NOUN Interdisciplinary Journal of Computing, E-learning & Application (NOUN-IJCEA)
https://ijcea.nou.edu.ng
Volume 1 Number 1, April 2026 pp. 39-51

The Effectiveness of Two-Factor Authentication in Preventing Online Banking Fraud in Nigeria

[1]Grace Egenti, *[2]John Ojo Ajayi

[1]Department of Cybersecurity, National Open University of Nigeria
[2]Africa Centre of Excellence on Technology Enhanced Learning (NOUN), Abuja.
gegenti@noun.edu.ng, aonejotech@gmail.com
*Corresponding Author: aonejotech@gmail.com

ABSTRACT

This research evaluates the effectiveness of two-factor authentication (2FA) in the context of fraud in online banking in Nigeria. A mixed-method approach combining statistical data from 2019 to 2024, banking security experts' opinions and a challenge-response authentication system prototype evaluation is utilised to understand the effectiveness of the existing 2FA security mechanisms against online banking fraud in Nigeria. The findings show that fraud cases decreased by about 10-15% after the proliferation of 2FA while there was a reduction in the compromise rate to 0% for app-based authentication compared to 4% for SMS-OTP. The findings suggest that despite reducing the rate of low-level fraud by approximately 10-15%, 2FA has a minimal impact on financial losses, which is escalating because of sophisticated attacks such as phishing and SIM-swap fraud. Qualitative findings emphasise the numerous loopholes in SMS-based 2FA, such as latency, vulnerability to interception and dependency on unsafe fallback mechanisms; biometric and app-based authentication methods appear more practical, faster and secure and have been confirmed by the prototype evaluation with a drastic reduction in the compromise rate and improvement in user experience in app-based 2FA, especially against complex attack scenarios. Hence, it recommends the use of a combination of security measures such as advanced authentication systems, real-time fraud detection mechanisms (using artificial intelligence), and user education awareness programmes, as 2FA alone is not sufficient to defend against the increasing threats, thus it would be of interest to banking institutions and regulators hoping to improve security frameworks within developing digital economies.

Keywords: Artificial intelligence, Banking fraud detection, Biometric authentication, Cybersecurity, Digital banking, Multi-factor authentication

1. INTRODUCTION

The role of digital banking in the banking industry has grown rapidly in Nigeria, increasing financial inclusiveness, and continues to change and create both opportunities and challenges for banks, as such making it easier for hackers to access financial systems. Fraud in Nigeria's banks amounts to N52.26 billion in 2024, up from N11.61 billion in 2020 despite a decline in the amount of reported incidents (Nigeria Inter-Bank Settlement System [NIBSS], 2025). There has been a 325% rise in internet banking fraud from 2022 to 2023, where over 50% of bank fraud loss occurs from the internet/mobile devices (NIBSS, 2024) and academic studies support that there is a positive relationship between internet usage and fraud: “The overall online banking system in Nigeria is responsible for an

increased probability rate of bank fraud, specifically with poor control of the regulatory bodies" (Olelewe & Onwumere, 2024). Likewise, "a negative and strong correlation exists between amount of e-fraud and incidence of e-fraud in Nigerian banks" (Fatoki, 2023). The statistics clearly point to evolving fraud, especially with hacking, making it vital to test for the efficacy of security measures, such as two-factor authentication (2FA), against these changing tactics in Nigeria. While Nigerian banks use SMS, OTP, app-based and biometric 2FA, fraud is prevalent. Such fraud is often due to issues such as SIM swaps, phishing and network delays that render security measures ineffective, especially SMS-based 2FA, where SMS-based 2FA is a risk as it passes through middlemen to the user, making it accessible to interception (Ogunrinde, 2025). Mustapha and Sinha (2024) also found that Nigerian banks' use of 2FA still has auditing and usability challenges that facilitate continued exploitation even after it has been deployed.

These problems show that two-factor authentication is insufficient; the combination of problems with technology and operations still allows threat actors to navigate around these controls, and continues to commit fraud, even when 2FA is nominally in place. There is a lack of empirical evidence to support the actual effectiveness of two-factor authentication in combating the issue of online banking fraud in Nigeria, despite 2FA being commonly adopted in the Nigerian banking sector. Most of the research has focused more on the existence of 2FA in a banking environment rather than on its effectiveness in combating new kinds of threats like phishing, social engineering and SIM swap attacks. Furthermore, there has not been enough research to compare different kinds of 2FA used by banks in Nigeria, especially regarding its usability, vulnerability and its actual impact on fraud. The absence of adequate research implies a dire need to adequately determine the effectiveness of 2FA through both technological and human aspects (Momoh and Ogbeide, 2025).

