ALUKO & OYEBODE
ALN

THE CENTRAL BANK OF NIGERIA INTRODUCES

New Instant Payment Security Requirements:

Compliance Considerations for Financial Institutions

Introduction

On 12 March 2026, the Central Bank of Nigeria ("**CBN**") issued its circular titled "Additional Functionalities for Instant Payment" addressed to all banks, other financial institutions ("**OFIs**") and payment service providers ("**PSPs**") (together, "**Financial Institutions**") operating in Nigeria (the "**Circular**"). The Circular took effect from 1 July 2026 and introduces a suite of new mandatory safeguards designed to strengthen fraud prevention and identity assurance.

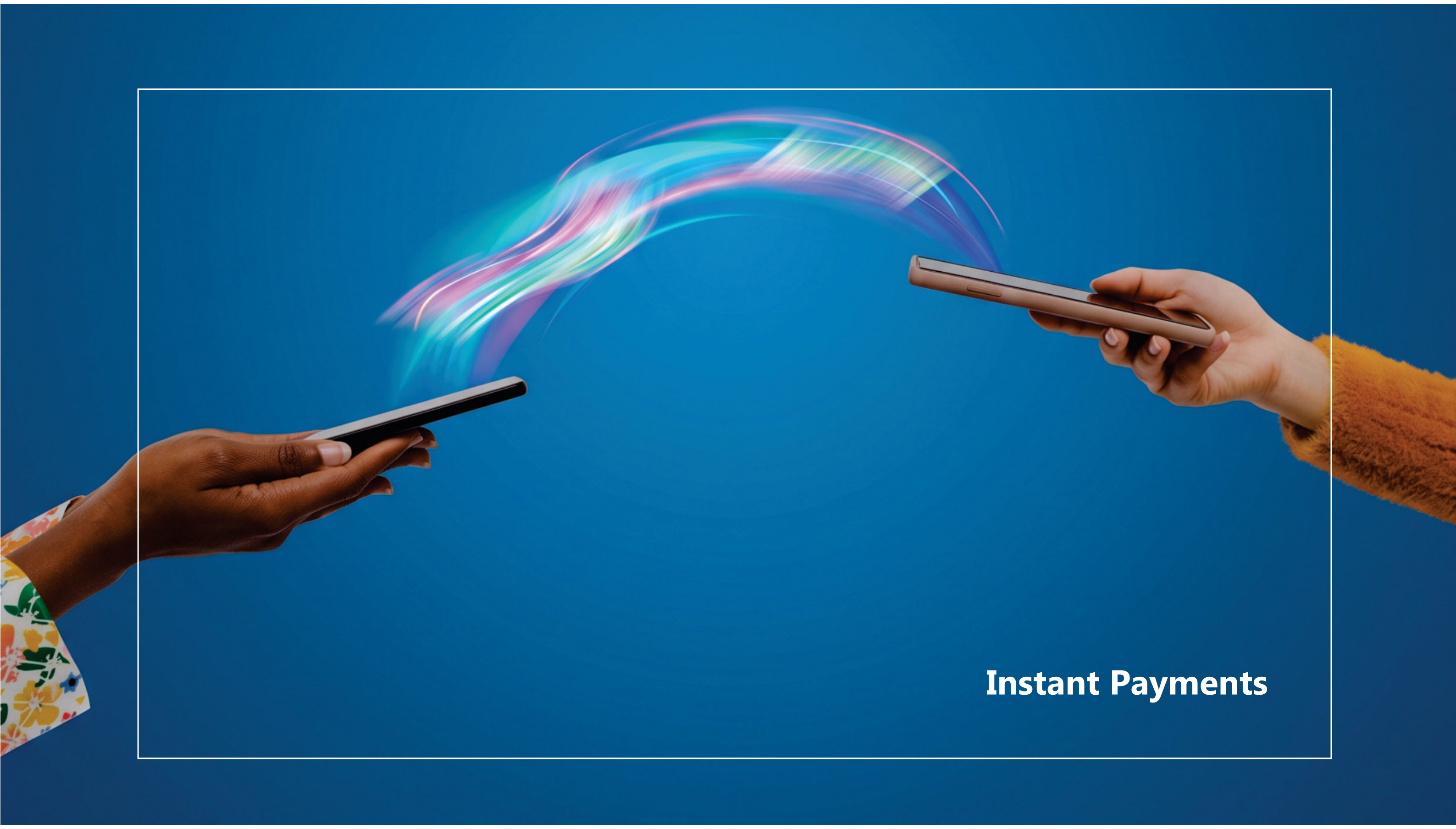
The Circular signals a notable regulatory shift and reflects the CBN's ongoing commitment to promoting financial system stability and addressing the evolving fraud risks associated with the rapid growth of instant payment services in Nigeria's digital financial ecosystem. Rather than merely facilitating payment speed and efficiency, the CBN now expects financial institutions to build stronger preventive controls into instant payment structures. The resulting obligations have significant operational, legal, data protection, cybersecurity and consumer protection implications.

