

EIGHTH EDITION ■ ■ ■ OCT. 2026



# COMPLIANCE DIGEST

NEWS LETTER

INSIGHTS.  
PERSPECTIVES.  
A STRONGER  
COMPLIANCE  
COMMUNITY

[www.accobin.org.ng](http://www.accobin.org.ng)

## FROM FRAUD TO FINANCIAL CRIME INTELLIGENCE

COMPLIANCE • ETHICS • TRUST • SUSTAINABLE GROWTH

# Table of Contents

---

Trade-Based Money Laundering in Nigeria:  
Turning Trade Data into an Early-Warning System

02

Nigeria's Next GIABA Mutual Evaluation:  
From Technical Compliance to Demonstrable  
Effectiveness

04

From Fraud Events to Financial Crime Intelligence:  
Closing the Gap Between Fraud and AML

06

Financial Institutions as Barriers to Financial Crime:  
From Detection to Prevention, Disruption and  
Useful Intelligence

08

Sanctions Screening in Nigeria:  
Can Your Institution Demonstrate That Its Controls  
Work?

10

# Trade-Based Money Laundering in Nigeria: \_\_\_\_\_

## TURNING TRADE DATA INTO AN EARLY-WARNING SYSTEM

**T**rade-based money laundering occurs when criminals misuse legitimate trade transactions or networks to disguise and move criminal value. The trade may appear genuine on its face, while value is transferred through manipulated price, quantity, quality, description, documentation, shipment, payment terms or counterparties.

For Nigerian banks involved in imports, exports, letters of credit, bills for collection, guarantees, foreign-exchange transactions and other trade-related activity, the key question is not only where the funds originated. Institutions must also assess whether the customer, goods, counterparties, route, price, documentation, payment flow and stated commercial purpose make sense when viewed together.

Common TBML methods include over-invoicing and under-invoicing, multiple invoicing of the same goods, over-shipment or under-shipment, false description or classification of goods, and fictitious or phantom trade. Exposure may also arise where the bank does not finance the shipment, but processes related account or payment activity.

### The Regulatory Foundation

The MLPPA 2022, BOFIA 2020, CBN AML/CFT/CPF Regulations 2022 and CBN CDD Regulations 2023 provide the principal banking obligations relevant to TBML, including risk assessment, CDD and beneficial-ownership verification, EDD, ongoing monitoring, scrutiny of unusual transactions, record keeping, internal controls and suspicious-transaction reporting. Relevant sanctions and proliferation-financing obligations must also be considered where trade goods, parties, vessels, routes or jurisdictions create exposure.

These obligations align with FATF Recommendations I, 10, 11, 18, 19, 20, 21, 24 and 25. Payment transparency under Recommendation 16 and targeted-financial-sanctions obligations under

Recommendations 6 and 7 may also be relevant.

## What Should Banks look for

FATF and the Egmont Group organise Trade Based Money Laundering (TBML) indicators around the structure of the business, trade activity, trade documents and commodities, and account and transaction activity. Indicators should be assessed in combination and context. One indicator alone does not establish TBML, and a credible commercial explanation should be tested rather than assumed.

### Business Structure and Customer Profile

- A newly formed or low-capacity business undertakes trade materially inconsistent with its stated activity, facilities, turnover, staff or history.
- Ownership or control is opaque, unusually complex or disconnected from the stated trade purpose.
- Counterparties, intermediaries or related parties have no clear commercial role.

### Trade Activity

- Price, quantity, quality or profit margin appears materially inconsistent with reliable comparable information after considering grade, Incoterms, freight, insurance and market conditions.
- Goods, trade route, shipping pattern or jurisdiction has no clear economic logic for the customer.
- Repeated amendments, circular trade, unexplained trans-shipment or activity between related parties lack a credible commercial rationale.

