© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722715

# Democratizing AI-Powered Fraud Detection: A Regulatory-Compliant Framework for Public Access to Receipt Verification in Nigeria's Banking Sector

DAUNIMIGHA TAMARAETUWEMI FAITH[1], ANYANWU LONGY[2], OSARENWINDA OSAS[3]
[1,2,3]*Department of Computer Science and Technology, Igbinedion University, Okada, Nigeria*

***Abstract-*** ***Nigeria's banking industry has adopted artificial intelligence (AI) for fraud detection and receipt verification as it continues to transform global financial systems. However, the general public the population most frequently harmed by scams, falsified receipts, and transaction fraud in the first place does not have access to these AI-driven safeguards. The exclusion is directly examined in this work, which treats it as bot a technological and a regulatory issue rather than just one. The study compares the current level of institutional AI adoption to the almost complete lack of tools designed for public use, drawing on a qualitative synthesis of academic literature, industry reporting, and stakeholder perspectives. It also examines how data-protection and cybercrime laws influence what can be safely implemented outside of institutional walls. The study then suggests a six-layer, legally compatible structure for public-facing fraud detection that combines explainable AI, consent-based data processing, and low-bandwidth access channels like USSD and WhatsApp. The results point to one main conclusion: as Nigeria's economy continues to digitize at a rapid pace, addressing this access gap is crucial for financial transparency, restoring consumer trust, and safeguarding regular users.***

***Index Terms-*** ***Artificial intelligence, fraud detection, receipt verification, financial inclusion, data protection, regulatory compliance, Nigeria, USSD.***

## I. INTRODUCTION

Transaction fraud has increased in tandem with the growth of digital finance in Nigeria, with the banking industry bearing a large portion of this burden [1]. A bank's ability to lend and invest in customer-facing services is reduced, credit for individuals and businesses downstream slows, and confidence in digital finance generally declines when it absorbs a fraudulent transaction [1]. The speed at which this has escalated is demonstrated by recent statistics. Twenty-four commercial banks reported fraud losses totaling ₦5.79 billion in the second quarter of 2023, a 1,125% increase from the ₦472 million reported just one quarter prior [2]. The overall value of attempted fraudulent transactions increased by 278% during that time, from ₦2.58 billion to ₦9.75 billion; fraudulent loans accounted for 94.35% of the losses, while computer/web fraud and mobile fraud contributed an additional ₦59.5 million and 3.39%, respectively [2].

The harm extends beyond banking: Nigerian customers are now more cautious about making purchases online due to fraud on digital payment platforms, which is pushing the market back toward cash-on-delivery and away from the government's objectives for a cashless economy [3]. While merchants lose money due to chargeback fraud and identity theft [5], consumers absorb this through account takeover and SIM-swap schemes[4].

Institutions have changed over time. In order to reduce fraud losses by about 30% in 2022, FirstBank integrated biometric verification, device fingerprinting, and behavioral analytics into its risk engine [6]. Access Bank, GTBank, Zenith Bank, and fintech companies like Flutterwave, Paystack, Carbon, and Interswitch all use machine learning to identify unusual logins, unusual transaction frequency, and unknown devices [7]. The ability to reveal intricate, changing patterns instead of matching against a predetermined list of warning signs is what makes these systems effective [8], and deep learning techniques are especially effective at capturing the temporal and multivariate signatures that fraud typically leaves behind [9]. However, none of this capability first reaches those who are presumably most vulnerable to deception. Small businesses and individual customers, who are most

affected by phishing, falsified receipts, and phony cellphone alerts, lack an impartial means of verifying the authenticity of a transaction. Theoretically useful tools like Paystack's, Flutterwave's, VerifyMe's, IdentityPass's, and Sudo Africa's authentication and risk-profiling APIs are designed for developers and businesses and are inaccessible to the average user due to technical requirements or subscriptions [7].

