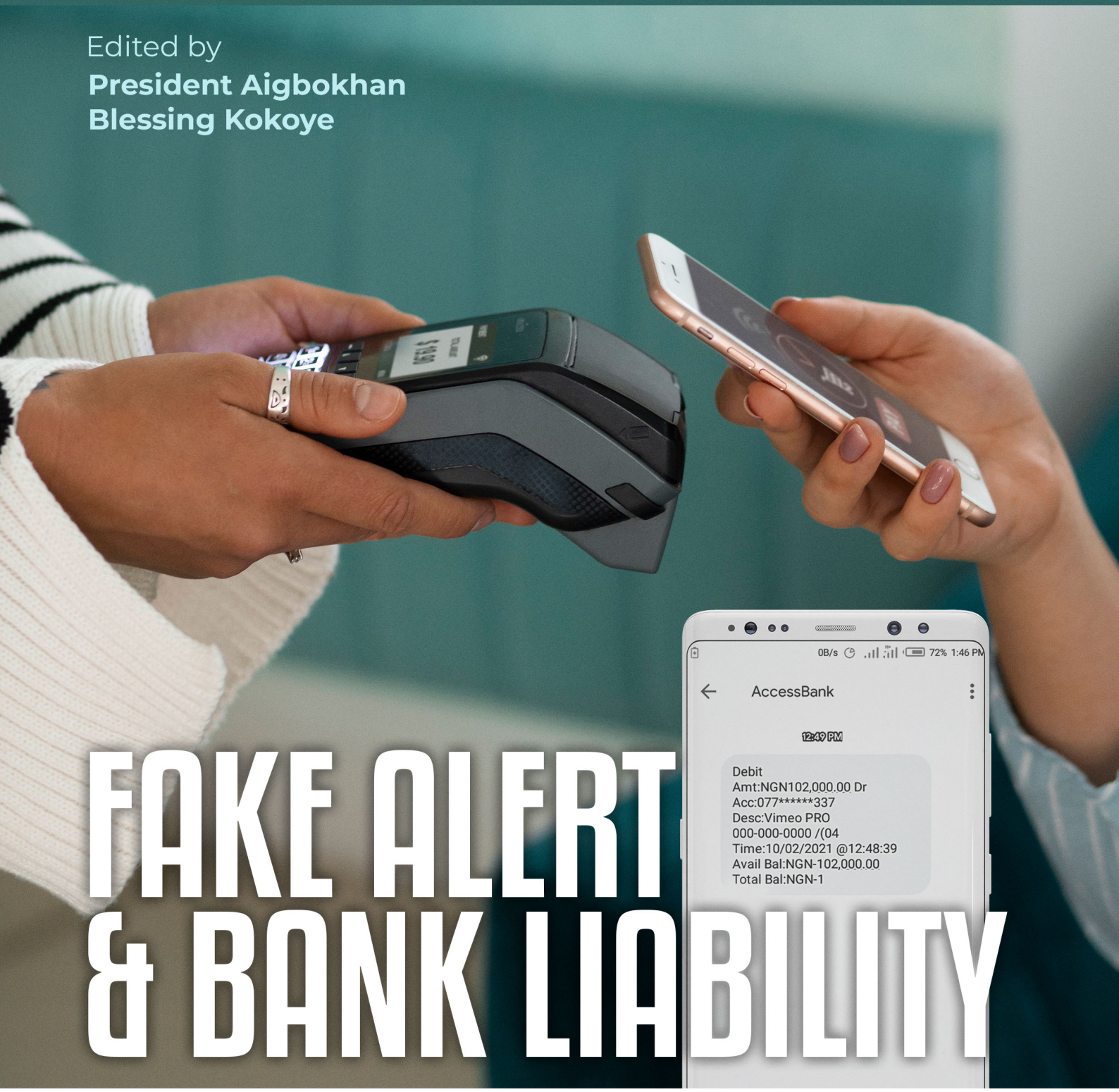
THE PRESIDENT'S NEWSLETTER

Vol. 3 No. 2, 2024

Edited by
President Aigbokhan
Blessing Kokoye



FAKE ALERT & BANK LIABILITY

FOI COUNSEL RUDILAC Rural Development, Information And Legal Advocacy Centre

A PUBLICATION OF FREEDOM OF INFORMATION COUNSEL AND RURAL DEVELOPMENT, INFORMATION AND LEGAL AID CENTER (RUDILAC)

