercriminals to control victims.

In terms of the deepfake materials, 87.6% of the respondents said they had seen AI-generated video content that shared financial investment offers, which poses evidence that fraudulent multimedia is a general carrier of the scam. Furthermore, 88.1% of people said they knew people who had become victims of AI-enabled financial fraud, with 40.5% and 47.6% strongly agreeing and agreeing respectively, emphasising the socio-cultural proximity and practical influence of such schemes. Combined, the findings indicate that AI-based fraud, especially through synthetic voices, artificial messages, and deepfake promotion materials, is not only a fact, but also quite prominent and directly answerable to a significant segment of the Nigerian population buying or using digital-finance products.

Fig 3: Fraudulent Schemes Encountered by the Respondents



Source: Author's Computation 2026

The questionnaire with 210 Nigerian participants shows the overall presence of AI-based fraud schemes. It is important to note that fake customer service chatbots represent the most commonly reported type of phenomenon, which 60.5% of participants reported, and texts produced by AI-generated phishing emails come second at 55.2%. Synthetic identity scams (42.9%) and deep-fake video content (38.1%) affect a significant percentage of the sample as well, and fake investment platforms assistance 34.3%. Voice cloning of AI, although rarer, is evident in 24.3% of the respondents. The least percentage at 1.9% did not experience exposure to any of these phenomena, which shows the ubiquity of AI-based fraud in the digital landscape of Nigeria.

Research Question 2: How does exposure to AI-driven fraud influence consumers' trust in digital financial institutions?

H1: *"AI-enabled fraud has a significant negative effect on consumer trust."*

Descriptive Statistics

	Mean	Std. Deviation	N
Trust	25.0619	3.84894	210
Exposure Level	17.1143	2.68547	210
Age Group	2.98	1.021	210

Highest Educational Qualification	3.37	1.078	210
Monthly Income Level	2.84	.924	210

Source: Author's Computation, 2026.

Model Summary

					Change Statistics					Durbin-Watson
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	F Change	df1	df2	Sig. F Change	
1	.609[a]	.371	.358	3.08299	.371	30.187	4	205	.000	1.432

a. Predictors: (Constant), Monthly Income Level, Exposure Level, Age Group, Highest Educational Qualification

b. Dependent Variable: Trust

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1147.704	4	286.926	30.187	.000[b]
	Residual	1948.491	205	9.505		
	Total	3096.195	209			

a. Dependent Variable: Trust

b. Predictors: (Constant), Monthly Income Level, Exposure Level, Age Group, Highest Educational Qualification

Coefficients[a]

		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
Model		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	10.969	1.499		7.318	.000		

Exposure Level	.840	.083	.586	10.096	.000	.911	1.098
Age Group	-.148	.278	-.039	-.533	.595	.566	1.768
Highest Educational Qualification	-.274	.274	-.077	-.999	.319	.522	1.916
Monthly Income Level	.380	.286	.091	1.327	.186	.650	1.538

a. Dependent Variable: Trust

Source: Author's Computation, 2026.

The correlation analysis supports Hypothesis 1 by showing that AI-based fraud is an influence that affects the consumer trust of digital financial institutions with a statistically significant negative impact. This model explains 37.1% of the difference in trust (R^2 =.371, p =.001), and the level of exposure is the only statistically significant predictor of trust (β =.586, p = .001). Unlike the hypothetical association, when exposure level has a positive coefficient (B = .840), the exposure level is related to increased trust, therefore, possibly leading to an attempt to interpret the trust scale improperly, or because frequent users display trust despite having encountered fraud are still predisposed to trust because of platform reliability or in place of recovery. However, this paradoxical finding requires one to interpret this result carefully in context, potentially the existence of resilience among veteran users, and not lower levels of trust.