*Trade documents and commodities*

- Invoices, bills of lading, customs declarations, purchase orders, certificates or payment instructions contain material inconsistencies.
- Descriptions are vague, goods appear misclassified, quantities or weights conflict, or documents appear reused or altered.
- Evidence of shipment, delivery or import/export activity is absent or inconsistent with the payment.

*Account and transaction activity*

- Payments are made by or to unrelated third parties without a reasonable explanation.
- Trade payments are split, routed or settled in a manner inconsistent with contractual terms or the customer profile.
- Account activity, FX flows, source of funds or settlement behaviour does not align with the customer's known business and expected activity.

**From Transaction Monitoring to Trade Intelligence**

TBML detection requires an integrated view of KYC/KYB information, beneficial ownership, customer risk ratings, trade documents, account activity, FX transactions, sanctions screening, payment data and case history. Where lawfully available and reliable, shipping, customs and external price information can strengthen the assessment. Data provenance, quality and differences in goods or contract terms must be considered before drawing conclusions.

Automated monitoring can help identify patterns across transactions, but it should not replace trade expertise and human judgement. Institutions should define scenarios, thresholds and escalation triggers from their TBML risk assessment, test both false positives and missed-risk outcomes, control overrides and maintain an auditable rationale for decisions.

**Investigation, Escalation and Reporting**

A red flag is a prompt for further inquiry, not proof of criminal conduct. Investigators should review the customer profile, beneficial ownership, counterparties, trade purpose, documents, goods, pricing basis, routes, payment flows and explanations. Requests for additional information and the reasons for closure or escalation should be documented.

Where the institution forms a suspicion of money laundering, terrorist financing or proliferation financing, the matter should be escalated and reported through approved procedures in accordance with applicable law and regulatory requirements. Confidentiality and tipping-off restrictions must be observed. Records should be sufficient to reconstruct the transaction and the institution's decision-making.

**Governance and Evidence of Effectiveness**

The Board and senior management should receive decision-useful information on material TBML exposures, high-risk trade corridors and products, alert ageing, investigation quality, reporting outcomes, data limitations, control exceptions and remediation. Responsibilities across Business, Trade Operations, Compliance, Technology, Risk and Internal Audit should be clearly documented.

Effectiveness should be tested through file reviews, scenario validation, data-quality testing, thematic analysis, staff competency assessment and independent assurance. The aim is not simply to process compliant-looking documents, but to demonstrate that the institution can identify transactions whose economic substance, value movement or trade rationale is inconsistent with legitimate activity.

## Final Message

The core question for each trade-related relationship or transaction is: does the activity make commercial and economic sense when assessed against the customer's known business, beneficial ownership, goods, counterparties, route, documentation, payment flows and stated purpose? Banks that convert trade data into reliable, connected and explainable financial intelligence will be better positioned to identify suspicious activity and support the integrity of Nigeria's financial system.



# Nigeria's Next GIABA Mutual Evaluation: From Technical Compliance to Demonstrable Effectiveness.

**N**igeria is at a defining point in strengthening its framework against money laundering, terrorist financing and proliferation financing. For Nigerian banks, the next mutual evaluation should not be treated as a documentation exercise. The decisive question is whether laws, policies, systems and institutional arrangements are producing reliable and measurable outcomes.

FATF assessments examine technical compliance with the 40 Recommendations and effectiveness through 11 Immediate Outcomes. Technical compliance concerns the required legal, regulatory and institutional framework. Effectiveness concerns whether that framework works in practice, having regard to Nigeria's risks and context.

## Clarifying the timetable

GIABA's consolidated calendar lists Nigeria's tentative on-site assessment for March 2028 and plenary discussion for November 2028, and states that all dates are subject to change. Any 2027 initiative should therefore be described as a national readiness programme, not as the mutual evaluation itself, unless an official competent-authority instrument states otherwise.

## The Regulatory Foundation

The domestic framework includes the MLPPA 2022, TPPA 2022, POCRMA 2022, BOFIA 2020, CBN AML/CFT/CPF Regulations 2022, CBN CDD Regulations 2023, applicable targeted-financial-sanctions instruments and the CBN Baseline Standards for Automated AML Solutions issued on 10 March 2026.