Table of Contents

Editorial Team

Editor-in-Chief
President Aigbokhan

Deputy Editors
Robinson Otuakhena, Esq.
Eunice Uchechukwu
Kokoye Blessing Ifedayo
Nwaogwugwu Rosemary

Publication Design & Layout
Kelvin Odemero

Introduction

In the digital era, the widespread occurrence of fake alerts significantly impacts both consumers and financial institutions. These deceptive communications, often posing as harmless emails, SMS messages, or phone calls, are designed to trick recipients. Similar to opening Pandora's Box, these scams can result in unauthorized transactions, identity theft, and considerable financial losses. Fake alerts typically involve sending money to a bank account from which the recipient cannot withdraw funds. This practice, known as alert flashing, uses SMS to mimic a bank's transaction alert to deceive unsuspecting victims. It also encompasses unsolicited or promotional messages from banks and other financial institutions. A bank bears the legal and financial responsibility if a customer falls victim to fraudulent activities by third parties or dishonest staff. The bank's liability is influenced by factors such as its failure to implement adequate security measures to protect customer accounts.

Legal Framework and Bank Liability

Fake alerts, often caused by technical errors or AI malfunctions, can lead to significant frustration for customers, resulting in unnecessary concern and operational disruptions. This issue affects both banks and other financial institutions. Sending fake alerts is a criminal offense, punishable by law, as it involves various forms of fraud and cybercrime that are illegal in Nigeria.

The Bank and Other Financial Institutions Act (BOFIA) outlines penalties and enforcement mechanisms for financial institutions and individuals who fail to adhere to its provisions, including those related to cybersecurity breaches and fraud. While the Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers provide comprehensive measures to prevent and mitigate cybersecurity risks, they often lack specific provisions for directly sanctioning offenders involved in cybersecurity threats. Consumers of financial services have the option to pursue legal action by filing a civil suit or making a criminal complaint. They can seek fines or imprisonment through the High Court or the Federal Competition and Consumer Protection Commission

The Nigeria Inter-Bank Settlement System PLC (NIBSS) is a shared-service e-payment infrastructure company that facilitates electronic payments within the Nigerian financial sector. As an industry-owned entity, NIBSS develops and manages the infrastructure for transactions between banks across Nigeria. The organization is owned by all licensed banks, discount houses, and the Central Bank of Nigeria (CBN). NIBSS operates by accessing customer account reports and ensuring that banks transmit financial transaction data through secure online networks. This process aligns with the regulations set for the Nigerian financial sector, as outlined in the company's Memorandum and Articles of Association. NIBSS provides the infrastructure for the automated processing, settlement, and transfer of

payment instructions between banks, discount houses, and card companies in Nigeria. Its mandate includes enabling same-day clearing and settlement of inter-bank transfers and payments. The company is responsible for ensuring efficient automated processing and settlement of transactions related to deposit placements and fund transfers between banks.

In 2010, the Nigerian government introduced a cashless policy aimed at reducing the volume of cash in circulation and curbing the excesses associated with cash handling. However, this policy inadvertently led to the emergence of fraudulent bank applications designed to exploit the system. These apps, which often disguise themselves as legitimate financial tools, have become a significant problem by facilitating fake alerts and fraudulent activities. Fraudsters behind these apps only require minimal customer details to carry out their schemes. Some of the fraudulent applications known for generating fake alerts include, but are not limited to, Flash Fund Apps, Lofty SMSs App, Money Prank App, Millionaire Fake Bank Account, and Fake Alert Makers for Android. These apps are specifically designed to deceive users into believing they have received financial notifications or transactions that are entirely fictitious, thereby exploiting their trust and personal information for fraudulent purposes.

The Role of Technology and AI in Banking

With the growing dependence on AI, algorithms, and advanced systems, banks are seeing significant improvements across various aspects of their operations. For example, customer service is increasingly handled by AI-powered chatbots, which offer 24/7 support. Routine tasks, such as processing transactions and managing accounts, are now automated, minimizing the need for manual intervention and enhancing overall efficiency. Established in 1993, NIBSS plays a crucial role in standardizing technical and operational practices across the financial system. The system utilizes advanced algorithms to enable real-time settlement of interbank transfers, greatly reducing the time required for funds to be transferred between banks. The BVN (Bank Verification Number) system, supported by NIBSS, uses biometric data and AI to verify each customer's identity across the banking sector, thereby reducing fraud and enhancing security. However, a downside is that AI systems can occasionally misclassify legitimate transactions as suspicious, leading to false alerts, and vice versa. Technical glitches or system downtimes in AI processing are key factors contributing to the occurrence of fake alerts. On August 2, 2014, the National Information Technology Development Agency (NITDA) National Center for Artificial Intelligence (NCAIR) released a draft of the National Artificial Intelligence (AI) Strategy 2024. This draft outlines risk mitigation strategies for AI, focusing on issues such as accuracy, bias, transparency, and governance. Its goal is to strengthen privacy rights, prevent discrimination, ensure algorithmic accountability, and enhance data protection.