Understanding Instant Payments

Instant payments have become the backbone of Nigeria's digital economy. They refer to electronic fund transfers in which payment instruction is transmitted and processed and the corresponding funds are made available to the beneficiary in real time or near real time (usually within seconds and on a 24-hour/7-day basis). Instant payments in Nigeria have significantly accelerated financial inclusion and cashless transactions and are enabled principally through the Nigeria Inter-Bank Settlement System Instant Payment infrastructure.

However, the speed that characterises instant payments also creates unique risks. Fraudulent transactions can be completed and settled within seconds, leaving little opportunity for intervention once a transaction has been executed. This may be exploited through various means, including taking over accounts with stolen credentials, using fabricated identities to receive illicit proceeds, deceiving customers into authorising payments themselves and hijacking mobile numbers to intercept authentication codes.

It is this combination of speed and near irrevocability of settled transactions that has prompted the CBN to require Financial Institutions to adopt additional security mechanisms for instant payment services.



Additional Functionalities Introduced by the Circular

The Circular provides that all Financial Institutions offering instant payment services shall provide five categories of additional functionalities, representing minimum standard requirements for the operation of instant payments in Nigeria:

1. Voluntary Opt-In and Opt-Out Functionality

The Circular requires that customers have the option to opt out of, or opt in to, instant payments service at any time and for any given period, subject to Multi-Factor Authentication **("MFA")** to ensure such changes are intentional and authorised through verified checks. The default setting for new customers upon onboarding shall be opt-in. Where a customer opts out, online instant transfers may not be initiated from the account, although transfers may still be effected through a physical visit to the Financial Institution.

This preserves the customer's ability to transact whilst removing the risk of unauthorised online transfers during periods when the customer considers their account to be at significant risk.

2. Voluntary Transaction Limit

Customers may set their own transaction limits, subject to the existing maximum transaction limit of 25,000,000.00 (Twenty-Five Million Naira) for individuals and 250,000,000.00 (Two Hundred and Fifty Million Naira) for corporate bodies. Any such adjustment to transaction limits shall be subject to customer consent reflected through MFA, enhanced due diligence and appropriate risk assessment by the Financial Institution.

This requirement ensures that limit increases are at customer convenience and are not processed without adequate scrutiny, mitigating the risk that a compromised account could be used to execute high-value fraudulent transfers.

3. Enterprise Fraud Monitoring

All Financial Institutions must implement and activate enterprise fraud monitoring for both inflows and outflows to facilitate fraud detection and restriction of suspicious transactions. This provision applies to both incoming and outgoing transactions, reflecting the need to monitor beneficiary accounts as well as originating accounts for effective fraud detection.

4. Liveliness Checks for Online Account Opening and Reactivation

The Circular introduces three specific requirements in respect of online account opening and account reactivation, that is, liveliness checks for accounts opened online, real-time Bank Verification Number/National Identification Number **("BVN/NIN")** validation for online account opening or account reactivation and enhanced authentication mechanisms (including MFA, biometric authentication, soft tokens, hard tokens, and liveliness checks) for online account reactivation.