The public is exposed to a well-known vulnerability if they are left with only mobile banking apps and SMS alerts as their default confirmation tools. Both can be convincingly faked through spoofing apps and altered screenshots, and no central portal, neither from the CBN nor from NIBSS, allows anyone to directly verify a transaction reference. Nigeria's cybersecurity and data protection laws complicate matters even more. The Cybercrime (Prohibition, Prevention, etc.) Act, the Nigeria Data Protection Regulation (NDPR), and the Nigeria Data Protection Act (NDPA) all exist to protect security and privacy, but they were not designed with public-facing fraud-detection tools in mind, and their compliance burden tends to discourage precisely the kind of tool that this paper claims is lacking. As a result, the public has no real-time recourse and protection is centered solely within institutions. This distance leads to four goals. The objectives of this paper are to: (i) map the current use of AI in Nigerian financial institutions for fraud detection and receipt verification; (ii) assess the risks associated with keeping the public out of those same tools; (iii) trace how the NDPR, NDPA, and Cybercrime Act shape and constrain what a public-facing AI tool could look like; and (iv) propose a framework, based on both technical design and policy, that reconciles data privacy, cybersecurity, and digital inclusion rather than treating them as competing goals.

The contribution of the paper is threefold. It details a problem with public access in Nigeria's AI-driven fraud detection system that hasn't gotten any consistent scholarly attention. It pulls together three threads financial regulation, digital inclusion, and AI system design that are rarely examined collectively, even though they all influence what a practical, safe, and compliant tool would truly need. With ramifications that go beyond Nigeria to other Sub-Saharan African economies dealing with similar legislative fragmentation, it also suggests a tangible, legally valid framework that can be accessed by USSD and WhatsApp and is specifically tailored to vulnerable and low-literate people.

This is how the remainder of the paper goes. Related research on AI-driven fraud detection, receipt verification, and public access to financial AI tools is surveyed in Section II. The approach is outlined in Section III. The institutional environment of AI fraud detection in Nigerian banks is mapped out in Section IV. The shortcomings of current public-facing tools are examined in Section V. The governing legislative and regulatory framework is reviewed in Section VI. The suggested framework is presented in Section VII. The results are discussed in Section VIII, and recommendations and conclusions are concluded in Section IX.

## II. RELATED WORK

### A. Fraud Detection Using AI and Machine Learning

In general, artificial intelligence refers to a machine's ability to mimic cognitive functions that would normally need a person, such as reasoning, pattern recognition, and decision making. In contrast to traditional software, machine learning, a subtype of artificial intelligence, learns patterns from data and becomes more accurate as it sees more of it [9]. A fraud-detection system's ability to recognize patterns in real time is what allows it to identify anomalies that a static rule set would easily miss [10]. Additionally, it explains why manual audits and static rules continue to lose ground: They produce a lot of false positives and take a long time, if at all, to adjust to new fraud strategies [11]. This shortcoming has forced e-commerce, banking, healthcare, and education to use adaptive, learning-based detection [12].

A significant portion of the field's conceptual foundation was established early on: foundational surveys listed statistical and AI-based detection techniques and established classification frameworks that are still used today [13], [14], and [15], while more comprehensive reviews charted the development of data-mining-based fraud detection as

a field [16]. The blind spot that all studies have in common is that they were all based on Western datasets and institutions, and none of them offer a means of making the resulting tools available to the general public or small and medium-sized enterprises (SMEs). This study revisits this issue below.

B. Verification of Receipts and Authenticity of Transactions

In Nigeria's digital economy, receipt verification is crucial to preventing fraud, yet it is still one of the least developed sectors. Mobile editing apps and cloned receipt templates are sufficient for fraudsters to trick merchants and service providers [7], and the lack of a standardized, public method to verify a receipt contributes significantly to the persistence of these schemes [17]. When verification capability is present, it is not intended for the intended audience: The payment APIs offered by Flutterwave, Paystack, and Moniepoint are designed for developers and business clients rather than the customer or small seller who is really in possession of the receipt [18]. Offline vendors are most affected by this gap because they lack the technological tools to verify a receipt in real time if they rely on visual inspection [19].

The imbalance that results is referred to as a "fraud asymmetry" by Adejumo [20]: fraudsters have simple-to-use forging tools, but their victims have nothing similar to defend themselves with. While blockchain-based, tamper-evident receipt tracking is being discussed in academia without significant funding [22], Nigeria has not yet adopted this model on a large scale. Kenya and India, for example, both operate public verification portals and USSD-based checks that allow users to confirm a transaction identifier directly with their financial institution [21].

