SIXTH EDITION

ACCOBIN
Association of Chief Compliance Officers of Banks in Nigeria
Transparency, Integrity & Ethics

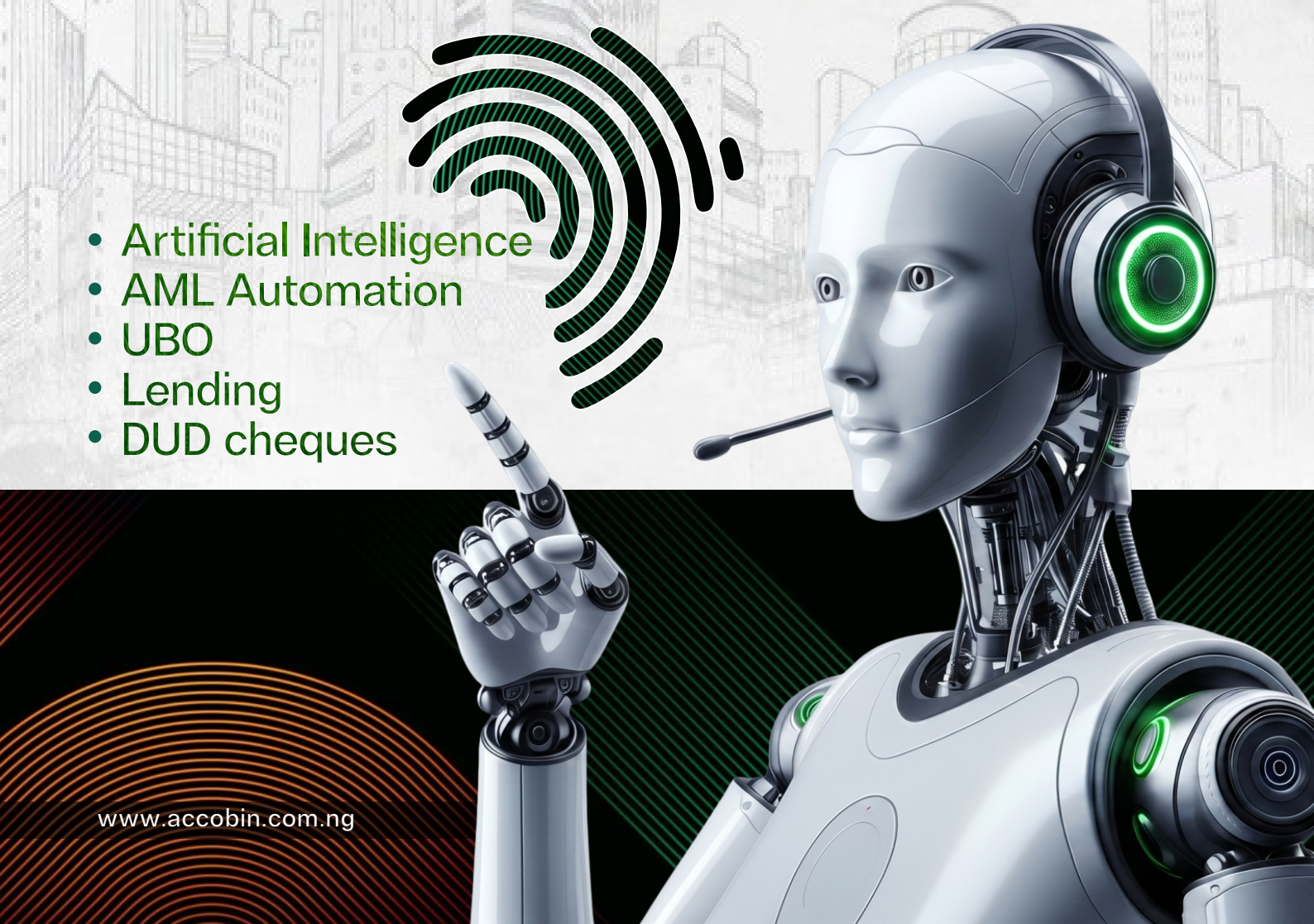
COMPLIANCE DIGEST

NEWS LETTER

MAY 2026

COMPLIANCE IN THE DIGITAL AGE – MAINTAINING STANDARDS, COMPLIANCE CULTURE, AND AUTOMATION.