5. **Additional Requirements for Mobile Financial Services via Mobile Applications**

The Circular introduces security measures applicable to mobile banking and digital financial services applications, including:

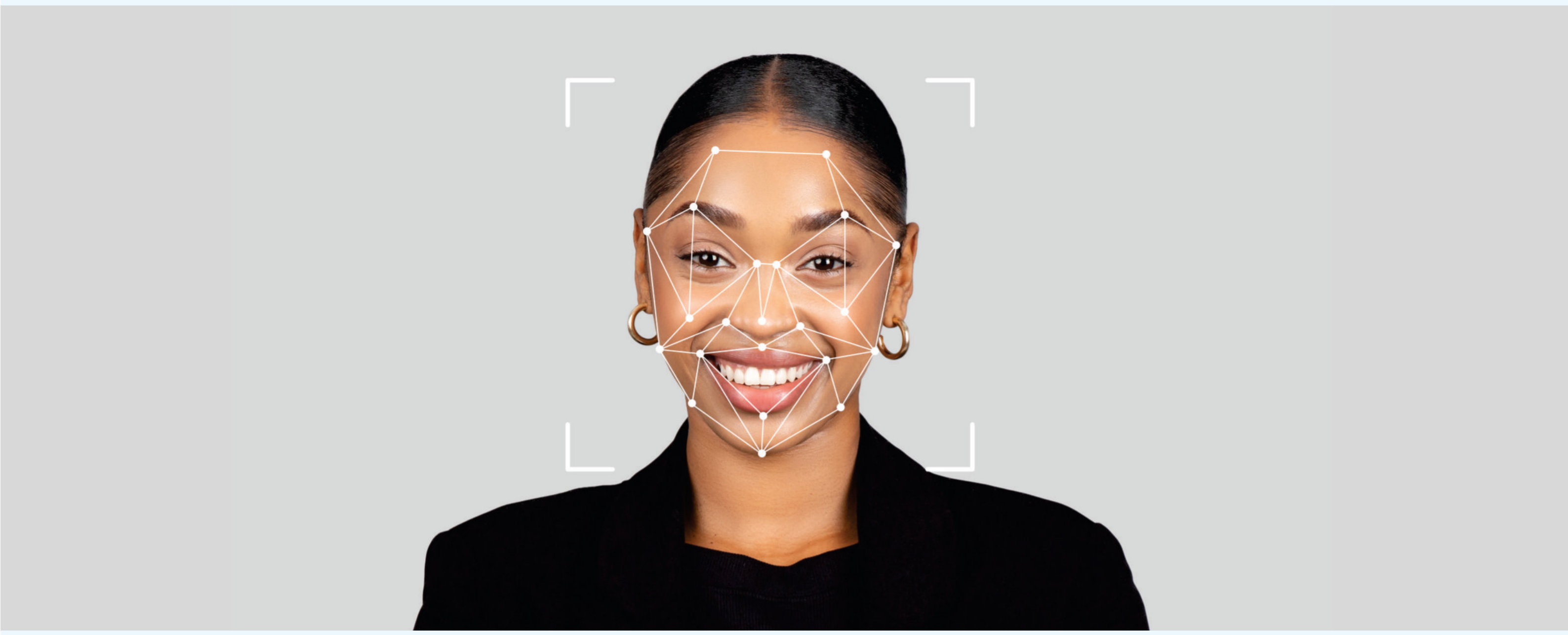
I. Mandatory Device Binding: Mobile financial services apps shall operate on only one registered device at a time;

ii. Reactivation upon device migration: Financial Institutions are to ensure automatic reactivation and authentication when customers migrate to a new device, preventing migration of a compromised session to a fraudulent device;

iii. Transaction limits for new accounts on newly activated apps: For new accounts, transaction limits (both inflow and outflow) shall be imposed on a newly activated mobile financial services app in the first 24 hours of activation, as determined by the Financial Institution, subject to a maximum transaction limit of ₦20,000.00 (Twenty Thousand Naira). This cooling-off period restricts the exposure of newly opened accounts to immediate fraudulent high-value transfers;

