OLANIWUN AJAYI

FEBRUARY 2026

Tackling Push Payment Fraud: An Overview of the Central Bank of Nigeria's Draft Guidelines for Handling Authorised Push Payment Fraud

OALP Technology, Innovation and Fintech Newsletter

INTRODUCTION

In November 2025, the Central Bank of Nigeria (**CBN**) circulated an exposure draft of the Guidelines for Handling Authorised Push Payment (**APP**) Fraud (the **Guidelines**). The Guidelines intend to respond to the growing incidence of fraud arising from customer-authorised digital transfers induced through deception, social engineering, or impersonation. They introduce minimum standards for prevention, detection, investigation, reimbursement, and reporting of APP fraud across Nigeria's payments ecosystem.

The Guidelines are issued pursuant to the CBN Act, 2007 and the Banks and Other Financial Institutions Act (**BOFIA**) 2020 and are intended to operate alongside existing consumer protection and payments regulations.

WHAT IS APP FRAUD ?

APP fraud occurs when a customer is manipulated or deceived into authorising a transfer to a fraudster's account. Unlike unauthorised transactions, the payment is validly initiated by the customer, making detection and recovery more complex. Users are misled or coerced into making transfers by bad actors under false pretences.[1] Popular instances include vendor impersonation or purchase scams, where a user is deceived into authorising a push payment to a fraudulent "vendor", after which the fraudster disappears, and no product or service is delivered. A common type of APP fraud in Nigeria is bank impersonation scams, in which a fraudster poses as a bank officer and induces the customer to authorise a payment.

APP fraud is a serious global problem, with the UK reporting a loss of £341 million (three hundred and forty-one million Pounds Sterling) to APP fraud in 2023 and global losses estimated to be around $1.03 trillion (one trillion, thirty billion US Dollars).[2] On a local level, it remains one of the most prevalent forms of banking fraud in Nigeria, with a significant amount of the 12,000 (twelve thousand) reported cases of fraud being instances of APP.[3]

SCOPE AND APPLICABILITY

The Guidelines apply to all Financial Institutions (**FIs**) regulated by the CBN. The Guidelines cover all electronic push payment channels, including mobile banking applications, internet banking, Unstructured Supplementary Service Data (USSD) services and payment gateway.[4]

WHAT AMOUNTS TO APP FRAUD UNDER THE GUIDELINES?

The Guidelines define APP fraud to include, but not be limited to:

i. User or customer inducement or coercion, for example, scams via WhatsApp, SMS, emails, and any other communication channel to a third party's account or wallet; [5]

1. Elizabeth Lumley, 'The global fight against APP', (Compliance Corylated, 2025) <*The global fight against APP fraud*> *accessed 14 December 2025*
2. *2Joanna Carruthers, 'Authorised Push Payment (APP) Fraud: A global 'scamdemic'' (WTW, December 2025) <Authorised Push Payment (APP) Fraud: A global ''scamdemic' - WTW> accessed 12 December 2025*
3. *Yemi, 'MoneyRise Weekly Briefing: CBN vs Fraud' (moneyrise, December 2025) <*MoneyRise Weekly Briefing: CBN vs FRAUD | Risevest Blog *> accessed 10 December 2025*
4. *Paragraph 3.0 of the Guidelines*
5. *Paragraph 4.0 (i) of the Guidelines*

II. FI facilitation, negligence, or non-compliance, including failure to act on red flags, weak Know Your Customer (KYC) process, ineffective fraud controls, staff collusion, delayed resolution, and use of accounts for fraudulent purposes.[6]

While the Guidelines set out a robust and non-exhaustive definition of APP fraud, they do not explain how additional forms are to be identified or recognised within the scope. Although this flexibility allows the Guidelines to evolve as fraud methods change, the absence of clarity on how new forms of authorised fraud will be incorporated may ultimately undermine their effectiveness by creating uncertainty.

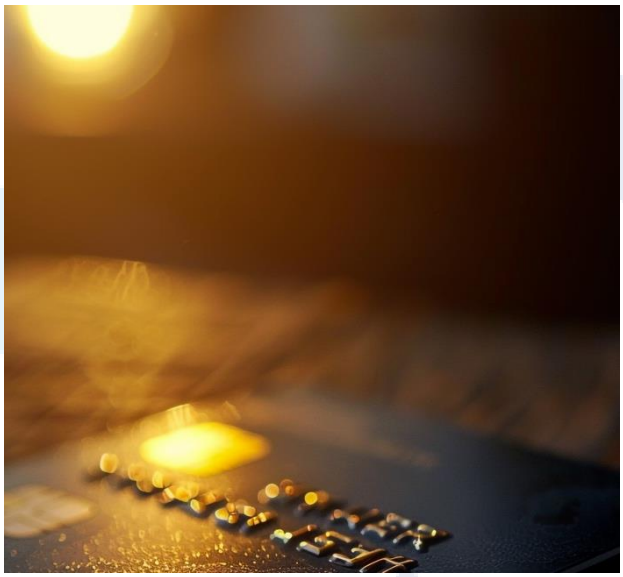
In the United Kingdom, APP Fraud is governed by two pieces of legislation, the Financial Services Markets Act 2023 (FSMA) and Payment Services (Amendment) Regulations 2024 (PSR). Nonetheless, APP Fraud is not expressly defined in either statute. FSMA outlines that a qualifying case for reimbursement of fraudulent transactions is where a payment has been made through the Faster Payments Scheme and the payment was as a result of fraud or dishonest activity.[7] This is further supplemented by the PSR, which details the reimbursement obligations, timelines, and allocation of liability payment service providers. These measures help create a clear scope of APP fraud, whilst still allowing regulatory guidance to develop alongside evolvement of fraud.[8]