- Artificial Intelligence
- AML Automation
- UBO
- Lending
- DUD cheques



www.accobin.com.ng

Table Of Contents

Artificial Intelligence, Deepfakes, and the New Face of Financial Crime:

Is Nigeria Ready?

The meeting lasted less than ten minutes.

On the screen sat what appeared to be senior executives of a multinational company discussing an urgent financial transaction. The faces were familiar. The voices sounded authentic. The instructions were clear.

The employee followed the directive and processed the transfer. Hours later, the truth emerged: None of the executives in the virtual meeting were real.

The entire interaction had been generated using Artificial Intelligence-powered deepfake technology. What once belonged in Hollywood movies has now entered the daily reality of financial crime. And for compliance professionals across Nigeria and beyond, the implications are profound.

For decades, financial crime was largely associated with forged signatures, suspicious cash movements, insider collusion, fake documents, phishing emails, and identity theft. Today, however, a new generation of criminals is emerging one armed not with weapons, but with algorithms, synthetic identities, voice-cloning tools, and AI-generated deception.

The battlefield has changed, and many institutions are still fighting yesterday's risks.

The Age of Digital Deception

Artificial Intelligence is undoubtedly one of the greatest technological breakthroughs of our time. Across industries, it is improving efficiency, automating processes, enhancing customer experiences, and transforming decision-making:

- Banks are using AI for transaction monitoring.
- Fintechs are using AI for customer onboarding.
- Businesses are using AI for analytics and automation.

But criminals are learning just as quickly.

Today, freely available AI tools can clone a person's voice within minutes using short audio samples from social media videos, interviews, or online recordings. Deepfake technology can generate highly realistic videos capable of imitating facial expressions, speech patterns, and even emotional tone.

The frightening reality is this:
Seeing is no longer believing. And increasingly, hearing is no longer proof.

Globally, cybersecurity and fraud monitoring reports continue to warn about the rise in AI-enabled financial crime. Financial institutions have become primary targets because trust, speed, and digital access are at the centre of modern banking operations. Fraudsters understand this perfectly.2.

A New Generation of Criminals:

The traditional fraudster once needed forged documents, stolen cheque books, or physical access to systems. The modern criminal may only need a laptop, internet access, publicly available data, and AI software. The tools have changed dramatically.

Today's criminals can:

- Generate fake identity documents.
- Create synthetic customer profiles.
- Manipulate facial verification systems.
- Produce convincing executive deepfakes.
- Launch personalized phishing campaigns using AI-generated language.
- Clone voices to authorize fraudulent payments.
- Use automation to scale scams globally within hours.

In many cases, institutions do not immediately realize they have been compromised because the deception appears authentic. This is what makes AI-driven fraud especially dangerous: it attacks the foundation of trust.

Nigeria's Expanding Digital Economy

Nigeria's financial ecosystem has experienced a remarkable transformation in recent years:

- Digital banking has expanded rapidly.
- Fintech innovation continues to attract global attention.
- Instant payments have become routine.
- Virtual onboarding has accelerated financial inclusion.
- Agent banking networks have grown significantly across the country.

These developments represent important progress for the economy. However, every advancement in technology also creates new vulnerabilities.

Nigeria already faces persistent challenges involving cybercrime, identity theft, insider abuse, SIM swap fraud, account takeovers, social engineering, and mule account syndicates. Artificial Intelligence now introduces a more sophisticated layer to these threats:

- **Scenario A:** Imagine a fraudster combining stolen customer information with AI-generated identity documents and manipulated facial verification technology to open fraudulent accounts digitally.

- **Scenario B:** Imagine a cloned executive voice instructing a hurried employee to bypass controls during a "sensitive transaction."