Nigeria's November 2024 follow-up report recorded 36 Recommendations as Compliant or Largely Compliant. That follow-up report addressed technical compliance and expressly did not analyse progress in effectiveness. The next challenge is therefore sustained and demonstrable implementation.

## What Banks Should be Doing Now

### *Refresh enterprise-wide ML/TF/PF risk assessments*

Assess actual exposure across customers, beneficial owners, products, services, delivery channels, geographies, correspondent banking, trade finance, cross-border payments, digital onboarding, agents, third parties and new technologies. Translate identified risks into risk appetite, controls, scenarios, assurance and remediation.

### *Test whether controls are genuinely effective*

Test data completeness, scenario coverage, threshold calibration, alert ageing, false negatives, override governance, investigation quality, STR usefulness and independent validation. Alert or STR volumes alone do not prove effectiveness.



### *Strengthen beneficial-ownership controls*

Identify and take reasonable measures to verify the natural persons who ultimately own or control customers. Address layered structures, legal arrangements, nominees and changes in ownership or control, and connect BO data to screening and monitoring.

### *Demonstrate effective TFS and PF controls*

Evidence timely list updates, screening, investigation, escalation, reporting and freezing without delay where required. Assess PF exposure in trade finance, cross-border payments, dual-use goods, opaque structures, trans-shipment and unusual payment chains.

### *Measure outcomes, not activity alone*

Distinguish activity, quality, timeliness and outcome measures. Review root causes, repeat findings, overdue remediation, data-quality exceptions, high-risk review quality and independent-testing results.

### *Validate technology, data and model governance*

The CBN March 2026 Baseline Standards require automated solutions supporting CDD/KYC/KYB, sanctions and PEP screening, risk assessment, monitoring, case management, reporting, audit, governance, integration, security and data protection. Institutions should evidence configuration, validation, audit trails, resilience and accountable change control.

### *Connect financial-crime intelligence*

Fraud may generate criminal proceeds that are subsequently laundered. Connect relevant intelligence across Fraud, AML, Sanctions, Cybersecurity, Investigations and Operations, subject to lawful access and confidentiality.

## **The Board and Senior Management Must Own The Outcome**

Oversight should extend beyond policy approval. Board should receive decision-useful information on material risks, high-risk exposures, sanctions incidents, overdue alerts and reviews, regulatory breaches, control limitations, assurance results, remediation, technology weaknesses and resource adequacy. The key question is: what evidence shows that the framework operates effectively against the institution's actual risks?

## **A Sector-wide Evidence Agenda**

Mutual-evaluation readiness is not solely a Compliance responsibility. Each institution should maintain an evidence inventory linking legal obligations and risks to controls, owners, data, testing, incidents, regulatory reports, management decisions and remediation. Evidence should be reliable, reproducible and capable of showing not only what was done, but what changed as a result.

The best positioned institutions for scrutiny will be those that can demonstrate, with credible data and documented evidence, that their controls prevent, detect, disrupt and report financial crime in a manner proportionate to their risks.



# From Fraud Events to Financial Crime Intelligence: Closing the Gap Between Fraud and AML

**F**raud and money laundering are often managed through different teams, systems and objectives. Fraud functions may focus on prevention, customer protection, containment and recovery, while AML functions assess whether activity indicates proceeds of crime, concealment, layering or other suspicious financial behaviour. When relevant intelligence is not connected, the institution may identify the initial fraud but lose sight of the proceeds, beneficiaries and wider network.

Money laundering does not always begin only after the fraud has ended. The movement, concealment or conversion of proceeds may occur during the fraud, immediately afterwards or as an integral part of the scheme. Effective financial-crime risk management therefore requires timely coordination without removing the distinct mandates, accountabilities and independent judgement of Fraud and AML functions.