C. Financial AI Tools Available to the Public

The majority of fraud-detection methods used by Nigerian banks are closed and proprietary, which is good for the institutions but leaves informal traders and small company owners with nowhere to turn when they come across a fraudulent transaction or a bogus warning [23]. The stakes are high since a significant portion of Nigeria's mobile-based financial activity involves individuals who are either underbanked or unbanked and who lack access to any kind of public fraud-checking tool. More than just annoying individual users, this absence contributes to a general skepticism in digital banking, especially among rural and low-literate populations who have nothing to rely on but the sender's or the institution's own word [24]. This is exacerbated by infrastructure deficiencies, legal obstacles, and poor public awareness: even in cases when interpretable anomaly-detection techniques are available technically, they seldom translate into an interface that the average user might truly utilize [25].

Low-bandwidth is one approach that researchers consistently recommend: USSD-based checks and WhatsApp bots that validate a receipt code, a timestamp, or a bank identifier are ideal for areas with low internet penetration [26], and there is a concurrent push for CBN-regulated, open-source APIs that would enable third-party developers and civic-tech organizations to incorporate verification directly into the apps that people already use [27].

D. Deficits in Current Literature

This set of work reveals five recurrent gaps. The first is the lack of interpretable models that have been evaluated against fraud signatures unique to Nigeria, such as SIM-swap schemes, insider collaboration, and forged receipts [28]. This is because the majority of published ML/DL models are trained on datasets that just do not reflect these patterns. The second is that because technical research almost exclusively focuses on institutional performance, there is virtually no theoretical work directed at public-facing frameworks, such as open-source fraud warnings and community verification APIs.

The third is directly related to the second: there isn't any theoretical or empirical support for democratizing the current AI fraud-detection capabilities for Nigerians. Fourth, rather than being based on real-time prediction, detection in Nigeria is still mostly reactive, prompted by user complaints or after-the-fact investigations [29]. As a result, there are very few adaptive, real-time models that are customized to local fraud typologies. Fifth, despite evidence that poorly calibrated fraud flags drive consumers in rural and underdeveloped areas away from digital platforms entirely, there is seldom any

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722715

connection between fraud-detection design and the larger socioeconomic picture, including digital trust, financial inclusion, and customer retention [30]. A typical sampling of investigations against these gaps is presented in Table I.

TABLE I. Representative Studies and Identified Gaps

| Study | Focus | Identified Gap |
|---|---|---|
| Ngai et al. (2011) | Categorized data-mining techniques (neural nets, decision trees, SVM) for fraud detection, mainly in Western industries. | No regional focus on Africa or Nigeria; no public-access consideration. |
| Abdulrahman et al. (2016) | Comprehensive review of fraud detection in telecom and banking, emphasizing backend/institutional systems. | No proposed model for public or SME-facing fraud mitigation. |
| Akinyemi & Adebisi (2022) | Examined how digital fraud erodes customer trust in Nigerian banks; recommends stronger institutional response. | Focuses on customer experience rather than AI system design for detection. |
| Kou et al. (2004) | Foundational survey categorizing statistical and AI-based fraud detection approaches. | Predates mobile-first, real-time banking prevalent in Nigeria today. |

## III. RESEARCH METHODOLOGY

Descriptive and conceptual analysis are combined in this qualitative, exploratory study. The descriptive section examines the current state of digital payment verification in Nigeria and its shortcomings, including inefficiencies, risks, and public access limitations. The theoretical framework and system architecture outlined in Section VII are developed from those discoveries in the conceptual half.

This analysis is based on two types of data. Peer-reviewed academic articles, industry and regulatory reports, and international fraud studies were the sources of secondary data. Institutional disclosures from Nigerian banks and fintechs, as well as guidelines from the Central Bank of Nigeria and the Nigeria Data Protection Commission, were also included. Unstructured, expert-informed observations of practice in Nigeria's banking, fintech, and informal-commerce sectors made up the smaller, supporting role of primary data, which was primarily utilized to contextualize and cross-check the secondary evidence rather than to stand alone as a statistical conclusion.

Since there isn't currently a centralized, public-facing fraud-verification system in Nigeria for this study to test empirically, a conceptual rather than experimental approach is appropriate in this case. Instead of assessing a deployed system, the paper synthesizes what is known about institutional AI adoption, current public-facing tools, and applicable regulation, and it creates a framework where each component is connected to a particular gap or constraint found along the way. This is part of a long-standing tradition in information systems research where a strong, empirically supported proposition does not need an existing tested artifact. Empirical testing of the framework through a deployed prototype and user studies — is left as a direction for future work, discussed in Section IX.