- **Scenario C:** Imagine deepfake video calls being used to impersonate regulators, auditors, or senior management.

These scenarios are no longer theoretical. The future of financial crime has already arrived.

Why Traditional Compliance Models Are No Longer Enough

One of the greatest risks facing institutions today is relying on compliance systems designed for an earlier era.

Traditional compliance frameworks focused heavily on rules, checklists, and historical transaction reviews. While these remain important, modern threats now require faster, more intelligent, and technology-driven responses. The compliance officer of the future cannot operate solely as a policy administrator; the role is evolving into something far more strategic.

Today's compliance professional must understand:

- Digital risk & cybersecurity threats.
- AI-enabled fraud patterns & emerging criminal typologies.
- Behavioural analytics & data intelligence.
- Technology governance.

Compliance is increasingly becoming a fusion of regulation, technology, risk management, ethics, and strategic judgment. This evolution is already reshaping expectations globally. Boards now expect compliance leaders to provide forward-looking risk insights, not merely policy updates. Regulators are paying closer attention to technology governance, AI controls, and operational resilience (the recent CBN Baseline standards guidelines speak directly to this).Institutions that fail to evolve may soon find themselves dangerously exposed.

The Human Factor Remains the Weakest Link

Ironically, despite advances in technology, financial crime still succeeds largely because of human behaviour.

- Criminals understand urgency.
- They exploit authority.
- They manipulate trust.
- They study emotions.

A deepfake succeeds because people trust familiar voices. A phishing attack succeeds because

someone acts too quickly. A fraudulent transfer succeeds because an employee fears delaying a senior executive or High-Net-Worth Individual **(HNI)** instruction.

Technology changes. Human psychology does not.

This is why compliance culture remains critically important. Institutions cannot solve AI-driven risks through software alone. They must also build environments where employees feel empowered to question unusual instructions, escalate concerns, and think critically under pressure. In many organizations, the real vulnerability is not the absence of technology it is the absence of a strong risk culture.

There have been publicly reported cases where many lost millions after employees were deceived by AI-generated executive impersonations.

Is Nigeria Prepared?

The honest answer is: Nigeria is improving, but significant gaps remain.
Financial institutions are investing more in cybersecurity, fraud monitoring systems, AML/CFT controls, and digital risk management. Regulators are also strengthening oversight around fintech operations, cybersecurity frameworks, and financial crime prevention.

Yet, the pace of criminal innovation remains alarming. Many organizations are still underestimating:

- The sophistication of AI-generated fraud.
- The speed at which deepfake technology is evolving.
- The reputational risks associated with digital deception.
- The governance implications of AI adoption.

There is also a growing talent gap. The compliance professional of tomorrow will require a completely different mindset from the compliance officer of yesterday. Technical regulatory knowledge alone will no longer be enough; continuous learning is becoming essential.

This is where institutions like the Compliance Institute, Nigeria **(CIN)** have a critical role to play preparing professionals for emerging realities through capacity building, specialized training, professional certification, and thought leadership around evolving financial crime risks.

The Future of Compliance Has Already Changed

Perhaps the greatest mistake institutions can make today is believing that AI-driven fraud is still a distant threat. It is already happening. The criminals are adapting, the technology is improving, and the attacks are becoming more convincing.
And trust the very foundation of financial systems is becoming more vulnerable.

For compliance professionals, this moment demands something deeper than technical expertise. It demands:

- Vigilance
- Adaptability
- Curiosity
- Courage
- The willingness to continuously evolve

Because in the era of Artificial Intelligence, compliance is no longer simply about regulatory obligations. It is about protecting institutional credibility in a world where reality itself can now be digitally manipulated.

And in that new world, preparedness may become the single most important compliance control of all.

Actionable Recommendations

- Strengthen verification control
- Simplement callback authentication
- Conduct deepfake awareness training
- Establish AI governance frameworks
- Test social engineering resilience

Contributed by

Bawo Egbakhumeh
CEO/Registrar @ Compliance Institute, Nigeria (CIN).