## From a Fraud Event to a Laundering Risk

Consider account takeovers, social-engineering incident, insider-enabled fraud, false-invoice scheme or unauthorised electronic transaction. The first response may identify the compromised account, restrict further loss and pursue recovery. The AML question is broader: were the proceeds rapidly transferred through mule or intermediary accounts, split across beneficiaries, withdrawn in cash, converted into assets, routed across institutions or jurisdictions, or otherwise moved to conceal their origin or ultimate beneficiary?

A fraud event is not automatically proof of money laundering and should not automatically result in an STR. It is, however, a material source of intelligence. The institution should assess the facts, transaction flow, customer profile, beneficiary relationships, ownership and control, destination of funds and any indicators of concealment or further criminality.

## The Nigerian Regulatory and Fatf Foundation

The MLPPA 2022, BOFIA 2020, CBN

AML/CFT/CPF Regulations 2022 and CBN CDD Regulations 2023 provide the principal banking obligations relevant to risk assessment, CDD, ongoing monitoring, beneficial ownership, record keeping, internal controls and suspicious-transaction reporting. These obligations align with FATF Recommendations I, 10, 11, 15, 18, 20, 21, 24 and 25.

The CBN Baseline Standards for Automated AML Solutions, issued on 10 March 2026, expressly address fraud monitoring and detection. They require relevant risk signals to be exchanged between fraud and AML capabilities while maintaining the integrity of AML/CFT/CPF controls. The regulatory direction is therefore integration of intelligence, data and workflow, not a mandatory merger of organisational functions.

## Why the Two Functions Must Connect

Fraud teams may hold attack method, compromised device, channel, beneficiary, timing, recovery and known-modus-operandi information. AML teams may add customer and beneficial-ownership data, linked-account analysis, transaction history, rapid movement, layering, unusual cash activity, cross-border flows, sanctions or PEP context and prior alert or case history. When these perspectives are combined lawfully and consistently, the institution can move from asking only whether a transaction was fraudulent to determining where the proceeds moved, who controlled or benefited from them, whether a wider network exists and whether suspicion has arisen.

## When Should Fraud Trigger an AML Review?

Institutions should maintain documented, risk-based referral criteria. Relevant triggers may include rapid onward movement of proceeds, use of multiple or apparently unrelated beneficiaries, mule-account indicators, shared devices or contact data, third-party cash-out, unexplained cross-border routing, asset conversion, repeated fraud exposure, customer-profile inconsistency, opaque beneficial ownership, insider involvement or

conduct apparently intended to disguise the source, ownership, control or destination of funds.

The trigger initiates an AML review; it does not predetermine the outcome. Investigators should document the information reviewed, gaps identified, enquiries made, explanation obtained, reasons for closure or escalation and any decision to reassess the customer's risk rating, apply enhanced monitoring or submit an STR.

## What Banks Should Do

- *Establish formal referral criteria and service standards*  
Define who refers, what information is required, priority categories, escalation timelines, decision authority and how urgent cases are handled.
- *Connect fraud typologies to AML risk assessment and monitoring*  
Use confirmed and emerging fraud methods to inform enterprise risk assessment, customer-risk factors, monitoring scenarios and thematic reviews. Govern scenario changes, thresholds, validation and feedback.
- *Coordinate investigations without blurring accountability*  
For material networked cases, create a shared case view and investigation plan while preserving role clarity, need-to-know access, evidential integrity, legal privilege where applicable and independent AML judgement.
- *Build a lawful, auditable intelligence architecture*  
Link relevant accounts, beneficial owners, signatories, beneficiaries, counterparties, devices, channels, contact details, IP or geolocation data where lawfully available, transaction patterns and case history. Apply access controls, data-quality checks and audit trails.
- *Improve STR quality, not merely volume*  
Use fraud findings to provide a factual chronology, transaction flow, parties, instruments, predicate-offence indicators, destination of proceeds and clear basis for suspicion. Avoid speculation and observe tipping-off restrictions.