2FA's relevance and implementation are key information for Nigerian banks, regulatory bodies, and cybersecurity practitioners as well as the everyday Nigerian bank user. Though 2FA is already a widely used feature in banking, adequate information is lacking about how 2FA can be best implemented in a bid to effectively combat fraud. It is observed in the opinion of Ama, Onwubiko and Nwankwo (2024) that SIM-swap and smishing attacks persist due to lack of effective control and users'poor cybersecurity awareness. Similarly, Mustapha and Sinha (2024) state that currently, designs of 2FA are easily exploitable because of a lack of adequate implementation and little user involvement. Ofoegbu (2024) suggests better security measures like biometrics, app-based tokenisation, and AI-driven fraud detection methods.

The premise of this study relies on cybersecurity risk management concepts as well as user-centric security theories, implying that the success of a security system is a combination of both technology and human interaction with the system and usability of the system. Numerous studies have identified the correlation between the adoption of a system of security (e.g., cybersecurity infrastructure, user awareness and technological integration) and occurrences of security breaches in banking. The effectiveness of 2FA is regarded here as a result of system design and user engagement with the system, a theory which broadly supports security principles of integrating technological solutions with human factors in preventing security risks. In this light, the effectiveness of 2FA is treated as a function of both system design and user engagement, supporting broader frameworks that aim to integrate technological security systems with human factors. Results derived from this research will aid banks in Nigeria with the optimisation of their identity verification and authentication strategies, enable regulatory frameworks (e.g., CBN risk-based cybersecurity guidelines) and raise the awareness of digital banking among individuals to significantly enhance the security of online banking in Nigeria. The relevance of this study lies in the analysis of the effectiveness of two-factor authentication to reduce unauthorised transactions by comparing data related to fraudulent transfers and account takeovers in comparison to metrics related to fraud and in identifying vulnerabilities in 2FA which range from SIM swaps, phishing, one-time password delays, and customer complaints. To

improve the use of 2FA in Nigeria, strategies such as the adoption of biometrics or app-based authentication and users' cybersecurity education, as well as increased awareness, have been advised alongside improvements in fraud detection measures.

2. LITERATURE REVIEW

2.1 Theoretical Foundations of Two Factor Authentication

2FA makes security stronger by combining 'something you know, like a password, with 'something you have', like a one-time-password sent to user's device or a smartphone, or 'something you are', like biometrics. Two key findings are paramount: two-factor authentication can make accounts more secure but usability issues like hardware tokens reduce its effectiveness. The second is that user convenience and satisfaction are important to understand and achieve sustainable security compliance. In furtherance to this, 2FA is used by Twitter and Facebook, and some domain hosting companies, meaning that a login credential and a verification number obtained via a mobile device is used (Budiningsih et al., 2019; Jain et al., 2021; Khader et al., 2021). This process lessens the chance that an account will be compromised and restricts an attacker from stealing a genuine account and using it to the attackers' advantage.

The efficiency of multi-factor authentication (MFA) in contemporary systems has been better understood. When used correctly, multi-factor authentication dramatically lowers the risk of credential-based attacks (National Institute of Standards and Technology 2022). Similarly, to this, the European Union Agency for Cybersecurity (2021) states that while phishing-related attacks are a persistent problem, financial institutions which are applying strong authentication mechanisms have a lower susceptibility to attacks. Additionally, Grassi, Garcia, and Fenton (2021) clarify that rather than targeting encryption systems directly, attackers are increasingly taking advantage of weaknesses in authentication procedures, underscoring the necessity of a strong 2FA implementation.

2.2 2FA Adoption and Usage in Nigerian Banks

This paper proposed that 2FA should be linked to the nation's fraud prevention system, and that risk-based authentication should be deployed. However, this study did not account for practicability. Pilot models that use biometric and OTP tiers, like Imo State University in 2025 show promise in the making of 2FA security stronger when practical constraints are addressed. Different two-factor authentication methods offer different degrees of usability and security. Although SMS-based OTP is popular in developing countries, it is very vulnerable to sniffing and SIM swap attacks. However, biometric authentication systems and app-based authenticators are better to protect from unauthorised access but can introduce technical and user issues. Moreover, studies showed that phishing-resistant authentication systems, such as biometrics and hardware tokens, provide users better security confidence compared to SMS-based ones but also decrease user comfort and increase deployment expenses (Koyeda, 2025; Ponemon Institute, 2023). In support for the adoption of 2FA, Ezugwu et al., (2023) opined that adopting 2FA is an additional layer of security, and the researchers strongly recommended the adoption of the 2FA method.

2.3 Fraud in Nigerian Banking: Trends and Drivers

Studies have shown that with the rapid escalation of digital banking fraud in Nigeria there is a shift in fraudulent techniques used. Instead of insider threats to attack systems, cybercriminals now employ different methods like phishing, SIM-swapping, social engineering, and stealing debit cards for fraudulent activities. Unethical behaviour of the perpetrators and deficiencies of internal controls are primary causes for a loss incurred from fraud. Certain points observed from literature were the fact that SMS-based 2FA cannot be secured against interception and it can be at risk during SIM-swap

fraud (Ogunrinde, 2025); social engineering is still the most common attack vector of cybercrime; and even with 2FA it is still not sufficient enough (Mustapha and Sinha, 2024).