A key piece of legislation in Nigeria is the Banks and Other Financial Institutions Act (BOFIA) 2020, which regulates the operations of banks and other financial institutions in the country. Although BOFIA 2020 may have limitations in fully protecting consumers from cyber-related crimes, it addresses important issues related to the operational standards and liabilities

of financial institutions. For instance, Section 12(1) of the Act allows the governor to revoke the banking license of any institution that poses a threat to financial stability, which could result from infrastructural deficiencies. This emphasizes the need for banks to adhere to operational standards and prudential requirements to ensure soundness and stability, avoiding situations that could compromise consumer protection and increase exposure to cybercrime. Similarly, Section 66(1) of BOFIA mandates that all banks and financial institutions implement policies to prevent transactions that could facilitate criminal activities, money laundering, or terrorism. In response to the increasing frequency of cybersecurity threats such as ransomware, targeted phishing attacks, and Advanced Persistent Threats (APTs), the Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks (DMBs) and Payment Service Providers (PSPs) were issued by the Central Bank of Nigeria (CBN) and became effective in 2019. These guidelines aim to strengthen the cybersecurity programs of financial institutions by adopting a risk-based approach to managing cybersecurity risks, thereby enhancing their overall cybersecurity posture

Sections 2(d) and 2(f) of the Central Bank of Nigeria (CBN) Act, 2007, played a crucial role in initiating the development of a Consumer Protection Framework (CPF). This framework is designed to safeguard consumer rights by ensuring that financial institutions maintain a secure and supportive banking environment, offer reliable channels and platforms for transactions, and provide efficient mechanisms for addressing claims or disputes. These provisions collectively underscore that banks in Nigeria are legally and regulatory obligated to uphold a high standard of consumer protection. Specifically, Section 2(d) mandates that financial institutions must create and maintain a safe banking environment, ensuring that their operational practices do not pose risks to consumer safety. Meanwhile, Section 2(f) requires the establishment of effective redress mechanisms, allowing consumers to resolve complaints and disputes in a timely and satisfactory manner. These regulations collectively emphasize the responsibility of banks to protect consumer interests and provide avenues for redress, reinforcing their commitment to maintaining trust and ensuring fair treatment of their customers. As such, financial institutions are held to rigorous standards, ensuring they meet legal obligations and deliver a high level of service and protection to consumers.

In the early 2010s, Nigerian banks began to explore AI technologies, initially focusing on automating routine tasks and improving customer service. Over time, the role of AI within banking operations expanded. Banks started utilizing AI for credit scoring, risk management, and providing personalized customer services. By early 2020, AI technologies had become a crucial component of banks' strategic operations in Nigeria. Machine learning algorithms were used to enhance credit risk assessments, forecast market trends, and deliver tailored financial products. Banks also began partnering with fintech companies, employing advanced AI solutions to improve their digital offerings and increase financial inclusion. Despite these advancements, there remains a lack of clear regulation addressing damages resulting from system glitches in AI-directed operations. This gap highlights the need for regulations to mitigate the risks and liabilities associated with AI technologies in the banking sector.

Recently, the functioning of algorithms used by banks and financial institutions has become increasingly opaque and difficult to review. This lack of transparency has led to erroneous, arbitrary, and unfair outcomes, such as situations where customers are debited without the corresponding funds being credited to the recipient bank. Despite significant investments in infrastructure and charges associated with automated processing and settlement of financial transactions, these issues have resulted in numerous failed transactions.

Banks have a crucial responsibility to oversee their technology and ensure that advancements in banking automation adhere to core values such as truthfulness, transparency, accountability, privacy, and security. They must protect customers' funds in their custody and are liable for any losses arising from unauthorized or fraudulent transactions. Given that banks charge for both operational and credit risk in cases of failed and successful funds transfers, as well as unauthorized debits, they must demonstrate due care, skill, and adequate infrastructure in managing customer accounts. The bank's duty includes ensuring that its systems are robust and reliable, and can effectively address any issues that arise. This responsibility extends to maintaining high standards of operational integrity and ensuring that technological advancements align with their commitment to safeguarding customer interests.