- *Reassess customer and network risk*  
Where fraud intelligence materially changes the understanding of a customer or connected parties, consider event-driven CDD, beneficial-ownership review, risk reclassification, enhanced monitoring and relationship-risk decisions.
- *Align recovery, restriction and AML decisions*  
Recovery activity, account restrictions, customer communications and AML review should be coordinated so that asset-protection action does not compromise investigation, reporting or confidentiality obligations.
- *Establish financial-crime governance and assurance*  
A management forum should review material cases, emerging typologies, data gaps, overdue referrals, control limitations and remediation. Independent assurance should test design and operating effectiveness.

## What Should Management Measure?

Useful indicators may include fraud-to-AML referral timeliness, completeness of referral data, linked-account or network identification, investigation ageing, repeat mule or beneficiary detection, customer-risk reassessment, STR quality review, recovery coordination, data-quality exceptions, scenario changes, overrides, control failures and closure of remediation. Metrics should show quality, timeliness and outcomes, not activity alone.

### The Strategic Message

Nigerian banks do not need to abolish separate Fraud and AML functions to achieve integration. They need a unified financial-crime framework in which intelligence is exchanged lawfully, responsibilities are clear, relevant systems interoperate, material cases are coordinated, decisions are auditable and the Board receives evidence that the framework works.

The defining question is: when fraud is detected, can the institution promptly identify the beneficiaries and connected network, trace the proceeds, determine whether money-laundering suspicion has arisen, preserve the evidence, coordinate recovery and meet all reporting and confidentiality obligations?

# Financial Institutions as Barriers to Financial Crime: From Detection to Prevention, Disruption and Useful Intelligence

**F**inancial institutions occupy a critical position in protecting the integrity of Nigeria's financial system. Through customer onboarding, payments, trade, foreign exchange, lending and other services, they encounter information that can help prevent misuse, identify suspicious behaviour, disrupt unlawful financial flows and provide useful intelligence to competent authorities.

Banks are not the sole defence against financial crime and cannot guarantee that every criminal will be excluded. They operate within a wider national framework involving regulators, the NFIU, law-enforcement agencies, prosecutors and other competent authorities. Their obligation is to apply effective, risk-based and proportionate controls while keeping legitimate financial services accessible and efficient.

## *The Nigerian Regulatory and FATF Foundation*

The MLPPA 2022, TPPA 2022, POCRMA 2022, BOFIA 2020, CBN AML/CFT/CPF Regulations 2022, CBN CDD Regulations 2023, applicable Nigerian targeted-financial-sanctions instruments and CBN Baseline Standards for Automated AML Solutions 2026 together establish relevant obligations concerning risk assessment, CDD, beneficial ownership, internal controls, monitoring, record keeping, reporting, sanctions, technology and cooperation with competent authorities.

These obligations align with FATF Recommendations 1, 6, 7, 10-12, 15, 16, 18-21, 24-27 and 35. For banks, the effectiveness question is whether preventive measures work in practice, financial intelligence is useful, sanctions obligations are implemented, weaknesses are identified and remediation is sustained.

## *The Bank As A Preventive Barrier*

CDD and KYC are not mere onboarding formalities. Institutions should identify and verify customers, understand the purpose and intended nature of relationships, identify and take reasonable measures to verify beneficial owners, establish expected

activity and obtain source-of-funds or source-of-wealth information where required by risk and applicable regulation. Reviews should be periodic and event-driven, with enhanced measures for higher-risk relationships and activities.

Prevention should remain proportionate. A risk-based approach requires stronger controls where risk is higher, but it should not be reduced to blanket rejection of customers, products or jurisdictions without an institution-specific assessment and documented rationale.

## *Monitoring in Customer Context*

Suspicious activity often appears as a pattern rather than one obviously suspicious transaction. Relevant indicators may include rapid movement of funds, unusual cash activity, transactions inconsistent with the customer profile, related-account networks, unusual cross-border activity or sudden behavioural change. The key question is whether the activity makes sense in light of the institution's knowledge of the customer, beneficial ownership, expected activity and risk profile.