KEY REGULATORY OBLIGATIONS

Governance and Board Oversight

The Guidelines strengthen the governance obligations by placing the primary responsibility for the APP Fraud risk management on the Board of Directors of FIs . In carrying out this responsibility, the Board must do the following:

i. adopt an APP fraud policy covering prevention, detection, mitigation, investigation, response, recovery, and conduct a post-incident review of APP fraud where they occur[9];
ii. periodically review APP Fraud trends and evaluate the effectiveness of the controls implemented[10];
iii. formulate, approve, and implement a comprehensive APP Policy which must contain particular elements, some of which include: the scope and definition of APP fraud, outline clearly the roles and responsibilities of the Board, committees, the risk assessment framework, the prevention and detection measures, and the investigation and escalation procedures;[11]
iv. review the APP Fraud Policy once every two years;[12]
v. assign the oversight responsibility of the APP fraud risk to the Board Risk Management Committee and investigation oversight to the Board Audit Committee;[13] and
vi. designate the Head of Compliance as responsible for implementation of the Guidelines.[14]



Risk Management and Early Warning Systems (EWS)

FIs are required to engage in proactive fraud prevention. One of the mechanisms required is the implementation of a robust Early Warning System (EWS) to flag suspicious accounts, identify unusual account activities, assess and monitor behavioural anomalies as well as extensively document EWS indicators.[15]

Once an account is flagged by the EWS, it must undergo enhanced monitoring and/or restriction pending a full investigation. Additionally, institutions must have a unit that will be responsible for carrying out fraud data analytics, with the allocated resources for this unit being proportional to the institution's size.

6. *Paragraph 4.0 (i) of the Guidelines*
7. *Section 72(2) Financial Services and Markets Act 2023*
8. *Merje, 'APP Fraud guide : UK mandatory reimbursement regulations' <APP fraud guide: UK mandatory reimbursement regulations> accessed 20 December 2025 and Payment Systems Regulator <Specific Direction 20 (July 2024)> accessed 20 December 2025*
9. *Paragraph 5.0 (i) of the Guidelines*
10. *Paragraph 5.0 (ii) of the Guidelines*
11. *Paragraph 5.0 (iii) (a)-(f) of the Guidelines.*
12. *Paragraph 5.0 (iv) of the Guidelines.*
13. *Paragraph 5.0 (v) and (vi) of the Guidelines.*
14. *Paragraph 5.0 (viii) of the Guidelines.*
15. *Paragraph 6.0 of the Guidelines*

Customer Reporting and Complaints Handling

FIs are to establish reporting mechanisms, provide clients with 24/7 fraud reporting channels, including hotlines, email, mobile apps, USSD, and physical branches, to ensure customers can report fraud incidents at any time.

The Guidelines introduce stricter timelines for reporting for FIs and customers. Customers are expected to report an APP fraud within 72 (seventy-two) hours of its occurrence. Failure to report within the time frame, without reasonable justification, may disqualify the customer from receiving a disbursement form. FIs are expected to acknowledge receipt of complaints within 24 (twenty-four) hours with a case reference number and complete investigations within 14 (fourteen) working days. Where a company is unable to complete this within 14 (fourteen) days, it must be escalated directly to the Central Bank of Nigeria (CBN)'s Consumer Protection Department (CPD), which will then take a final decision on the matter.

Reimbursement

The Guidelines introduce a mandatory, structured, and time-bound reimbursement procedure for non-negligent victims who fall into any of the following categories;[16]

i. the victim was deceived by a third party;[17]
ii. the victim reported the incident within the allotted 72 (seventy-two) hours;[18]
iii. there is no evidence of contributory negligence or collusion on the part of the victim; and[19]
iv. the bank was negligent in detecting the appropriate warning signs.[20]

Upon the conclusion of an investigation into the reported instance of APP fraud, where the institution is satisfied that the victim falls into any of these categories, they are mandated to reimburse the victims within 48 (forty-eight) hours of concluding their investigation.[21]

Additionally, the Guidelines provide that where the APP Fraud spans across multiple institutions, and it is unclear which institution is at fault, there will be shared liability amongst the institutions in issuing the reimbursement to the victim. This is similar to the current stance of the United Kingdom, where the Payment Systems Regulator (PSR) has implemented shared liability for Faster Payments and Clearing House Automated Payment System (CHAPS).[22] The reimbursement of fraud victims is divided equally between sending and receiving FIs.