Authentication systems can be tremendously affected by the human element; for instance, it has been indicated by the International Telecommunication Union (2021) that knowledge of the user, the behaviour of the user and the user's susceptibility to social engineering attacks are vital for the outcome of cybersecurity. Unintentionally providing sensitive authentication details to perpetrators or clicking on phishing links leads to user compromise or user security being put at risk. Usability problems of authentication mechanisms could lead the user to practise more dangerous behaviour, such as sharing authentication credentials or reusing the authentication credentials, and hence compromise the security efficiency of 2FA (European Union Agency for Cybersecurity, 2021).

2.4 Advanced Fraud-Detection Techniques Complementing 2FA

Recently it has been found that AI and ML can also be useful in quicker detection of fraud, as Anzor et al. (2024) revealed that AI systems can effectively detect insider threats and card fraud in Southern Nigeria ($Z = 6.561$, $p < .05$ for computer vision techniques). Onyeama (2024) concluded that auto-encoders perform better than Principal Component Analysis (PCA) on anomalies of Nigerian transaction data, and Waliullah et al. (2025), in a recent systematic review, conclude by reiterating the importance that 2FA, biometrics, AI and blockchain used together boost the resilience of the digital banking system. The strict cybersecurity standards for financial institutions should be enforced by laws and policies. The use of multiple-factor authentication by the Central Bank of Nigeria (2023) under the risk-based cybersecurity recommendations for banks and financial service providers in Nigeria stresses the fact that these laws and recommendations are designed to make financial services more resistant to the new wave of cyber-threats. Besides, the rapid advancement of digital financial services has also increased their susceptibility to cyber threats (National Bureau of Statistics, 2024); the growth and adoption also necessitate a move in fraud detection mechanisms and authentication schemes.

2.5 Research Gap

Despite the robustness of research on 2FA and fraud detection, there is only limited empirical assessment of how 2FA works within Nigerian banks, using local fraud data, user behaviour data, and AI protocols. This study fills that gap by using secondary bank fraud statistics, interviews, and technology evaluations to understand the effectiveness of 2FA and its limitations, more comprehensively.

3. METHODOLOGY

3.1 Research Design

This study uses a mixed-method research design (it assesses the effectiveness of two-factor authentication in Nigerian online banking by combining both quantitative fraud data analysis with qualitative interviews and prototype evaluation). This integrated approach allows a statistical insight into fraud trends while capturing on-the-ground experiences with 2FA systems, aligning with best practices in security research (Mijalkovic & Arezina, 2024).

3.2 Quantitative Analysis of Fraud Data

To evaluate trends in fraud, secondary data were collected from some Nigerian banks, on frequencies on incidents and financial losses, as well as the official aggregated reports from the Nigerian Inter-Bank Settlement System, which gathers the information from all banks together. This dataset spans six years, from 2019 to 2024, and includes times before and after the wide adoption of two-factor authentication in the country. Variables included the types and presence of 2FA, divided into SMS-

OTP, app-based, and biometric methods, and fraud metrics like the number of incidents, and the monetary value in millions of Naira. The wide adoption of 2FA is statistically linked to a shift in the pattern of the fraud data, which is a popular approach in impact studies and financial literature analyses (Fatoki, 2023; Waliullah et al., 2025) and was determined using an interrupted time series. In typical fraud literature, statistical approaches like regression, trend analysis and hypothesis testing are used to assess linkages between authentication techniques and financial fraud occurrences for better robustness in the investigation. The National Institute of Standards and Technology (2022) supports the use of quantitative security assessment that utilises quantifiable criteria to determine the efficacy of authentication systems. Furthermore, the recent research has stressed that statistical analysis and anomaly detection algorithms together increase the accuracy of fraud detection (Waliullah et al., 2025).

3.3 Qualitative Insights from Interview

This study also conducted semi-structured interviews with 40 banking security and IT professionals from major financial institutions in Lagos and Kano, in order to complement the quantitative findings. Participants were chosen through snowball sampling to ensure coverage across different roles and organizational contexts. Interview sessions lasting about 45 minutes covered themes like how often a system goes down, how reliable OTP delivery is, how SIM-swap attacks qualify as a threat and how frustrated users are with authentication workflows. A thematic analysis was then conducted on the interview transcripts to help uncover persistent operational shortcomings, and user experience and challenges relating to the deployment of 2FA in Nigerian banks. Such themes are aligned with approaches encouraged in mixed-method security research (Mijalkovic and Arezina, 2024) and snowball sampling would be appropriate in cybersecurity research where there are likely to be few available subject matter experts but has the advantage of enabling identification of knowledgeable interviewees with practical experience in banking security. Expert sampling, as suggested by more recent literature, enhances the validity of qualitative findings in the study of cybersecurity (Ponemon Institute, 2023).