Effective monitoring requires reliable and complete data, appropriate risk scenarios and thresholds, access to relevant KYC/KYB context, timely investigation, documented decisions, quality assurance, testing for missed-risk outcomes and independent validation. Alert volumes alone do not demonstrate effectiveness.

## *Targeted Financial Sanctions and Proliferation Financing*

Prevention also includes implementation of applicable targeted-financial-sanctions obligations. Institutions should maintain processes for current list updates, appropriate screening of customers, beneficial owners, connected parties and transactions, prompt investigation and escalation of potential matches, and freezing without delay where required by applicable law. PF exposure should be considered particularly in relevant trade-finance, cross-border and dual-use-goods activity.

### *Financial Crime Prevention is an Institutional Responsibility*

Prevention should not be left to Compliance alone. Business and operational functions should own risks and execute controls within their activities. Compliance should provide policy, oversight, monitoring and challenge. Technology, Fraud, Cybersecurity, Risk, Legal and other functions should contribute their specialist capabilities, while Internal Audit provides independent assurance. Responsibilities should be documented and supported by clear escalation and decision authority.

Information sharing should be lawful, secure, need-to-know and auditable, with appropriate confidentiality, data-protection and access controls. Connected intelligence is valuable only where its quality, provenance and permitted use are understood.

### *Suspicious Transaction Reporting and The Limits of The Bank's Role*

Financial institutions do not determine criminal guilt or exercise law-enforcement powers. They do, however, investigate alerts and customer activity sufficiently to determine whether suspicion exists, take appropriate internal action and submit required reports through approved channels. They should maintain confidentiality and avoid tipping off.

The value of STR reporting depends on quality, timeliness and usefulness, not volume alone. A meaningful report should present relevant facts, chronology, transaction flow, parties, instruments, indicators, linkages and the objective basis for suspicion, supported by records sufficient to reconstruct the activity and the institution's decision-making.

### *Technology as An Enabling Barrier*

The CBN Baseline Standards for Automated AML Solutions, issued on 10 March 2026, establish minimum functional, governance and control expectations for technology supporting CDD/KYC/KYB, sanctions and PEP screening, customer risk assessment, transaction monitoring, case management, reporting, audit, integration, security and data protection. Automation must support demonstrable effectiveness rather than feature-based compliance.

Institutions should distinguish technologies that screen or interdict before onboarding or transaction completion from transaction-monitoring processes that generate alerts for investigation. AI, behavioural analytics and network analysis may improve detection, but they require reliable data, explainability, documented governance, human oversight, validation, change control, security, operational resilience and appropriate third-party oversight.

### *A Culture That Makes Financial Crime More Difficult*

Culture is demonstrated through decisions and evidence. The Board should set risk appetite and oversee material exposures, incidents, backlogs, control limitations, assurance results, overdue remediation and resources. Senior management should assign accountability, remove obstacles and ensure timely remediation. Staff should understand how to identify, escalate and document relevant concerns.

### **The Takeaway for Nigerian Banks**

The strength of a financial-crime framework should not be measured solely by alert volumes, STR volumes or regulatory examinations. Management should consider whether controls reduce exposure, identify suspicious behaviour earlier, disrupt unlawful flows, protect customers, produce useful intelligence and remediate weaknesses.

The strategic objective is a financial system that is increasingly difficult and unattractive for criminals to misuse while remaining accessible, innovative and efficient for legitimate customers and businesses. Strong financial-crime controls are not an alternative to good banking. When proportionate and effective, they safeguard the institution, its customers, shareholders and the integrity of Nigeria's financial system.