In the United States, the Electronic Fund Transfer Act (EFTA) was enacted in 1978 to address the shift from physical checks to electronic monetary transfers. The Act was introduced to build trust and predictability for consumers using electronic payment methods, particularly in situations involving errors or fraud. It mandates that financial institutions allow consumers to dispute incorrect financial statements and outlines procedures for resolving disputes between consumers and institutions. The EFTA is a federal law designed to protect consumers engaging in electronic money transfers. It sets forth guidelines for correcting errors and limits liability for unauthorized transactions. The Act covers various types of transfers, including ATM withdrawals, direct deposits, and online payments, with the aim of enhancing transparency and security in electronic financial transactions.

It establishes specific timeframes for consumers to report issues such as incorrect amounts, unauthorized transfers, or missing transactions. Financial institutions are required to investigate these errors and correct them within a designated period. If the investigation extends beyond the standard timeframe, provisional credit must be provided to the consumer's account. The EFTA ensures that banks are held accountable for resolving these issues and specifies their liability in cases of non-compliance or errors.

Challenges, Consumer Protection, and Recommendations

Despite the presence of frameworks such as the Banks and Other Financial Institutions Act (BOFIA) and various consumer protection laws designed to safeguard financial consumers, there remains a significant gap in addressing issues related to fake alerts and fraudulent transactions originating from automated banking systems. Legal precedents have shown that banks can be held accountable for errors and inaccuracies in their financial systems. For

example, numerous court rulings have established that banks are responsible for correcting unauthorized transactions. These cases highlight the need for banks to ensure the accuracy and reliability of their automated systems to avoid legal consequences and maintain customer trust. However, current Nigerian consumer protection laws do not specifically address the problem of fake alerts resulting from automated systems.

This regulatory gap leaves consumers exposed to the negative impacts of such errors without clear avenues for recourse. In contrast, the U.S. Electronic Fund Transfer Act (EFTA) offers explicit provisions for holding banks accountable for errors, including those caused by system glitches and fraudulent transactions. The EFTA establishes procedures for reporting errors, resolving disputes, and protecting consumer rights, providing a more comprehensive framework for defending customers against the impacts of fake alerts. To reduce customer frustration and improve consumer protection, the Nigerian government should consider adopting similar legislation to address these issues more effectively.

Public dissatisfaction with banks and financial institutions has surged, with daily customer feedback on social media highlighting increasingly erratic digital services from these institutions. This issue primarily stems from inadequate investment in technology infrastructure, leading to the lack of an efficient digital portal for handling high volumes of electronic transactions and resulting in faulty application programming interfaces (APIs) due to customer traffic. To address these problems, banks must upgrade their technology infrastructure and security measures to facilitate seamless payment and settlement of financial transactions.

Additionally, they should integrate ethical principles into the design, implementation, and operation of automated systems to minimize losses and create a virtual environment that prioritizes consumer welfare. Incorporating clear regulations and provisions that specifically address fake alerts from automated banking systems could help Nigeria establish a more secure and responsive banking environment. Banks must implement AI solutions that optimize the use of consumer data, ensuring that any data in their possession is adequately protected. In the event of a data breach, banks should take full responsibility and work to mitigate harm. Such measures will not only help prevent customer dissatisfaction but also bolster overall trust in the financial system. Holding banks accountable for errors and providing a transparent mechanism for addressing grievances will contribute to a more equitable and reliable banking experience for everyone.

FOI Counsel is a law group established primarily to provide legal assistance to NGOs and the media seeking for information, under the Freedom of Information Act 2011. We are also, the first Freedom of Information Act (FOIA) Liigation-specialized firm in Africa. As the demand for our services increased we billowed into four thematic areas of work and these are: FOI Advocacy & Litigation, Human Rights Litigation, Land reforms & rural development and Research & Policy Advocacy

This current newsletter edition and all previous editions can be downloaded for free online via: www.foicounsel.com/publications

Contact Us Today

FOI HOUSE: 4 Ikpokpan Street off Sapele Road,
opposite Edo State Ministry of Infrastructure, Benin City.
info@foicounsel.com | +2348032683434