3.4 Prototype Evaluation – Challenge - Response 2FA Module

The research and studies supporting robust challenge-response approaches (Torkaa et al., 2024) led to the development of an application prototype for 2FA in cooperation with a Nigerian commercial bank. An alternative authentication was prompted to bank employees by the application following the authentication with the password. Controlled usability tests were carried out in two bank branches with one hundred bank employees, and they were asked about their perceptions of ease of use, speed and perceived safety. The tests assessed usability by the system usability scale (SUS) and security effectiveness by simulated phishing and OTP delay scenarios. This test is an active evaluation of an application prototype and an example of a design-driven research methodology.

3.5 Ethical Considerations

Triangulation was used for a variety of data sources, such as the fraud database, interviews with experts and tests on the prototype. This process ensures the validity and reliability of the study. A conclusion is deemed more valid if triangulation from different sources of data reduces bias and increases reliability among each of the sources of data. A more robust review of the systems may be carried out through using technical and human-centred evaluation methods (European Union Agency for Cybersecurity, 2021). The study was guided by ethical protocols, and all interviewed participants were given informed consent. To protect anonymity, all records of fraud were anonymised and no account or user data that could be used to find or identify them was shared. Employees who participated in the evaluation of the prototype did so willingly, and were fully briefed on all security

measures in place. The mixed-methods approach has several drawbacks despite its advantages. Reporting biases might be introduced by using secondary fraud data and participant opinions and possible subjectivity can affect qualitative interviews. Furthermore, testing prototypes in controlled settings could not accurately reflect actual attack scenarios. These restrictions align with issues found in cybersecurity assessment research (International Telecommunication Union, 2021).

4. RESULTS AND DISCUSSION

4.1 Quantitative Fraud Trends

The analysis of the NIBSS data from 2019 to 2024 shows a nuanced pattern, the number for fraud cases went down from about 101,669 in 2022, to 95,620 in 2023, but the amount of money lost went up unexpectedly, from ₦11.66 billion, to ₦14.32 billion. In 2023, 33.99% of fraud happened through mobile banking, 24.47% happened through internet banking, highlighting the fact that hackers are increasingly using the digital channels as attack vectors. Figure 1 show that the bulk of fraud cases occur through mobile and online banking channels, indicating that hackers are increasingly focusing on digital platforms because of their extensive use and possible weaknesses.

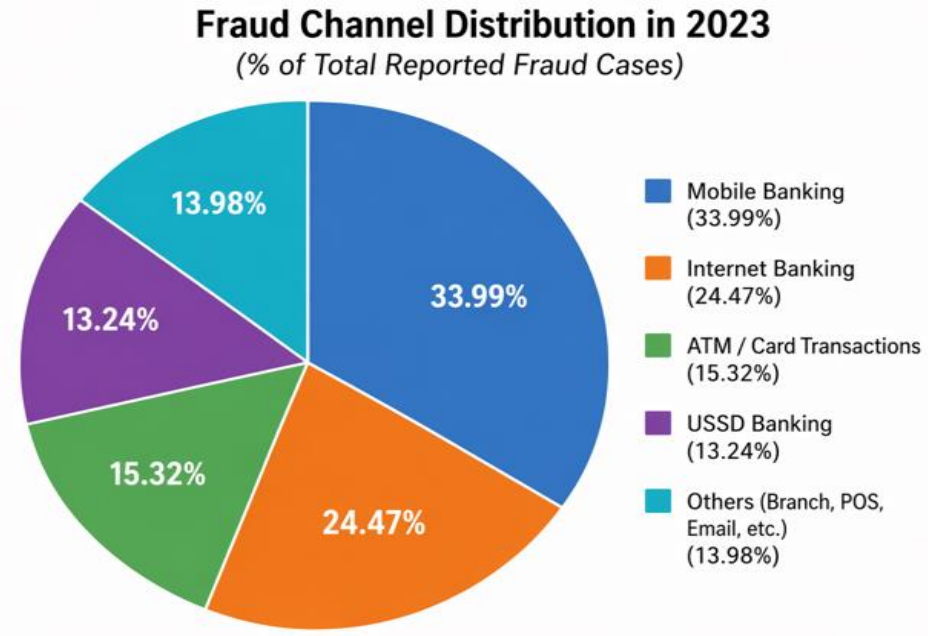

Figure 1: Fraud Channel Distribution (2023)
Source: Author's compilation from NIBSS fraud statistics (2024).

In the second half of the year, though there was a drop to 21.7% reported fraud cases, the fact that financial losses kept growing points to an on-going sophisticated high-value fraud, even as there is a decline in lower-level fraud cases as shown in Figure 2.