# Sanctions Screening in Nigeria: Can Your Institution Demonstrate That Its Controls Work?

**F**or Nigerian financial institutions, sanctions screening is not merely a technology control or a regulatory formality. It is a core component of the broader AML/CFT/CPF framework. The decisive test is whether the institution can identify applicable designations promptly, prevent prohibited activity, investigate potential matches consistently, implement required freezing measures without delay, and make the necessary reports while preserving a reliable audit trail.

A framework may expose an institution to regulatory, financial, operational, correspondent-banking and reputational risk where it is poorly designed or ineffectively implemented. Accordingly, The Boards, Senior Management and Chief Compliance Officers should look beyond the existence of a policy or screening engine and require evidence that the end-to-end control works against the institution's actual customer, product, channel, geographic, payment and trade-finance risks.

## The Nigerian Sanctions Compliance Framework

Nigeria's targeted-financial-sanctions framework includes the Terrorism (Prevention and Prohibition) Act 2022; the Regulation for the Implementation of Targeted Financial Sanctions on Terrorism, Terrorism Financing and Other Related Measures 2022; the separate 2022 Regulation addressing targeted financial sanctions relating to proliferation financing; the CBN AML/CFT/CPF Regulations 2022; applicable CBN TFS Guidelines; the United Nations Consolidated Sanctions List; and the Nigerian Sanctions List.

The CBN's regulatory reminder dated 17 April 2025 called on banks, Payment Service Banks and other financial institutions to maintain robust and dynamic sanctions-compliance frameworks, respond promptly to applicable list changes, prevent their systems from being used for transactions involving designated persons or entities, conduct real-time screening of customers, transactions and beneficial

owners, file appropriate reports with the NFIU and notify the CBN where necessary.

At the international level, FATF Recommendation 6 addresses targeted financial sanctions relating to terrorism and terrorist financing, while Recommendation 7 addresses targeted financial sanctions relating to proliferation. These obligations should be understood alongside the risk-based approach in Recommendation 1, customer due diligence and beneficial ownership requirements in Recommendations 10, 24 and 25, payment transparency under Recommendation 16, internal controls under Recommendation 18 and suspicious transaction reporting under Recommendation 20.

## Are we screening the right parties and data?

A screening engine cannot compensate for incomplete or inaccurate customer and transaction data. The scope of screening should be determined by applicable legal obligations and the institution's risk assessment and may include applicants, customers, beneficial owners, controllers, directors, authorised signatories, connected parties, counterparties and relevant payment or trade-finance data.

For legal persons and arrangements, institutions should identify and take reasonable measures to verify the natural persons who ultimately own or control the customer. Changes in name, nationality, identification data, directorship, ownership or control should trigger appropriate rescreening and customer-risk review. Screening results should remain linked to the correct customer relationship and underlying evidence.

## Speed Matters: From List Change to Action

Designations, amendments, aliases and delistings can occur at any time. Institutions should therefore maintain a documented process for receiving,

validating, deploying and reconciling applicable list updates, with defined ownership, escalation and evidence of successful implementation.

The critical outcome is prompt implementation and, where applicable, freezing without delay and prevention of funds or other assets being made available directly or indirectly to or for the benefit of a designated person or entity. Management should understand the elapsed time from official publication to deployment, retrospective screening, investigation, restriction or freezing, reporting and closure.

### **Managing False Positives Without Creating False Assurance**

Poorly calibrated screening can produce excessive false positives, investigator fatigue and alert backlogs. Conversely, fewer alerts may reflect improved precision or may indicate thresholds, matching logic or data defects that suppress genuine matches. Alert volumes alone do not establish effectiveness.

Effectiveness testing should cover aliases, transliteration, reordered names, date-of-birth and identifier variations, ownership and control relationships, payment-message fields and relevant geographic or vessel information where applicable. Threshold changes and whitelisting should be governed, approved, documented, time-bound where appropriate and independently reviewed. Testing should assess both false positives and false negatives.