## IV. THE AI FRAUD DETECTION INSTITUTIONAL LANDSCAPE

There have been three major waves of digitization in Nigerian banking. ATM withdrawals, online banking, and mobile alerts became commonplace during the early adoption years (2000s–2015), and the 2014 launch of the Bank Verification Number (BVN) strengthened digital identity and reduced impersonation fraud. Fintech companies including Paystack, Flutterwave, and Opay joined the subsequent mobile banking boom (2015–2020), and USSD codes made banking accessible to Nigerians without dependable internet access, especially outside of big cities.

With AI chatbots, remote onboarding, and digital-only banks like Kuda Bank, ALAT by Wema, and VBank changing what a "bank" even means to many consumers, adoption has accelerated even further after the pandemic (2020–present).

Beneath this, whenever institutional AI fraud detection is implemented, it typically follows a similar pathway. Transaction records, behavioral indications (location, device identifiers, login habits), and external sources like the BVN/NIN databases are all used in data collecting. After preprocessing and labeling the data against past fraud and valid cases, feature engineering extracts signs that are worth keeping an eye on, such as an odd login time, a fast series of multi-ATM withdrawals, or a BVN/NIN mismatch. Three approaches are used in modeling itself: supervised techniques like Random Forest or logistic regression trained on labeled cases, unsupervised techniques like k-means or Isolation Forest for identifying outliers without a prior label, and, increasingly, deep learning for the more intricate patterns required for real-time detection. High-risk transactions are then blocked or flagged for human inspection via score-based monitoring, and a feedback loop feeds Three approaches are used in modeling itself: supervised techniques like Random Forest or logistic regression trained on labeled cases, unsupervised techniques like k-means or Isolation Forest for identifying outliers without a prior label, and, increasingly, deep learning for the more intricate patterns required for real-time detection. High-risk transactions are then blocked or flagged for human inspection via score-based monitoring, and a feedback loop feeds. Table II lists representative deployments across several institutions. The pattern holds regardless of which bank or fintech is involved: fraud-detection capability is genuinely sophisticated, but it never leaves the institution's own infrastructure.

TABLE II. Selected Institutional AI Fraud-Detection Deployments in Nigerian Banking

| Institution | AI Application | Reported Focus / Outcome |
|---|---|---|
| FirstBank of Nigeria | Biometric verification, device fingerprinting, behavioral analysis | ~30% reduction in fraud-related losses (2022) |
| Access Bank | Login-pattern and geolocation anomaly detection | Automated account locks on anomalous login behavior |
| GTBank | Real-time transaction monitoring, AI chatbots | Customer profiling; complaint data feeds fraud pipeline |
| Zenith Bank | Predictive risk engine on historical transaction data | Flags deviations from customer behavioral baseline |
| Flutterwave | Behavioral analytics, device fingerprinting | Real-time alerts on anomalous transaction frequency |
| Paystack | Risk engine (IP reputation, transaction velocity) | Configurable fraud rules exposed via developer API |
| Carbon | Behavioral scoring on mobile/SMS/financial data | Flags loan-stacking and account-takeover patterns |

## V. THE GAP IN PUBLIC ACCESS

The average Nigerian has very little to work with when attempting to verify the authenticity of a receipt or payment confirmation, despite the sophistication detailed in Section IV. The tools that are now available are designed for developers, banks, and merchants, and they support business partnerships, subscriptions, and APIs. Nobody operates a centralized platform where the public may enter a transaction reference and receive a real-time response, including the CBN, NIBSS, and individual

banks. As a result, people, vendors, and unofficial enterprises are unable to independently verify anything.

A few more recent tools reduce but do not completely close this gap. The Federal University of Technology, Akure's Cybersecurity Science Department created OpenFraudDB, also known as FraudSentry, which is Nigeria's first open fraud database. It accepts public data contributions and provides a free, research-focused API, but registration is still necessary. ReceiptNG, a Lagos-based company, exclusively verifies receipts by email-requested API access; it is not available to the general public. The Eagle Eye App from the EFCC allows the public to report suspicious activities, but it is not a verification tool; rather, it is a reporting route. Although Taggun's fake-receipt detector uses artificial intelligence (AI) to identify tampering or duplication, it was not designed for Nigeria and does not have access to Nigerian bank records. In keeping with the theme of this study, PalmPay has implemented its own AI-driven fraud monitoring system, but it remains internal. The platforms that are most frequently referred to as "public-facing" actually fall short in Table III.