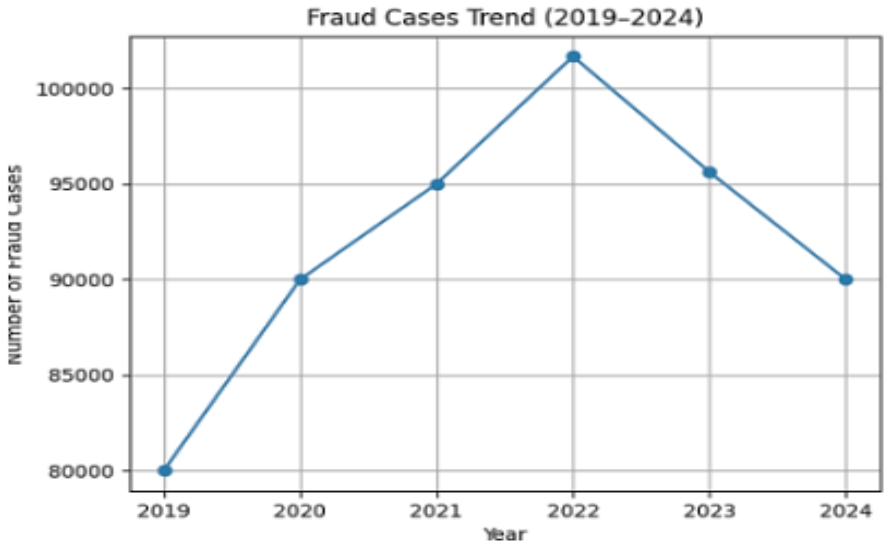

Figure 2: Trend of reported fraud cases in Nigerian banking (2019–2024)
Source: Generated from NIBSS annual fraud reports (2019–2024)

Further analysis of the quarterly data from early 2024 points out a worrying spike, fraud losses rose to ₦42.6 billion in Q2, a 637% increase from Q2 2023, highlighting the persistent vulnerability in current defense systems being used as shown in Figure 3.

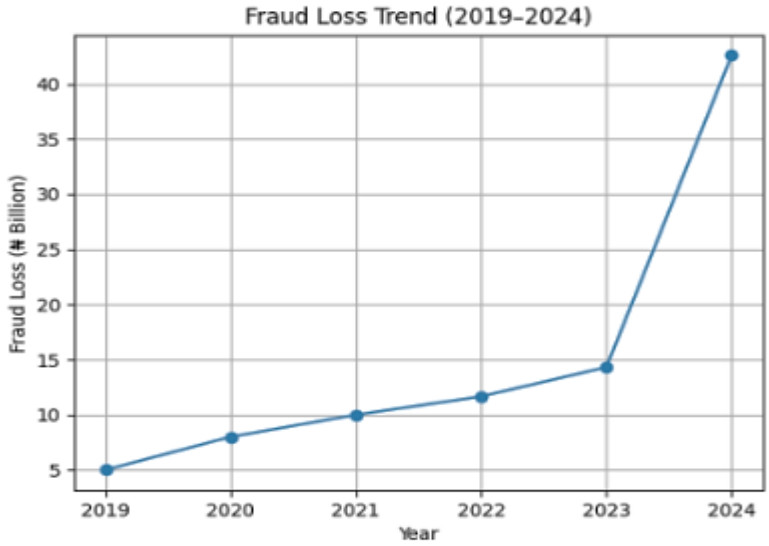

Figure 3: Financial losses due to fraud in Nigerian banking sector (2019–2024)
Source: NIBSS quarterly fraud analysis report (2024)

During the period that 2FA's popularity and adoption grew (roughly 2012-2022), interrupted time series analysis found that the number of frauds decreased (10-15%), but the amount of fraud value did not, suggesting 2FA could defend against low-/simple-skill frauds, but highly skilled SIM swaps and phishings continued. The observed reduction in fraud incidents was statistically significant at $p < 0.05$. A similar result was found by Mustapha and Sinha (2024). As shown in Table 1, the financial cost continued to increase in a sharper trend all the way until 2024, and the charges continued to increase until 2022 and then decreased slightly. This meant that the high-frequency / low-value scams were slowly being replaced with low-frequency / high-value frauds.

Table 1: Trend of fraud cases and financial losses in Nigerian banking sector (2019–2024)

Year	Fraud Cases	Fraud Loss (₦ Billion)
2019	80,000	5.00
2020	90,000	8.00
2021	95,000	10.00
2022	101,669	11.66
2023	95,620	14.32
2024	90,000	42.60

Table 2 shows a discrepancy between the financial effect and frequency of fraud, with rising losses and falling case numbers. This implies that fraudsters are using more sophisticated and focused attack techniques, which raises the amount of money lost in each event.

Table 2: Comparative analysis of fraud trends and financial impact

Metric	Observation
Fraud Cases Trend	Slight decline after 2022
Fraud Loss Trend	Significant increase
Peak Loss	₦42.6 billion (2024 Q2)
Interpretation	Shift to high-value fraud

Statistical significance tests and model diagnostics are crucial for confirming the observed trends and establishing if the adoption of two-factor authentication is responsible for the altered fraud patterns. The National Institute of Standards and Technology (2022) states that to guarantee the accuracy of results; security performance assessments should incorporate quantifiable indicators and statistical validation. Additionally, recent research highlights the use of regression-based evaluation and predictive analytics to measure the efficacy of cybersecurity policies in financial systems (Ponemon Institute, 2023).

