Key contacts

Emmanuel Gbahabo
Partner,
Investigation White Collar Defense & Compliance
emmanuel.gbahabo@templars-law.com

Francis Jarigo
Associate,
Dispute Resolution
francis.jarigo@templars-law.com

Onyinye Omenugha
Associate,
Investigation White Collar Defense & Compliance
onyinye.omenugha@templars-law.com

Client Alert

Automated AML Solutions in Nigeria: Key Deadlines for Financial Institutions *Part 1*

Introduction

Nigeria's financial sector is entering a more technology-driven phase of anti-money laundering ("**AML**"), combating the financing of terrorism ("**CFT**") and countering proliferation financing ("**CPF**") compliance. New Baseline Standards[1] which were issued by the Central Bank of Nigeria (**CBN**) on 10 March 2026 in line with its objective to promote a sound financial system[2], now require financial institutions[3] to strengthen how they identify, monitor, investigate and report financial crime risks.

Deposit Money Banks are expected to achieve full compliance within 18 months from the 10th of March 2026 when the Baseline Standards took effect, while other financial institutions have 24 months. Full compliance therefore falls due on 10 September 2027 for Deposit Money Banks and on 10 March 2028 for other financial institutions. Implementation roadmaps were due to the Compliance Department of the CBN within three months of issuance, by 10 June 2026; institutions yet to file should do so as a priority.

The Baseline Standards mark a major development in financial crime compliance. Affected institutions are required to implement automated AML systems capable of detecting, analyzing and reporting suspicious activity in real time or near real time.

Who Is Affected

The standards apply to a broad range of regulated financial institutions supervised by the CBN.

---

[1] The Baseline Standards: https://www.cbn.gov.ng/Out/2026/CCD/CBN%20issues%20Baseline%20Standards%20for%20Automated%20Anti-Money%20Laundering%20Solution.pdf > accessed 11 March 2026

[2] Section 2 (d) of the CBN Act 2007

[3] Deposit Money Banks, Merchant Banks, Payment Service Banks, Mobile Money Operators, Payment Service Providers, International Money Transfer Operators and other institutions supervised by the CBN. The Baseline Standards also apply to new market entrants.

Application is, however, proportionate. Every CBN-regulated institution must operate an automated AML/CFT/CPF solution, but the depth and configuration required is calibrated to its transaction volumes, product complexity, customer base, geographic footprint and delivery channels, and its own documented ML/TF/PF risk assessment. The AML solutions are also expected to integrate with domestic and global sanctions, watchlists, and high-risk/PEP registers[4], providing real-time or near-real-time screening of customers, beneficial owners, related parties, and transactions. The solution is also expected to support advanced matching techniques, negative media monitoring, automated interdiction or transaction holds, internal watchlists, and verifiable logging to demonstrate effectiveness. Institutions in business lines with elevated inherent risk, as identified in National and Sectoral Risk Assessments, must apply enhanced monitoring regardless of size, and where the Baseline Standards overlap with other laws the more stringent requirement applies[5].

The CBN will assess compliance through off-site surveillance, on-site examinations and thematic reviews. Institutions seeking authorisation after 10 March 2026 must demonstrate compliance with, or a credible plan to achieve compliance with, the Baseline Standards as part of the licensing process[6].

What the Standards Require

Financial institutions must deploy automated AML platforms[7] that detect suspicious activity across customer accounts and transactions.

At a minimum, these solutions should cover[8]:

a. Customer identification and verification;
b. Customer and enterprise-wide risk assessment;
c. Sanctions, watchlist and politically exposed person screening;
d. Transaction monitoring and risk-based analysis;
e. Case management and investigations;
f. Regulatory and internal reporting; and
g. Audit trails, governance controls and data protection.

Monitoring built on raw transactional data alone will not be accepted: an AML Solution that is not effectively linked to CDD/KYC/KYB information and customer risk assessments will not be regarded as compliant. Institutions must maintain, for each customer and its related parties, a consolidated view linking KYC/KYB data, risk classification, transactional behaviour, alerts and case history[9].

Practical Next Steps for Financial Institutions

In light of the new Baseline Standards, financial institutions should consider taking the following steps to position themselves for timely compliance:

a. **Conduct a Gap Assessment of Existing AML Monitoring Systems:** Institutions should undertake a comprehensive gap assessment of their AML monitoring frameworks against the functional and governance requirements set out in the Baseline Standards. This assessment should evaluate the capabilities of existing monitoring systems, including transaction monitoring rules, risk-scoring models, sanctions screening tools, and reporting mechanisms.

[4] Paragraph 5.3 of the Baseline Standards
[5] Paragraph 4 of the Baseline Standards (Proportionality Principle).
[6] Paragraph 7 of the Baseline Standards.
[7] Paragraph 5.1 of the Baseline Standards
[8] The Baseline Standards set out the minimum AML system capabilities and governance requirements, while allowing institutions to adopt more stringent controls based on their risk profile.
[9] Paragraph 4 of the Baseline Standards.

b. **Develop a Technology Implementation Roadmap:** Following the gap assessment, institutions should develop a structured technology implementation roadmap outlining how they intend to achieve compliance within the prescribed regulatory timelines.

c. **Address Regulatory Notification Obligations:** Institutions should confirm that the CBN has been notified of all AML solutions in use and their functional roles and, where automated alert closure is permitted, of that practice and the applicable threshold.

Institutions that fail to implement effective AML systems may face remedial directives, administrative sanctions and penalties against both the institution and accountable individuals under applicable laws and regulations, including BOFIA, MLPPA and the AML/CFT/CPF Administrative Sanctions Regulations 2023.

If you require any further clarification, do not hesitate to contact us.