TABLE III. Public-Facing Verification Tools and Their Limitations

| Tool / Platform | Promise | Limitation |
|---|---|---|
| VerifyMe / IdentityPass | Identity and document verification; fraud-risk scoring | B2B only; no receipt-level verification for individuals |
| Sudo Africa | Card-issuing API with fraud-protection tools | Developer-centric; no consumer-facing interface |
| Paystack / Flutterwave APIs | Transaction verification and receipt tracking | Requires technical integration; built for merchants |
| Bank apps / SMS alerts | Public confirmation of balances and transfers | Easily forged via spoofing and fake-alert apps |
| POS devices | Print receipts and log transactions | Often offline; not cross-verified with bank data in real time |

The discrepancy is worse than the tool count alone indicates due to two additional factors. Even with systems specifically designed to combat fraud, such as KYC/AML checks, risk scoring, and ID validation, access is still merchant-only. These tools are priced for institutions rather than individuals or small vendors and need integration effort. Additionally, low trust is exacerbated by digital illiteracy: even when a tool is ostensibly available, understanding of it is poor, trust in fintech apps is unstable, and victims of fraud sometimes don't report what occurred to them at all due to ignorance or fear. When taken as a whole, this suggests a systemic access issue rather than a lack of underlying technology; inclusive design, enforcement, and reach—rather than algorithmic capability—are lacking.

## VI. LEGAL AND REGULATORY FRAMEWORK

In Nigeria, regulations pertaining to AI and financial data are still being developed, and they now provide problems for anyone attempting to create a tool that is visible to the public while still serving as a vital safeguard. The Regulatory Framework for Open Banking (2021) and the Risk-Based Cybersecurity Framework for Deposit Money Banks and Payment Service Providers [31] are two of the fintech-related frameworks released by the Central Bank of Nigeria. While both define data-sharing and security procedures, neither mandates or even actively promotes the use of AI tools by the general public.

Open Banking, in principle, allows third parties to access financial data with customer consent, but

rollout has been sluggish security concerns and the lack of a legal mandate for end-user-facing AI have slowed it down [32] which makes it harder for anyone to build a public verification platform in partnership with the banks that hold the data.

The Nigeria Data Protection Regulation (NDPR) of 2019, which prioritizes user privacy and requires express agreement for data processing, is still the most important piece of legislation in the field of data protection [33]. The deployment of machine-learning models that analyze personal financial data for fraud detection is actually questionable since it does not directly address AI or automated decision-making [34]. Building on this, the Nigeria Data Protection Act (NDPA) of 2023 expressly prohibits automated decision-making, including AI-driven profiling, that has a legal or otherwise substantial impact on an individual unless there is express agreement, a contractual requirement, or a legal obligation [35]. In practical terms, this means that consent must be the foundation of any public-facing verification tool from the start rather than being bolted on afterwards.

Any AI tool that analyzes transaction data or messages for fraud must be carefully constructed to avoid violating the Cybercrime (Prohibition, Prevention, etc.) Act of 2015, which renders unauthorized access to computer systems and communication interception illegal [36]. AI-driven innovation at the infrastructure level is supported by the Nigerian Communications Commission's National Policy on Fifth-Generation (5G) Networks (2021), but it was created for business, not for the general public [37]. Legal experts have raised the more general point that Nigeria's financial and cyber laws have not kept up with technological advancements; fraud is still mostly viewed as a criminal justice issue that needs to be addressed after the fact rather than as something that public-facing technologies may prevent [38]. The institution-only status quo from Sections IV and V is essentially maintained by the Cybercrime Act, which mandates that institutions report breaches but falls well short of compelling them to make any fraud-detection capabilities available to the public[36], [39]. When combined, these tools reduce to four practical requirements for any public-facing AI fraud-detection tool: data security, to prevent personal information from falling into the wrong hands; consent management, so users are knowingly opting in; transparency, so a flagged decision can actually be explained; and ongoing compliance, considering how new much of this legislation is. Each of these is directly included into the subsequent structure in Section VII.

## VII. SUGGESTED REGULATION-COMPLIANT PUBLIC ACCESS FRAMEWORK

This paper presents a six-layer conceptual framework for public-facing, AI-powered receipt verification that is expressly designed to function within the NDPA, NDPR, and Cybercrime Act rather than outside them. It does this by combining the limitations mentioned in Sections V and VI.