### **Investigation, Escalation, Freezing and Reporting**

A potential match is the start of the control process, not its conclusion. Written procedures should define alert prioritization, information gathering, comparison of identifiers, escalation criteria, decision authority, quality assurance, record keeping and service standards. Investigators should document both the evidence considered and the rationale for disposition.

Where a true match or relevant legal prohibition is established, the institution should implement the action required by applicable law, including restriction or freezing without delay, prohibition on making funds or services available, reporting to the appropriate authority, and preservation of confidentiality. Where suspicion of ML, TF or PF

arises, the institution should consider its separate STR obligations. A sanctions alert should not be treated automatically as an STR without the required assessment.

Procedures should also address false matches, funds frozen in error, delistings, authorised access to frozen funds, attempted transactions, rejected or blocked payments, regulator requests and prohibited disclosure. Legal and Compliance functions should be engaged where the applicable obligation or ownership/control analysis is uncertain.

### **Governance: Technology Supports the Control but Does Not Own the Risk**

The Board and senior management should approve the institution's sanctions-risk appetite and receive decision-useful information on material exposures, confirmed matches, attempted activity, backlogs, overdue investigations, list-update performance, control limitations, system changes, testing results and remediation.

Institutions should establish a documented RACI across business units, Operations, Compliance, Technology, Legal and Internal Audit. Technology should support reliable integration, access control, resilience and change governance. Compliance should provide subject-matter oversight and challenge. Operational owners should execute the control. Internal Audit or another suitably independent function should test design and operating effectiveness.

### **Technology, Integration And Evidence**

Screening effectiveness depends on more than automation. Institutions should assess system coverage, data lineage, completeness, timeliness, interface reconciliation, access rights, change management, audit trails, resilience and the treatment of manual workarounds. Integration should reflect the institution's actual channels and risks, including onboarding, core banking, payments, digital platforms, correspondent banking, trade finance, international transfers and beneficial-ownership records.

Any reference to a specific CBN automated-AML standard should be supported by the instrument's exact title, date and provision. Regardless of the technology used, the institution must be able to demonstrate how the control operates from input

data and list update through alert generation, investigation, action, reporting and independent assurance.

*Seven warning signs requiring management attention:*

- Applicable sanctions-list updates depend on uncontrolled manual steps or cannot be reconciled to successful deployment.
- Screening omits relevant beneficial owners, controllers, connected parties or transaction fields required by the institution's legal and risk framework.
- Changes to material customer or ownership data do not trigger appropriate rescreening.
- Alerts exceed approved service standards, and management cannot explain or remediate the backlog.
- Management relies only on alert volume or false-positive rate and does not test false negatives or missed-risk scenarios.
- Thresholds, matching logic, whitelists or overrides are changed without documented governance and independent challenge.
- The institution cannot evidence the complete path from designation or list update to identification, restriction or freezing, reporting and closure.

These indicators do not, by themselves, prove a regulatory breach. They should trigger prompt risk assessment, root-cause analysis, accountable remediation and escalation proportionate to materiality.

**Conclusion: Evidence is The Real Test**

As Nigeria sustains its AML/CFT/CPF reforms and prepares for future GIABA scrutiny, Boards, Chief Compliance Officers and senior management should apply a simple test: if a designated person or entity attempted to establish a relationship or execute a transaction today, or if an existing customer or beneficial owner became designated, could the institution identify the exposure, take the legally required action and prove every step?

A credible answer requires evidence of current lists, reliable customer and ownership data, appropriate transaction and payment screening, effective matching logic, prompt investigation, lawful freezing or restriction, accurate reporting, clear governance, adequate resourcing, auditable records and independent testing. The objective is not merely to operate a screening system. It is to demonstrate that the sanctions-control framework works.

[www.accobin.org.ng](http://www.accobin.org.ng)

[exec.sec@cccobin.org.ng](mailto:exec.sec@cccobin.org.ng)

+234 806 918 7180

First Floor, Front Wing, Union Bank Building,  
609 Obafemi Awolowo Way, Alausa, Ikeja, Lagos