iv. Transaction limits for existing accounts on newly activated apps: For existing accounts, outflow transaction limits shall be imposed on a newly activated mobile financial services app in the first 24 hours of activation, as determined by the Financial Institution, subject to a maximum transaction limit of 20,000 (Twenty Thousand Naira). This requirement addresses situations wherein a fraudster gains access to an existing account through a new device, limiting potential loss during the first 24-hour window;

v. Additional MFA requirements for first-time internet banking access from a new device.



Compliance Implications for Financial Institutions Offering Instant Payment Services

1. Operational Implications

The Circular creates substantial operational obligations for Financial Institutions. Financial Institutions will be required to develop and deploy system modifications to core banking systems, mobile applications, customer consent management processes and customer support workflows as well as maintain records of customer elections and authentication to cater to customer opt-in/opt-out choices in real time.

The requirement for enterprise fraud monitoring is even more significant. Financial Institutions will need to invest in transaction surveillance tools and systems to monitor incoming and outgoing transactions in real time. Similarly, mandatory device binding and migration controls will require system redesigns to ensure that mobile applications cannot operate concurrently across multiple devices while maintaining continuity of service.

2. Legal Implications

The Circular also elevates former discretionary security practices into mandatory regulatory requirements. Institutions that fail to implement the prescribed minimum controls may therefore face regulatory scrutiny and potential sanctions, particularly where a fraud incident reveals that the Financial Institution failed to satisfy minimum security standards required by the Circular.

It also strengthens record-keeping obligations relating to customer consent. As changes to transaction limits take effect immediately upon successful MFA and customer authorisation, Financial Institutions should maintain reliable records evidencing both the customer's consent and the authentication process in the event of a dispute.

The mandatory adoption of enterprise fraud monitoring may also influence the standard of care expected of regulated entities. In future fraud-related claims or regulatory investigations, institutions may find it difficult to defend their conduct unless they can demonstrate effective transaction monitoring, risk assessment as well as authentication controls.

3. Data Protection Implications

The requirements relating to liveliness checks, biometric authentication, device recognition, and real-time BVN/NIN verification will involve the collection, processing, transfer and retention of sensitive personal information. As a result, institutions should reassess their compliance with the Nigeria Data Protection Act 2023, the General Application and Implementation Directive 2025 and other data protection laws in Nigeria.

4. Cybersecurity Implications

The Circular strengthens cybersecurity across the payments ecosystem by requiring real-time enterprise fraud monitoring and additional MFA. These measures reduce exposure to account takeover, SIM-swap fraud, credential theft, device cloning and unauthorised access of applications.

5. Consumer Protection Implications

The Circular directly advances consumer protection objectives by reducing fraud exposure and increasing customer control over payment services.

The opt-in/opt-out functions empower customers to control exposure to immediate transfer risks and introduce a protective mechanism that permits users to deactivate instant payment capabilities where fraud is suspected. Real-time BVN/NIN validation strengthens customer due diligence, while enterprise fraud monitoring supports the detection of suspicious transactions and illicit fund flows.

Similarly, customer-controlled transaction limits provide individuals and businesses with greater flexibility while ensuring that high-risk transactions are subject to enhanced scrutiny and risk assessment. The restrictions applicable during the first 24 hours following activation of a mobile financial services application also provide a safeguard against account compromise following onboarding or device migration.

Compliance Recommendations

In view of the Circular's implications and the compliance obligations it imposes, stakeholders in Nigeria's instant payments ecosystem need to assess their systems, policies and processes against its requirements. Any identified gaps should be promptly addressed through clear remediation timelines and appropriate compliance measures.

Where existing systems cannot support the Circular's measures, Financial Institutions should promptly upgrade their infrastructure or outsource to suitable technology infrastructure providers. They should also thoroughly test all new and modified features before deployment and document the results for appropriate governance and compliance review.