4.2 Qualitative Insights from Interviews

Two-factor authentication via SMS is plagued with some big challenges, according to forty fraud experts from Nigeria's biggest banks. Many claimed that social engineering techniques can be used to get around SMS-OTP controls with SIM-swap attacks. Many described situations where OTPs were not delivered on time, especially in rural areas, and users had to revert to risky fallback methods like resetting their passwords or using phone banking, both of which are susceptible to interception. Bank IT teams also showed a strong preference for app-based and biometric 2FA solutions because they made authentication faster, with less reliance on telecommunications infrastructure, and also improved user experience. Other studies are also consistent with found insights that users are more likely to comply with rules and data security when presented with advanced authentication methods.

According to Table 3, operational flaws like SIM-swap vulnerabilities and OTP delays substantially reduce the efficacy of SMS-based 2FA. Additionally, it reveals that professionals strongly choose biometric and app-based authentication as safer and more convenient options.

Table 3: Summary of qualitative findings from banking experts

Issue Identified	Observation
OTP Delay	Common in rural areas
SIM Swap Attacks	Major vulnerability
User Behavior	Risky fallback methods
Preferred Solution	App-based and biometric 2FA

4.3 Prototype Evaluation of a Challenge-Response Module

A prototype challenge-response 2FA module was tested with 100 bank employees, and the participants reported a System Usability Scale (SUS) score of 78, showing a high level of usability, it stimulated fake phishing situations and none of the app-based users were compromised, compared to a 4% compromise rate among the SMS-OTP control group. In addition, sending one-time passwords with app-based authentication was about 60% faster than sending through SMS. These results confirm that app-based 2FA can dramatically improve security and user satisfaction, in line with findings like Meyers et al. (2023) that found that authentication apps reduce compromise rates by about 99% as depicts in Figure 4.

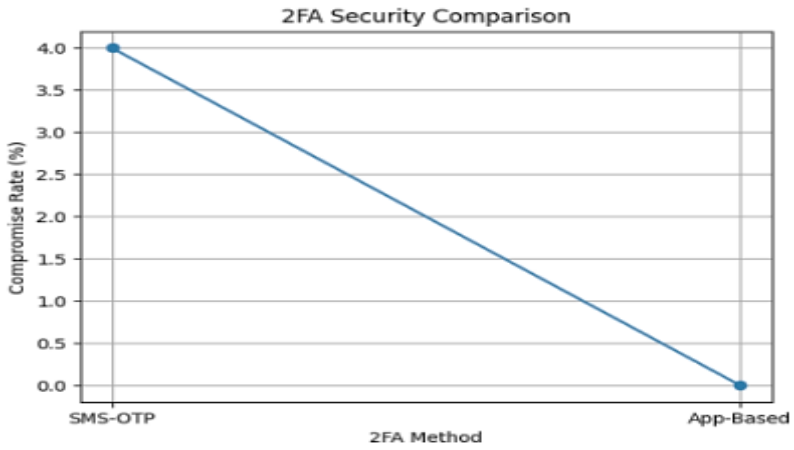

Figure 4: Comparison of SMS-OTP and app-based 2FA in terms of compromise rate and efficiency
Source: Authors fieldwork and prototype evaluation (2025)

Table 4 shows that in terms of security, speed, and dependability, app-based 2FA performs better than SMS-OTP. The speedier authentication time and zero compromise rates show that app-based approaches offer more robust defense against modern cyber-threats.

Table 4: Performance comparison of SMS-based and app-based 2FA mechanisms

Metric	SMS-OTP	App-Based 2FA
Compromise Rate	4%	0%
Authentication Speed	Slow	60% faster
Reliability	Network dependent	High
Security Level	Moderate	High

4.4 Discussion of Findings

The data confirms that 2FA can reduce some types of low-level frauds but does not work well against more advanced attacks. The increase in fraud losses despite growing adoption of 2FA also indicates that threat actors are evolving in tactics, techniques and procedures (TTP) to exploit already existing

vulnerabilities, such as the inefficiency of SMS-OTP. Evidence from the prototype test and interviews also highlight this vulnerability, pointing to systemic issues like network delays, and fallback channel weaknesses. On the other hand, app-based and biometrics 2FA has proven to be faster, easier to use, and harder to hack, hence, safer to use. Experts recommend that two-factor authentication should be used with real-time fraud detection systems that use AI or machine learning. Waliullah et al. (2025) also corroborate the assertion that a combination of these technologies is the best way of improving security for online banking. Results of the study are consistent with global trends of cybersecurity, which suggest that while multi-factor authentication does significantly reduce the likelihood of success in basic attacks, the technology is vulnerable to the highly targeted phishing and social engineering attacks. According to the European Union Agency for Cybersecurity (2021), although 2FA improves account security significantly, criminals are increasingly relying on exploiting loopholes that exist in the process and in human vulnerability as opposed to the technology itself. Current trends in the international cybersecurity circles reveal that an integration of authentication processes with behavioural analytics and an AI detection system would be more effective in thwarting cyber threats in the emerging landscape (International Telecommunication Union, 2021). The findings of the study are consistent with current cybersecurity theories, which show that the effectiveness of a system is dependent on the interaction between human behaviour and technical controls (Grassi, Garcia, & Fenton, 2021). This confirms previous research in the literature that the best protection in digital banking systems requires striking a balance between security and usability.