May 26th 2026

Understanding the CBN Baseline Standards for Automated AML Solutions.

The financial sector is becoming increasingly digital, and with this growth comes greater exposure to financial crimes such as money laundering, terrorism financing, fraud, and cyber-related risks. To strengthen the integrity of Nigeria's financial system, the Central Bank of Nigeria **(CBN)** recently introduced the Baseline Standards for Automated Anti-Money Laundering **(AML)** Solutions for financial institutions in Nigeria.

The new standards are designed to improve how financial institutions detect, monitor, and report suspicious financial activities using technology-driven systems rather than relying heavily on manual processes.

What Are the Baseline Standards?

The Baseline Standards are minimum compliance and technology requirements issued by the **CBN** to guide financial institutions in implementing effective automated **AML/CFT/CPF** solutions. These standards are aimed at promoting operational efficiency, regulatory compliance, and stronger financial crime detection mechanisms across the Nigerian financial system.

The standards encourage institutions to move from traditional manual compliance processes to more intelligent and automated monitoring systems capable of identifying suspicious transactions in real time.

Why Do the Standards Matter?

Financial crimes are becoming more sophisticated, and manual compliance processes alone may no longer be sufficient to effectively identify suspicious activities. Automated AML solutions help institutions strengthen their monitoring capabilities and improve compliance with regulatory requirements.

The standards are important because they help financial institutions:

- Detect suspicious transactions more effectively
- Improve customer risk assessment processes.
- Strengthen sanctions screening and monitoring
- Enhance regulatory reporting.
- Reduce operational and compliance risks.
- Promote transparency and accountability.

The framework also aligns Nigeria's financial system

with global best practices and Financial Action Task Force (FATF) recommendations.

Key Features of the New Standards

Real-Time Transaction Monitoring:
Financial institutions are expected to deploy systems capable of identifying unusual or suspicious transaction patterns promptly.

Integrated KYC and Customer Risk Profiling:
The standards emphasize the importance of linking AML systems with customer due diligence and KYC information to enable more effective risk assessment.

Sanctions and Watchlist Screening:
Institutions are expected to screen customers and transactions against sanctions lists, politically exposed persons (PEPs), and other regulatory watchlists.

Automated Reporting and Audit Trails:
The framework encourages proper documentation, case management, and reporting mechanisms to support regulatory oversight and compliance reviews.

What Should Stakeholders Know?

All stakeholders within the financial ecosystem have a role to play in supporting effective **AML/CFT/CPF** compliance and the successful implementation of the **CBN** Baseline Standards.

Financial institutions are expected to strengthen their compliance frameworks and adopt effective automated monitoring systems capable of identifying suspicious activities in real time.

Compliance officers and operational staff must ensure accurate customer onboarding, proper documentation, timely escalation of suspicious transactions, and adherence to regulatory requirements.

Customers and members of the public should also understand the importance of providing accurate information during onboarding and complying with KYC requirements, as these measures help protect the financial system from abuse by criminal elements.

Technology vendors and service providers supporting financial institutions are equally expected to ensure that compliance solutions meet regulatory expectations and maintain adequate data security standards.

Ultimately, collaboration among all stakeholders is essential in strengthening financial crime prevention efforts and promoting trust, transparency, and stability within Nigeria's financial system.

Looking Ahead

The introduction of the **CBN** Baseline Standards represents a major step toward strengthening Nigeria's **AML/CFT** compliance framework and improving the resilience of the financial sector.

As financial institutions continue to embrace digital transformation, automated compliance solutions will play an increasingly important role in protecting institutions, customers, and the broader financial system from financial crime risks.

Ultimately, strong compliance practices combined with effective technology solutions will help promote trust, transparency, and stability within Nigeria's financial ecosystem.

AML/CFT/CPF

ULTIMATE BENEFICIAL OWNER (UBO) UNDERSTANDING BENEFICIAL OWNERSHIP- WHY DIG DEEPER?