Financial Institutions ought to update their internal policies, operating procedures, customer terms and privacy notices to reflect the new Circular functionalities. Frontline compliance, fraud prevention and customer service personnel should be trained to apply the requirements, respond to customer enquiries and escalate suspected fraud. Financial Institutions would be well advised to regularly assess their incident-response processes and reliance on third-party providers to identify and address risks that could undermine compliance.

Clear customer communication will also be essential to the effective implementation of the Circular. Customers should receive information on the implications of the additional requirements regarding their use of instant payments. Mobile money operators and other PSPs should implement these safeguards in a manner that remains accessible to customers with limited digital literacy or connectivity, without weakening the security standards prescribed by the Circular.

Conclusion

The Circular marks a significant development in Nigeria's instant payments regime by placing fraud prevention and consumer protection at the centre of digital payment services. Through enterprise fraud monitoring, enhanced authentication, customer-controlled payment safeguards and stronger identity-verification measures, the CBN has raised the minimum-security standards applicable to participants in the payments ecosystem.

The Circular also advances the objectives of the CBN's Payments System Vision 2028[1], which seeks to establish a globally connected, safe and efficient payments ecosystem that supports financial inclusion in Nigeria. Its requirements recognise that the continued growth of instant payments depends not only on speed and accessibility, but also on effective safeguards against fraud and the resulting financial and reputational harm to consumers and Financial Institutions.

Financial Institutions should therefore treat compliance with the Circular as an ongoing operational responsibility rather than a one-off implementation exercise. Institutions that continuously test, review and improve these controls will be better positioned to manage emerging risks, maintain customer trust and compete effectively in Nigeria's increasingly real-time digital economy.

---

[1] Central Bank of Nigeria, *Nigeria Payments System Vision 2028* (2026) Nigeria Payments System Vision 2028.pdf accessed 20 July 2026

Authors

Ajibola Asolo
Partner

T: +234 810 216 4161
E: Ajibola.Asolo
@aluko-oyebode.com

Glory Akani
Associate

T: +234 916 834 9167
E: Glory.Akani
@aluko-oyebode.com

Imadenobiejeh Adejumo
Associate

T: +234 707 469 3482
E: Imadenobiejeh.Adejumo
@aluko-oyebode.com

Disclaimer

Aluko & Oyebode (the Firm) owns all copyrights and similar rights in the contents of this presentation; all rights in the contents of this publication are reserved to the firm and all trademarks, logos and brands displayed in this publication are either owned by the firm or licensed to it and must not be reproduced without its consent. Unauthorized copying is illegal. The contents of this publication, either in whole or in part, may not be reproduced, stored in a data retrieval system or transmitted in any form or by any means, electronic, mechanical photocopying or otherwise without the written consent of the Firm.

The views and opinions contained in this publication are those of the authors and should not be considered as independent legal advice to be relied upon for any purpose whatsoever. The Firm accepts no liability for the consequences of any reliance placed on the contents of this publication. The views, opinions and statements contained herein should not be relied upon for any personal, legal, contractual or financial or other decisions or possible gain. The information, opinions or views expressed in this publication may include inaccuracies or typographical errors. The firm accepts no liability for any errors in any of the views expressed here in.

If you are not the intended recipient(s), please contact Aluko & Oyebode via telephone (+234 201 4628360) or e-mail (ao@aluko-oyebode.com). For further information about Aluko & Oyebode, please visit our website at www.aluko-oyebode.com.

ALUKO & OYEBODE
ALN

Lagos

1, Murtala Muhammed Drive
(formerly Bank Road)
Ikoyi, Lagos, Nigeria

T: +234 201 462 8360 -71
E: ao@aluko-oyebode.com
W: www.aluko-oyebode.com

Port Harcourt

3rd Floor, Plot 173,
Sani Abacha Road
GRA Phase III, Port Harcourt
Rivers State, 234
Nigeria

T: +234 703 192 260

Abuja

Plot 1348A, Agulu Lake Street
Maitama, Abuja, Nigeria