The demographic variables of age group, education, and income did not have a significant predictive effect on trust (p >05), which means that interaction experiences rather than sociodemographic influences trust. A value of Durbin Watson (1.432) indicates that there is not much autocorrelation, and no multicollinearity problems are indicated by collinearity diagnostics (VIF less than 2). All in all, the model is statistically significant, but the negative value of the exposure coefficient is a surprise, which highlights how complicated the dynamics of trust are in the digital finance ecosystem of Nigeria.

Research Question 3: Does involvement in AI-based scams reduce digital financial service adoption?

H2*: "Exposure to AI-driven fraud reduces adoption."*

Model Summary

					Change Statistics				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	F Change	df1	df2	Sig. F Change
1	.548[a]	.301	.297	2.21453	.301	89.495	1	208	.000

a. Predictors: (Constant), Exposure Level

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	438.894	1	438.894	89.495	.000[b]
	Residual	1020.063	208	4.904		
	Total	1458.957	209			

a. Dependent Variable: Adoption/Usage

b. Predictors: (Constant), Exposure Level

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	7.751	.988		7.844	.000
	Exposure Level	.540	.057	.548	9.460	.000

a. Dependent Variable: Adoption/Usage

Source: Author’s Computation, 2026.

The regression findings refer to Research Question 3 but act contrary to Hypothesis 2. The model shows that there is a statistically significant relationship between the exposure to AI-driven fraud and the adoption of digital financial services (R^2 =.301, p = =.001), where the exposure level is the only predictor. However, the exposure coefficient is not standardised (B =.540, b =.548, p =.001), with a positive value indicating that the more the exposure, the higher the adoption, not the other way round. This observation suggests that users who experience AI-enabled fraud are not always left discouraged by the emergence of digital financial services, and there is a probability that they will continue or even increase their usage, possibly because of the lack of other options, confidence in the safety of platforms, or a habitual nature.

These findings imply that, in the Nigerian environment, exposure to AI-based fraud is not affecting the uptake of digital finance. This questions the existing counterpart premise that fraud has a direct and negative impact on usage and emphasises the tribulation or addiction of users to digital sites during risky-time. Despite the strength of the model (F = 89.495, p = <.001), the deviant pattern of the relationship suggests a qualitative investigation in detail regarding the motivations of the user, their perception of risks, and coping mechanisms against the danger of fraud.

Research Question 4: Which demographic groups are more vulnerable to AI-enabled fraud in Nigeria?

***H3**: “Demographic factors significantly influence vulnerability.”*

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)

Pearson Chi-Square	229.983[a]	156	.000
Likelihood Ratio	142.008	156	.782
Linear-by-Linear Association	6.421	1	.011
N of Valid Cases	210		

a. 172 cells (94.5%) have expected count less than 5. The minimum expected count is .00.

Symmetric Measures

		Value	Asymptotic Standard Error	Approximate T[b]	Approximate Significance
Interval by Interval	Pearson's R	.175	.078	2.568	.011[c]
Ordinal by Ordinal	Spearman Correlation	.092	.071	1.338	.182[c]
N of Valid Cases		210			

a. Not assuming the null hypothesis.

b. Using the asymptotic standard error assuming the null hypothesis.

