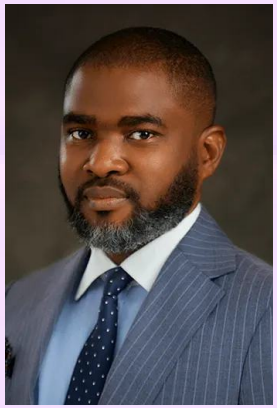
The Question Isn't "Can You Afford Compliance?" It's "Can You Afford Not To?"



Christine Sijuwade
Partner



Chisom Ndubuisi
Senior Associate



Ayooluwa Osigwe
Associate



Nigeria’s fintech sector is one of Africa’s fastest-growing digital finance markets, reshaping payments, lending, remittances, digital assets and financial inclusion. As fintech businesses increasingly perform functions associated with licensed financial institutions, Nigerian regulators are moving from primarily enabling innovation to reinforcing governance, consumer protection, market integrity and systemic stability. Compliance is therefore no longer simply a licensing requirement. It is central to operational resilience and sustainable market participation.

The sector’s growing importance has brought greater scrutiny. Regulatory breaches may result not only in financial penalties, but also operational restrictions, reputational damage and closer enforcement attention. For fintech operators, the relevant question is no longer whether compliance is affordable, but whether the business can absorb the consequences of neglecting it.



Get Started

Subscribe to our mailing list

u-law ulawsocial

REGULATORY OVERSIGHT AND FINTECH OBLIGATIONS

Fintech businesses operate within a multi-regulator environment. Depending on their activities, they may be supervised by the Central Bank of Nigeria (CBN), Securities and Exchange Commission (SEC), Nigerian Data Protection Commission (NDPC), Federal Competition and Consumer Protection Commission (FCCPC), Economic and Financial Crimes Commission (EFCC), Special Control Unit Against Money Laundering (SCUML) and Nigerian Financial Intelligence Unit (NFIU).
The precise obligations depend on the operator's services, licence and regulatory classification. Common requirements include licensing, know-your-customer procedures, anti-money laundering and counter-terrorism financing controls, transaction monitoring, cybersecurity, data protection, consumer protection and periodic reporting. Key legislation includes the Money Laundering (Prevention and Prohibition) Act 2022, CBN AML/CFT/CPF Regulations 2022, Nigeria Data Protection Act 2023, Federal Competition and Consumer Protection Act 2018, Investments and Securities Act 2025 (where applicable), and the Cybercrimes (Prohibition, Prevention, etc.) Act.

A compliance framework should therefore reflect the risks of the operator's products and business model, whether it is a payment service provider, digital lender, remittance company, switching company, crowdfunding platform, virtual asset service provider or another regulated financial service provider. A generic framework is unlikely to address the different risks arising from customer onboarding, transaction flows, data use and product distribution.



Regulatory expectations are also becoming more demanding. Between 2025 and 2026, the CBN strengthened requirements across payments, agent banking, remittances and foreign exchange markets, including through the Baseline Standards for Automated AML/CFT/CPF Solutions. The FCCPC introduced the Digital, Electronic, Online or Non-Traditional Consumer Lending Regulations 2025, while the NDPC issued the General Application and Implementation Directives 2025, addressing data governance, audits, breach reporting and Data Protection Officers.
Boards and senior management are increasingly expected to oversee compliance, enterprise risk management and financial crime controls actively. This includes ensuring that systems identify regulatory obligations, monitor compliance and escalate material deficiencies. Because mandates overlap, a weakness in customer onboarding, transaction monitoring, data governance or consumer disclosures may attract scrutiny from more than one regulator.

THE ACTUAL COST OF NON-COMPLIANCE

The cost of non-compliance extends beyond fines. Failures involving AML controls, unlicensed operations, deficient KYC procedures, data breaches, misleading lending practices or regulatory reporting may trigger sanctions. Regulators may also suspend operations, restrict products, withdraw conditional approvals or revoke licences. These measures can interrupt service delivery, weaken investor confidence and threaten continued market participation.

The commercial effects may outlast the formal regulatory action. Adverse publicity can undermine customer trust, damage relationships with banks and other financial institutions, and deter prospective investors. Remediation may also require substantial management time and resources. Compliance failures can therefore affect a fintech's reputation, access to counterparties, ability to raise capital and long-term viability.



CONCLUSION

Recent regulatory action concerning AML controls, consumer protection and operational risk management shows that supervision is becoming more proactive. Fintech businesses should identify and address deficiencies before they cause consumer harm, regulatory intervention or operational failure.

As Nigeria's fintech ecosystem matures, companies must move beyond reactive compliance and embed governance, risk management and regulatory accountability into product design and core operations. Proactive compliance protects operational continuity, customer trust, investor confidence and commercial sustainability. So, the more pertinent question is not whether a fintech can afford compliance, but whether it can afford the consequences of neglecting it.



Disclaimer

This article is provided for general information purposes only and does not constitute legal advice. The legal and regulatory considerations discussed may vary depending on the nature, structure and operations of a particular platform business. Founders should obtain specific legal advice based on their individual circumstances before taking any action.
For further information or enquiries, please contact the U-Law team at ulawteam@uubo.org"