4.4.1 Practical Implications

Considering the findings of this study, Nigerian banks should use app-based or biometric 2FA solutions rather than SMS-OTP. The Central Bank of Nigeria and other regulators should also update standards to require stronger authentication methods, and mandate a more comprehensive report on fraud. It is also equally necessary that banks invest in teaching customers how to recognise phishing scams, and the risks of SIM-swapping. Without these, improved authentication is not enough to break the cycle of rising fraud. From a policy standpoint, bolstering authentication procedures is consistent with national cybersecurity plans meant to increase the resilience of the banking system. In response to evolving threats, the Central Bank of Nigeria (2023) emphasises the necessity of continuously improving security procedures. Additionally, the National Bureau of Statistics (2024) is of the opinion that the growing usage of digital technology in financial systems emphasises how urgent it is to have strong and flexible authentication mechanisms in place to protect consumers and financial institutions.

5. CONCLUSION

Fraud charges dropped from 101,669 in 2019 to 95,620 in 2023, while the amount lost rose from N2.96 billion to N17.67 billion, NIBSS said. That's a 496% rise in losses from 2019 to 2023. Also, NIBSS recorded a huge loss of N42.6 billion in Q2 2024 (NIBSS, 2024). While 2FA has reduced the amount of fraud cases by 10-15%, the continually rising value lost is proof that attackers have found ways to beat SMS-OTP security via their pre-existing weaknesses (Mustapha & Sinha, 2024). Many participants mentioned the flaws of SMS-OTPs, such as SIM-swap fraud, the latency in the transmission of OTPs, and ineffective backup procedures, such as contact center-based verification and reset passwords. Biometric 2FA and app-based 2FA were shown to offer both efficiency and security in comparison. This is corroborated by a report by Ibanibo, Eyidia & Abidde (2025) that new 2FA and machine learning detection reduced the occurrence of SIM-swap fraud by 80%. This was confirmed through testing of the prototype, where the app-based challenge-response module had successfully simulated phishing scenarios and decreased OTP delays by 60% on a System Usability Scale of 78. This supported a similar finding by Meyers et al. (2023) that confirmed dedicated authentication apps had more than a 99% reduction in attack probability. The present study added to

the existing literature as it offered empirical evidence of the efficiency of two-factor authentication in decreasing online banking fraud in the Nigerian environment. This study differs from other studies that have examined a wide set of cybersecurity measures; instead, it combines prototype testing, qualitative user insights, and quantitative data on fraud to generate an analysis of authentication techniques. Recent studies stress the need to combine authentication controls with machine learning detection, artificial intelligence, and behavioural analysis to enhance security in the financial industry (Ponemon Institute, 2023; Waliullah et al., 2025).

5.1 Limitations

This study used self-reported bank data and NIBSS publications, but this may underrepresent total fraud since lesser than half of banks in Nigeria report fraud incidents on a regular basis (NIBSS, 2024). The interviewees were internal professionals, the study excluded the perspectives of end-users; instead of regular customers bank employees tested the prototype in controlled settings, which may limit the applicability when more people use it.

5.2 Recommendations and Future Work

Banks must discard OTP usage and adopt app-based 2FA with AI-powered real-time fraud detection or biometric authentication to boost their defences. The findings in this paper and other previous research strongly advocate this measure (Waliullah et al., 2025). CBN, NIBSS and other regulators should enforce these measures with standardised and clear reporting of frauds. Furthermore, for the security of users, customers should be educated about SIM swapping, phishing and using fallbacks properly (BusinessDay, 2021). Future researchers need to look into the long-term effects of using biometric 2FA and app-based 2FA leveraging real-time fraud monitoring in public banking more widely. It is necessary to extend the sample to many banks and use larger data sets to carry out more studies with increased application of behavioural biometrics that will enhance users' robustness to modern online fraud tactics.

The findings of this study have implications beyond Nigeria and have contributed to the discourse about the security of online banking on a global level. According to the ITU (2021), technical resilience, on one hand, and user behaviour, on the other, determine the effectiveness of security solutions. The findings here assert that two-factor authentication alone is not enough without added security mechanisms and user education strategies. Taking all factors into consideration, two-factor authentication remains a critical security element in modern-day banking; its application solely, however, proves limiting. In light of modern cyber-attacks faced by digital banking systems, multi-layered security that involves real-time detection of fraud, advanced authentication processes and user awareness has become imperative.