### A. Consent Layer and Data Gathering

Only when a user has expressly consented to the collection of financial and transactional data such as photos of receipts, SMS content, and sender identifiers after being informed of what is being collected, why (fraud analysis, nothing else), and how it will be used (detection only, never commercial). The NDPA's requirements for automated processing are initially satisfied by the ability to revoke consent at any moment.

### B. Explainability and Transparency of AI Models

Instead of using a black-box classifier, every verification choice is based on an explainable model. Instead of a simple, unexplained risk score, the user sees a plain-language explanation such as "logo mismatch" or "unverified sender ID" when a receipt is reported. The NDPA's demand that automated judgments with actual human repercussions be explicable is directly satisfied by this.

### C. Layer of Data Security and Privacy

All user-submitted data is secured while it's in transit and at rest. Receipt scans and message content are maintained for a brief, disclosed window, and users can request deletion at any time. Personally identifiable information is only retained for as long as verification strictly necessary. The purpose of this layer is to ensure that the system stays within the

boundaries set by the Cybercrime Act, NDPA, and NDPR.

D. Evaluation of Risk and Bias

The system undergoes a Data Protection Impact Assessment (DPIA) prior to becoming live, and the model is then routinely examined for bias toward particular banks or vendors as well as for false-positive rates that skew across user categories. In response to the fairness gap mentioned in Section II-D, disputed or flagged instances are sent to a human reviewer instead of being automatically resolved.

E. Regulatory Alignment, Ethics, and Governance

The system's operator must register as a data processor with the Nigeria Data Protection Commission, designate a Data Protection Officer to supervise it, and maintain risk documentation, model accountability records, and audit trails in accordance with the NDPC's General Application and Implementation Directive (GAID).

F. Regulatory Alignment, Ethics, and Governance

The system's operator must register as a data processor with the Nigeria Data Protection Commission, designate a Data Protection Officer to supervise it, and maintain risk documentation, model accountability records, and audit trails in accordance with the NDPC's General Application and Implementation Directive (GAID).

Put together, the evidence in this paper points toward one consistent conclusion: Nigeria's public-access gap in AI fraud detection is not, at its core, a technology problem. The modeling approaches covered in Sections II and IV supervised and unsupervised learning, deep architectures, explainable AI are mature and already running at scale inside Nigerian institutions. What's actually missing is inclusive design, a regulatory posture that makes public deployment easier rather than harder, and enough commercial or civic incentive for anyone to extend these tools past the institutions that built them. That reframing has policy implications: closing the gap should mean prioritizing interoperability mandates, open verification APIs, and USSD/WhatsApp-accessible interfaces, rather than pouring more investment into institutional-side detection accuracy that is already comparatively strong.

The regulatory analysis in Section VI points to something else worth naming: Nigeria's data-protection instruments, although framed as consumer protections, currently work asymmetrically. They do far more to constrain how a third party might build a public verification tool than they do to constrain how a bank processes the same kind of data internally for its own fraud system. Kenya and India, where public verification portals and USSD-based checks already run, suggest this asymmetry is a policy choice rather than something data-protection law makes unavoidable and that a regulator-sanctioned sandbox for public-facing fraud tools, of the kind recommended in Section IX, could fix it without weakening the privacy protections underneath.

This study carries limitations that come with its conceptual design. It synthesizes secondary evidence and a limited amount of primary observation rather than testing a live system, so questions about the proposed framework's usability, latency, and real-world detection accuracy remain open until it's actually validated empirically. The literature reviewed also skews toward Lagos-centric fintech activity, and the framework's assumptions about USSD and WhatsApp accessibility specifically need testing against rural and lower-income user segments before any deployment.

## VIII. CONCLUSION AND RECOMMENDATIONS

This paper set out to examine Nigeria's growing institutional reliance on artificial intelligence for fraud detection and receipt verification, and has argued that the resulting protections remain almost entirely out of reach for the public they are, indirectly, supposed to serve. A review of existing platforms Paystack, VerifyMe, and Flutterwave among them, alongside newer entrants such as OpenFraudDB and ReceiptNG shows that current tools simply weren't built with public usability in mind, whether the obstacle is technical complexity, restricted access, or regulatory friction. The result is that individuals and small businesses stay exposed to

fake alerts, manipulated receipts, and unauthorized transactions, with no centralized, legally compliant, user-friendly way to check any of it — a significant and largely unaddressed vulnerability in Nigeria's digital payment ecosystem.