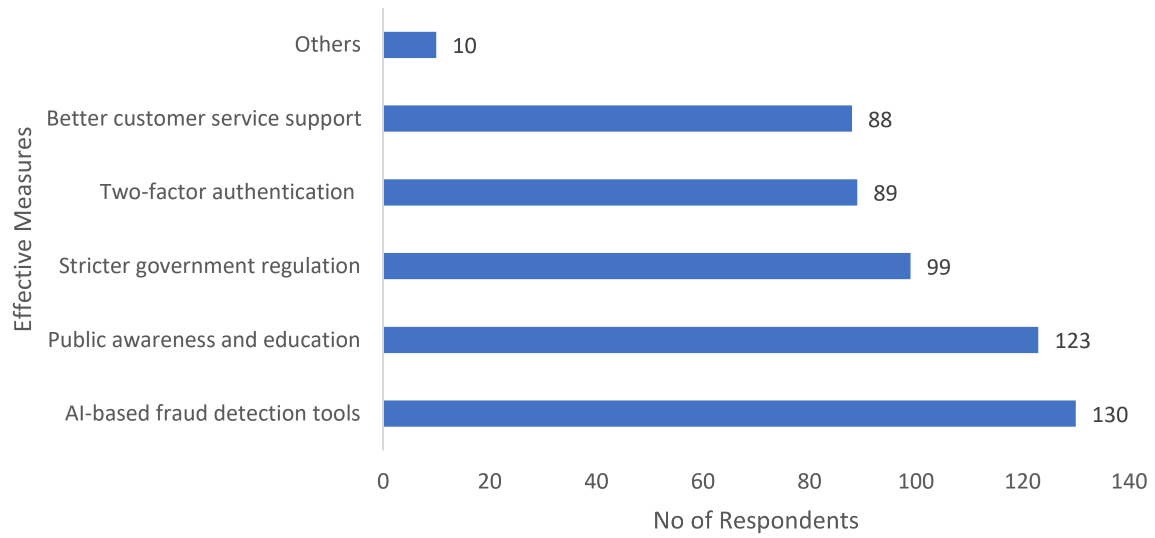
c. Based on normal approximation.

Source: Author’s Computation, 2026.

The outcome of the chi-square test shows that there is a statistically significant relationship between demographic and biographic variables, such as gender, age, education, employment, and income, and exposure to AI-enabled fraud (Pearson χ^2 = 229.983, df = 156, p =.000), which validates Hypothesis 3, which stated that demographic variables mediate vulnerability. This inference is, however, compromised by the sparsity of data, with 94.5^{-} of contingency cells having the expected frequencies less than five, which invalidates the strength of the chi-square. In conjunction with this, a significant Pearson correlation (r = .175, p = .011) shows a weak but statistically significant linear relationship between a composite measure of demographic factors and fraudulent exposure. The Spearman rank correlation is non-significant (ρ = .092, p = .182), which indicates that the ordinal relationship between the two variables is not strong.

Research Question 5: What effective measures can mitigate AI-driven fraud risks?

Fig 4: Effective Measures taking by Fintech Companies to Reduce AI-driven Fraud Risks



Source: Author's Computation, 2026.

The most effective interventions toward mitigating AI-prompted fraud were overwhelmingly supported by respondents (61.9%, n = 130) and the public awareness or education programmes (58.6%, n = 123). Two-factor authentication (42.4 %, n = 89) and a stronger government regulation (47.1%, n = 99) also had a wide support, indicating the need for intervention, both technological and political. Support was moderately greater in the case of the increased identity verification (23.8%) and better customer service (41.9%) as well, which means that users attach importance to the proactive security measures and to the prompt support. The low "Others" category (4.8%) indicates consensus around these key strategies. In general, the results highlight a more complex dual-tactic at the same time: complex AI protection and consumer empowerment via education as the strategy that is considered necessary to regain trust in the digital financial landscape of Nigeria.

Conclusion and Recommendations

This study shows that AI-driven fraudulent schemes, namely, AI-generated messages, voice-cloning, and deep-fakes, are common and individually experienced by a significant portion of users of digital-finance in Nigeria. However, the opposite results were obtained through quantitative analysis, which found that the more AI-driven fraud was exposed to, the higher the trust levels and use of digital financial services. It is an apparent behavioural trend of those who are well-established users and just continue using such services, either because the utility of the product can be noticed or because it has some institutional protection. Conversely, the qualitative results and additional evidence confirm that fraud cases significantly undermine the trust of new/vulnerable users, which is a threat to the promotion of financial inclusion.

The hypothesis that the level of vulnerability varies according to socio-demographic categories is supported by the demographic analysis, which, however, does not allow for determining high-risk groups due to methodological limitations. However, the answers provided by the respondents were quite concrete in terms of the immediate solutions, i.e, the introduction of AI to detect fraud, the strength of the activity aimed at educating the public, stricter regulation, and strengthening authentication processes.