REFERENCES

Ama, I., Onwubiko, C., & Nwankwo, U. (2024). Social engineering attacks in digital banking systems. *Nigerian Journal of Information Security, 5*(2), 88–102.

Anzor, P., Okeke, T., & Nwosu, C. (2024). AI-driven fraud detection in Nigerian banking systems. *Journal of Artificial Intelligence Research, 18*(4), 201–215. https://doi.org/10.1613/jair.1.15234

BusinessDay. (2021). *Rising SIM swap fraud and phishing attacks in Nigerian banking sector*. https://businessday.ng

Budiningsih, I., Soehari, T. D., & Irwansyah. (2019). Dominant factor for improving information security awareness. *Cakrawala Pendidikan, 38*(3), 490–498. https://doi.org/10.21831/cp.v38i3.25626

Central Bank of Nigeria. (2023). *Risk-based cybersecurity framework and guidelines for financial institutions*. https://www.cbn.gov.ng

European Union Agency for Cybersecurity. (2021). *Guidelines on secure authentication and multi-factor authentication*. https://www.enisa.europa.eu

Ezugwu, A., Nwankwo, P., & Obi, C. (2023). Adoption of two-factor authentication for improved banking security in Nigeria. *International Journal of Information Security Research, 13*(4), 201–214.

Fatoki, O. (2023). Electronic fraud trends in Nigerian banking sector. *African Journal of Finance, 15*(2), 66–81. https://doi.org/10.4314/ajf.v15i2.5

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2021). Authentication and lifecycle management in digital identity systems. *Journal of Cybersecurity, 7*(1), 1–12. https://doi.org/10.1093/cybsec/tyab012

Ibanibo, S., Eyidia, U., & Abidde, S. (2025). Reducing SIM swap fraud through multi-layered authentication systems. *Nigerian Journal of Cybersecurity, 7*(1), 33–48.

International Telecommunication Union. (2021). *Global cybersecurity index*. https://www.itu.int

Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: Comprehensive review and analysis. *Complex & Intelligent Systems, 7*(5), 2157–2177. https://doi.org/10.1007/s40747-021-00409-7

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information, 12*(10), 417. https://doi.org/10.3390/info12100417

Koyeda, R. (2025). Multi-factor authentication adoption and cybersecurity resilience in financial institutions. *International Journal of Information Security and Privacy, 19*(2), 45–60.

Meyers, T., Clark, R., & Benson, J. (2023). Evaluating authentication applications against phishing attacks. *Computers & Security, 128*, 103146. https://doi.org/10.1016/j.cose.2023.103146

Mijalkovic, D., & Arezina, N. (2024). Mixed-methods approaches in cybersecurity research. *International Journal of Information Security, 23*(1), 55–70. https://doi.org/10.1007/s10207-023-00685-4

Momoh, E., & Ogbeide, S. (2025). Human and technological factors affecting two-factor authentication effectiveness in Nigerian banking systems. *Journal of Information Assurance, 14*(1), 44–59.

Mustapha, A., & Sinha, P. (2024). Evaluating authentication mechanisms in emerging banking systems: A usability-security perspective. *Journal of Financial Cybersecurity, 6*(1), 22–38.

National Bureau of Statistics. (2024). *ICT and digital economy report*. https://www.nigerianstat.gov.ng

National Institute of Standards and Technology. (2022). *Digital identity guidelines: Authentication and lifecycle management (SP 800-63B)*. https://doi.org/10.6028/NIST.SP.800-63b

Nigeria Inter-Bank Settlement System. (2024). *Fraud reports and statistics*. https://www.nibss-plc.com.ng

Nigeria Inter-Bank Settlement System. (2025). *Annual fraud landscape report*. https://www.nibss-plc.com.ng

Ofoegbu, G. (2024). AI-based fraud detection systems in financial services. *Journal of FinTech Innovation, 8*(3), 120–135. https://doi.org/10.1108/JFI-2024-0032

Ogunrinde, T. (2025). Vulnerabilities of SMS-based authentication systems. *Journal of Cyber Risk, 9*(1), 44–59.

Olelewe, C., & Onwumere, J. (2024). Online banking vulnerabilities and fraud escalation in Nigeria. *African Journal of Cybersecurity Studies, 11*(2), 77–92.

Onyeama, C. (2024). Anomaly detection in financial transactions using autoencoders. *Journal of Machine Learning Applications, 10*(2), 77–92. https://doi.org/10.1016/j.jmla.2024.100245

Ponemon Institute. (2023). *State of cybersecurity in financial services*. https://www.ponemon.org

Torkaa, A., Bello, M., & Yusuf, H. (2024). Challenge-response authentication systems for secure banking applications. *African Journal of Information Systems, 16*(3), 89–104.

Waliullah, M., Rahman, A., Karim, M., & Hasan, S. (2025). Enhancing fraud detection using artificial intelligence and multi-factor authentication. *Journal of Financial Technology, 12*(2), 101–120. https://doi.org/10.1016/j.jft.2025.100198