In response, this paper proposes a publicly accessible, AI-powered verification framework built to work within the NDPA, NDPR, CBN KYC/AML guidance, and applicable fintech licensing requirements prioritizing usability, low cost, and integration with the mobile financial tools Nigerians already use. Based on these findings, six recommendations follow:

1) Build a public-facing AI verification platform: fintech firms and developers should work together on a mobile-first tool that lets individuals verify a receipt using its reference number, timestamp, or image.

2) Require regulatory support and open APIs: the CBN and NIBSS should mandate sanitized, public-use transaction-verification APIs under strict data-protection and consent rules, so third-party platforms can build public tools without running afoul of financial regulation.

3) Build in USSD and mobile channels from the start: verification tools need USSD or SMS support to actually reach users without smartphones or reliable data.

4) Fund public awareness and digital literacy: government agencies, banks, and civil-society groups should run real campaigns on recognizing fraud and using verification tools once they exist.

5) Open regulatory sandboxes: regulators should let experimental, public-facing fraud-detection tools be piloted under supervision before full rollout.

6) Keep it affordable and open: developers should lean toward freemium or open-source models so small vendors and individual users aren't priced out of a service meant to protect them.

From here, the natural next step is empirical: piloting the proposed framework as a USSD or WhatsApp-based prototype, testing usability specifically with rural and low-literacy users, and comparing results against the public verification systems already running in Kenya and India — work that could surface design lessons applicable well beyond Nigeria, across Sub-Saharan African markets facing similar regulatory and infrastructural limits.

REFERENCES

[1] M. Manyo, A. Olayemi, and C. Mgbemena, "Digital fraud and banking resilience in Nigeria," International Journal of Finance & Economic Studies, vol. 9, no. 3, pp. 133–149, 2023.

[2] D. Akintaro, "Nigerian banks lose ₦5.79 billion to fraud in Q2 2023," BusinessDay Nigeria, 2023.

[3] E. Okolie and T. Ojomo, "E-commerce fraud and cashless economy in Nigeria," Journal of Economic Perspectives in Africa, vol. 6, no. 4, pp. 88–102, 2020.

[4] V. Komandla, "SIM swap fraud in African mobile banking," Cybersecurity Trends in Emerging Markets, vol. 5, no. 1, pp. 70–82, 2024.

[5] A. Mutemi and F. Bacao, "Merchant risk and chargeback fraud in Nigeria's e-commerce," African Journal of Information Systems, vol. 10, no. 1, pp. 1–14, 2024.

[6] FirstBank of Nigeria, Annual Report and Audited Financial Statements, 2022.

[7] A. Adebayo and C. Eze, "Emerging risks in Nigeria's fintech landscape: Policy implications for digital fraud," African Journal of Finance and Policy, vol. 14, no. 2, pp. 44–59, 2022.

[8] P. Kamuangu, "A review on financial fraud detection using AI and machine learning," Journal of Economics, Finance and Accounting Studies, vol. 6, no. 1, pp. 67–77, 2024.

[9] I. H. Sarker, "Deep learning: A comprehensive overview on techniques, taxonomy,

applications and research directions," SN Computer Science, vol. 2, no. 6, art. 420, 2021.

[10] M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, "From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy," IEEE Access, vol. 11, pp. 80218–80245, 2023.

[11] E. I. Okoye and D. O. Gbegi, "Forensic accounting: A tool for fraud detection and prevention in the public sector," International Journal of Academic Research in Business and Social Sciences, vol. 3, no. 3, pp. 1–19, 2013.

[12] H. Drammeh, "The socioeconomic cost of fraud in West African digital economies," African Journal of Socioeconomic Research, vol. 11, no. 1, pp. 12–27, 2023.

[13] E. W. T. Ngai, Y. Hu, Y. H. Wong, Y. Chen, and X. Sun, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," Decision Support Systems, vol. 50, no. 3, pp. 559–569, 2011.

[14] A. Abdulrahman, M. A. Maarof, and A. Zainal, "Fraud detection system: A survey," Journal of Network and Computer Applications, vol. 68, pp. 90–113, 2016.