Consumer Education and Awareness

The Guidelines mandate FIs to ensure customers are aware of the fraud reporting channels that are available to them and provide clear, accessible, and continuous education on APP fraud risks and the reporting procedures.[23] FIs are to conduct quarterly awareness campaigns across diverse media and languages.[24]

Regulatory Reporting and Sanctions

Under the Guidelines, FIs must report APP fraud incidents, trends and remedial actions to the relevant supervisory department.[25] FIs must also provide evidence of financial literacy programs they have conducted, including the number of consumers reached and languages used, to the Director of the Consumer Protection and Financial Inclusion Department.[26] Further, they must maintain comprehensive records of APP Fraud incidents and provide them to the CBN upon request.[27]

The Guidelines also provide that non-compliance, including failure by institutions to investigate within the stipulated timelines or false reporting on the part of the individual, will attract monetary penalties and administrative sanctions for both the institution and the responsible individuals.[28] The nature and amount of these penalties and sanctions will be determined and prescribed by the CBN.[29]

16. *Paragraph 8.1 of the Guidelines*
17. *Paragraph 8.1(i) of the Guidelines*
18. *Paragraph 8.1(ii) of the Guidelines*
19. *Paragraph 8.1(iii) of the Guidelines*
20. *Paragraph 8.1(iv) of the Guidelines*
21. *Paragraph 8.0 (ii) of the Guidelines*
22. *CHAPS, it is a payment system that enables realtime settlements of transactions, allowing for instant and secure payments. See Equals Money, 'What is CHAPS? CHAPS Network & Payments Explained' What is CHAPS? CHAPS Network & Payments Explained | Equals Money Accessed 10 December 2025*
23. *Paragraph 10.0 (i) of the Guidelines*
24. *Paragraph 10.0 (ii) of the Guidelines*
25. *Paragraph 12.0 (i) a of the Guidelines*
26. *Paragraph 12.0 (i) b of the Guidelines*
27. *Paragraph 12.0 (ii) of the Guidelines*
28. *Paragraph 13.0 (i) and Paragraph 13.0 (ii) of the Guidelines*
29. *Paragraph 13.0(i) of the Guidelines*

REFLECTIVE ANALYSIS OF THE GUIDELINES

The Draft Guidelines signifies a step in the right direction by shifting the onus from the customer and imposing clearer obligations on banks. In particular, the emphasis on board-level accountability, the introduction of the 72 (seventy - two) hour reporting window for consumers, the time- bound investigations and reimbursement obligations of banks display a meaningful progress in consumer protection.

However, despite these positive developments, a closer look at the provision reveals several areas that could benefit from greater clarity and robustness.

The Reimbursement Process

While introducing a shared liability model is commendable and it aligns with international standards, the guidelines do not explicitly define the precise split of this liability. The absence of a clear, defined percentage split creates uncertainty and may lead to inconsistent application, which will undermine the effectiveness and predictability of the reimbursement process.

The Early Warning System (EWS)

The EWS and strict investigation timelines help in setting clear expectations for both banks and consumers. However, the Guidelines do not adequately define what amounts to EWS for the purpose of the Guidelines. This leaves a critical element of the Guidelines open to varied interpretation and consistent implementation across the different institutions.

Absence of Data Sharing and Collaboration

A key element that was omitted in the Guidelines is a provision that mandates data sharing and collaboration between FIs, telecommunications companies, social media platforms, and law enforcement agencies. Whilst the customer reporting aspects of the Guidelines are on par with systems utilised in jurisdictions like Australia,[30] the absence of provisions that promote or facilitate data-sharing is a grave oversight and undermines the Guidelines' objective of carrying out an effective defence against fraud. Effective fraud prevention and remediation depend on the ability to track funds and communications across multiple platforms, and without such collaboration, the overall effectiveness of the framework is materially weakened.

CONCLUSION

The Guidelines represent meaningful progress in the desired direction, modernising Nigeria's financial fraud landscape, and would be the premier regulation that addresses this form of fraud in Nigeria. While the shift of liability, the imposition of timelines, and the requirement for an EWS are commendable, the CBN must tackle these key issues in order to ensure the Guidelines' maximum effectiveness.

30. Australia has implemented the Scam-Safe Accord is a collaboration amongst Australian banks that aims to protect consumers from scammers. One of its key provisions is data sharing, which has been crucial to effectively tracking and monitoring fraud across institutions. See: Australian Banking Association<Keeping Australia Scam Safe - Australian Banking Association> accessed 15 December 2025 and Customer Owned Banking Association (COBA, November 2024) <Scam-Safe Accord one year on: Customer-owned banks make strides in scam prevention | Customer Owned Banking Association> accessed 15 December 2025

FOR MORE INFORMATION, PLEASE CONTACT :

Damilola Salawu
Partner
dsalawu@olaniwunajayi.net

Opeyemi Araromi
Senior Associate
oararomi@olaniwunajayi.net

Olufolajimi Otitoola
Associate
ootitoola@olaniwunajayi.net

Oluwapamilerin Ogunleye
Associate
oogunleye@olaniwunajayi.net