Knowing our business partners goes beyond identifying banks or company names. it means uncovering the real individuals who ultimately own or control the banks and companies we deal with. These people are called the Beneficial Owner.

Why Does This Matter?

In today's world, people sometimes hide behind complicated company ownership structures to cover up illegal activities, avoid taxes, or disguise their true identity. If we only look at the surface and fail to identify the actual people in control, we risk unknowingly enabling money laundering, terrorist financing, or proliferation financing activities.

We Dig Deeper Because:

- We need to confirm the legitimacy of businesses, corporates, and their beneficial owners.
- We must comply with **CBN,** sec, and **NFIU** regulations on transparency and due diligence.
- We're committed to ensuring that our personal or corporate funds do not indirectly benefit high-risk entites.

Report Red Flags

- Unusually complex ownership structures.
- Reluctance to disclose ownership information.
- Frequent ownership changes.
- Inconsistent documentation.
- Use of nominees or proxies.

Key Reminders

KNOW YOUR CUSTOMER AND CARRY OUT CUSTOMER DUE DILIGENCE (KYC/CDD):

Always identify and verify the real person behind a company.

DIG DEEPER WITH UBO:

Go beyond company names, identify the real individuals who ultimately own or control the account or business.

CARRY OUT CAC CHECKS:

Verify company details with the corporate affairs commission records until all beneficial owners are clearly identified.

KNOW YOUR VENDORS:

Always confirm the beneficial owner of any vendor or company deals with.

REPORT RED FLAGS:

Escalate unusual transactions or inconsistent customer behaviour to the risk management and compliance department.

Responsible Borrowing & Loan Repayment

Access to credit whether from banks, mortgage institutions, or fintech lenders can be a valuable tool for meeting financial needs.

However, it is important to ensure that all loan obligations are repaid as agreed.

The Central Bank of Nigeria **(CBN)** has emphasized the need to curb the activities of serial loan defaulters within the financial system. As part of this, financial institutions are required to:

- Conduct proper credit checks before granting loans
- Share borrower information through the Credit Risk Management System **(CRMS)**
- Report credit information to licensed Credit Bureaux

This means that loan defaults are increasingly visible across institutions, and a default with one lender may affect your ability to access credit anywhere.

Maintaining a good credit profile is therefore essential. Consistent repayment and responsible borrowing will help you:

- Preserve access to future credit opportunities.
- Maintain financial stability.
- Avoid unnecessary restrictions across financial institutions.
- Protect your financial reputation and credibility.
- **Do not borrow unless you are certain of your ability to repay as and when due.**
- Borrowers should assess their income and repayment capacity carefully before taking on financial obligations.

We are encouraged to borrow responsibly, stay on top of repayment obligations, and avoid taking on multiple loans that may be difficult to manage.

Where challenges arise, early engagement with lenders can help prevent escalation.

Financial discipline today protects your financial freedom tomorrow.

DID YOU KNOW

DUD CHEQUE AWARENESS

A DUD cheque (also known as a **bounced or dishonoured cheque**) is a payment instrument that is returned unpaid by a bank because the issuer **(the drawer)** does not have sufficient funds in their account to cover the amount.

Knowingly issuing, processing, or facilitating such transactions may constitute a **criminal offence.**

KEY FACTS!

01 Issuing or processing dud/fraudulent cheques is a criminal offence and can lead to disciplinary action, loss of employment, prosecution, and reputational damage.

02 We are advised to exercise due diligence at all times and avoid involvement in any suspicious cheque transactions.

03 Do not issue a cheque when you are unsure of your cashflow.

04 Where necessary, promptly notify the beneficiary of any issued cheque on insufficient funds before the cheque's value date.

PROTECT YOUR INTEGRITY.
PROTECT YOUR JOB. STAY COMPLIANT.

www.accobin.com.ng

exec.sec@cccobin.org.ng

5th Floor, Bankers House,
PC 19, Adeola Hopewell, Street, Victoria Island Lagos.