[15] Y. Kou, C. T. Lu, S. Sirwongwattana, and Y. P. Huang, "Survey of fraud detection techniques," IEEE Transactions on Systems, Man, and Cybernetics – Part C, vol. 31, no. 4, pp. 426–433, 2004.

[16] C. Phua, V. Lee, K. Smith, and R. Gayler, "A comprehensive survey of data mining-based fraud detection research," arXiv:1009.6119, 2010.

[17] K. Ogundele, "Visual deception: The rise of fake bank receipts," Nigerian Financial Monitor, vol. 3, no. 1, pp. 44–58, 2023.

[18] A. Nwosu and S. Akinlade, "Engineering fraud prevention APIs in Nigerian fintechs," TechPolicy Nigeria Journal, vol. 5, no. 1, pp. 88–100, 2023.

[19] A. Obasi and A. Ekong, "Informal vendors and the crisis of digital fraud," African Journal of Business and Society, vol. 7, no. 2, pp. 71–85, 2023.

[20] M. Adejumo, "Fraud asymmetry in Nigeria's informal sector," Journal of African Economic Review, vol. 10, no. 1, pp. 25–39, 2022.

[21] World Bank, "Digital financial services in Africa: Innovations and inclusion," World Bank Report, 2022.

[22] S. Ibrahim and E. Okoye, "Blockchain for receipt tracking in African finance," Journal of Financial Blockchain Research, vol. 2, no. 1, pp. 33–47, 2023.

[23] A. Tagbo and A. Adekoya, "Institutional bias in AI fraud detection in Nigeria," African Journal of Cyber Policy, vol. 2, no. 2, pp. 53–69, 2024.

[24] S. Kovacevic, J. Nwachukwu, and A. Abass, "The usability gap in African fintech: Trust and access," Digital Economy & Inclusion Journal, vol. 6, no. 1, pp. 11–29, 2024.

[25] B. Onyeama, "Machine learning interpretability for Nigerian fraud analytics," African AI Review, vol. 3, no. 2, pp. 22–36, 2024.

[26] J. Awosika, K. Umeh, and T. Olanrewaju, "Building inclusive fintech AI with USSD," Journal of Inclusive Tech for Africa, vol. 4, no. 2, pp. 93–107, 2023.

[27] M. Waliullah, E. Iro, and B. Ogunleye, "Enabling open-source AI in Nigerian fintech," Journal of Open Technology Governance, vol. 1, no. 1, pp. 1–22, 2025.

[28] D. Oyeniran and F. Okoye, "SIM-swap and insider fraud in Nigerian banking," West African Financial Crimes Journal, vol. 2, no. 2, pp. 70–85, 2021.

[29] A. Akinyemi and M. Adebisi, "Exploring customer trust and digital fraud in Nigerian banking," Journal of Financial Crime Studies, vol. 9, no. 2, pp. 112–129, 2022.

[30] N. Okafor and J. Ibe, "Digital trust and exclusion in Nigeria's cashless economy," Journal of Financial Inclusion, vol. 2, no. 3, pp. 60–76, 2023.

[31] Central Bank of Nigeria, "Risk-based cybersecurity framework for deposit money banks," CBN, 2021.

[32] K. Okafor and T. Bassey, "Open banking in Nigeria: From regulation to execution," Journal of African Financial Law, vol. 8, no. 2, pp. 29–47, 2023.

[33] Nigeria Data Protection Commission, Nigeria Data Protection Regulation (NDPR), 2019.

[34] T. Akinyemi and O. Solanke, "Privacy regulations and AI compliance in Nigeria's fintech industry," West African Journal of Digital Law, vol. 3, no. 1, pp. 40–54, 2024.

[35] Federal Republic of Nigeria, Nigeria Data Protection Act (NDPA), 2023.

[36] Federal Republic of Nigeria, Cybercrime (Prohibition, Prevention, etc.) Act, 2015.

[37] Nigerian Communications Commission, "National policy on 5G networks for Nigeria's digital economy," NCC, 2021.

[38] F. Adelakun and T. Lawal, "Legal perspectives on AI ethics and fraud in Nigerian fintech," Nigerian Law and Technology Review, vol. 7, no. 1, pp. 71–88, 2022.

[39] K. Oduwole, "Cybersecurity legal gaps in Nigeria's digital banking laws," Journal of Digital Law in Africa, vol. 4, no. 1, pp. 18–33, 2023