It is recommended that;

- Financial institutions integrate real-time AI-based fraud detection tools and require two-factor authentication, and at the same time invest in transparent incident-response systems.
- A collaboration should be established between the Central Bank of Nigeria (CBN) and the Economic and Financial Crimes Commission (EFCC) to develop AI-specific guidelines on cybercrime, raise the level of control over fintech uses, and create a national fraud-reporting system.
- The regulatory bodies and telecom companies should lead in public-awareness efforts to enlighten consumers, especially the youth and rural communities, to recognise AI-enabled fraud.
- Co-operation across banks, fintech organisations, and global organisations in intelligence-sharing can support the monitoring and breaking of the cross-border AI-fraud networks.

To ensure that the emerging threats brought about by AI are alleviated, and benefits realised in digital financial inclusion are not compromised, Nigeria can pursue a multi-stakeholder approach that incorporates innovative technology and introduces a level of trust.

References

Adelaja, A. O., Umeorah, S. C., Abikoye, B. E., & Nezianya, M. C. (2024). Advancing financial inclusion through fintech: Solutions for unbanked and underbanked populations. *World Journal of Advanced Research and Reviews*, *23*(01), 427-438.

Appiah, T., & Agblewornu, V. V. (2025). The interplay of perceived benefit, perceived risk, and trust in Fintech adoption: Insights from Sub-Saharan Africa. *Heliyon*, *11*(2).

Central Bank of Nigeria (CBN). (2021). Regulatory framework for open banking in Nigeria. https://www.cbn.gov.ng

Economic and Financial Crimes Commission (EFCC). (2024). Annual cybercrime report 2023. Abuja: EFCC Publications.

Emovwodo, S. O., & Ayo-Obiremi, I. (2024). The Implications of Deep Fakes Impact on Politics and Elections: The Nigerian Narrative. In *Navigating the World of Deepfake Technology* (pp. 378-396). IGI Global.

Enhancing Financial Innovation & Access (EFInA). (2023). Access to financial services in Nigeria (A2F) survey 2023. Lagos: EFInA.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS quarterly*, 51-90.

Mwange, A., Chibesa, K. C., Matoka, W., & Kalaba, L. (2025). An Investigation of the Impacts of Artificial Intelligence on Financial Inclusion in Developing Economies: Case of Sub-Saharan Africa. *African Journal of Commercial Studies*, *6*(3), 27-35.

Oni, O., Japinye, A. O., Ifarajimi, G. D., & Olubowale, F. O. (2025). Regulating fintech for financial stability in Nigeria: balancing cybersecurity risks and financial inclusion. *African Journal of Economic and Business Research*, *4*(2).

Oyedokun, G. E., Anyahara, I. O., & Oyedokun, P. O. (2025). Harnessing FinTech and Artificial Intelligence for Financial Inclusion and Entrepreneurial Growth: An Empirical Review. *Journal of Economics, Finance and Management Studies*, *8*(7), 4741-4749.

Pantserev, K. A. (2022). Malicious use of artificial intelligence in Sub-Saharan Africa: Challenges for Pan-African cybersecurity. *Vestnik RUDN. International Relations*, *22*(2), 288-302.

PwC Nigeria. (2024). Consumer trust in digital financial services: A 2024 survey report. Lagos: PwC.

Suri, T., & Jack, W. (2016). The long-run poverty and gender impacts of mobile money. *Science*, *354*(6317), 1288-1292.

World Bank. (2021). The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19. Washington, DC: World Bank. https://doi.org/10.1596/37258

Zhang, W., Siyal, S., Riaz, S., Ahmad, R., Hilmi, M. F., & Li, Z. (2023). Data security, customer trust, and intention for adoption of Fintech services: an empirical analysis from commercial bank users in Pakistan. *Sage Open*, *13*(3), 21582440231181388.