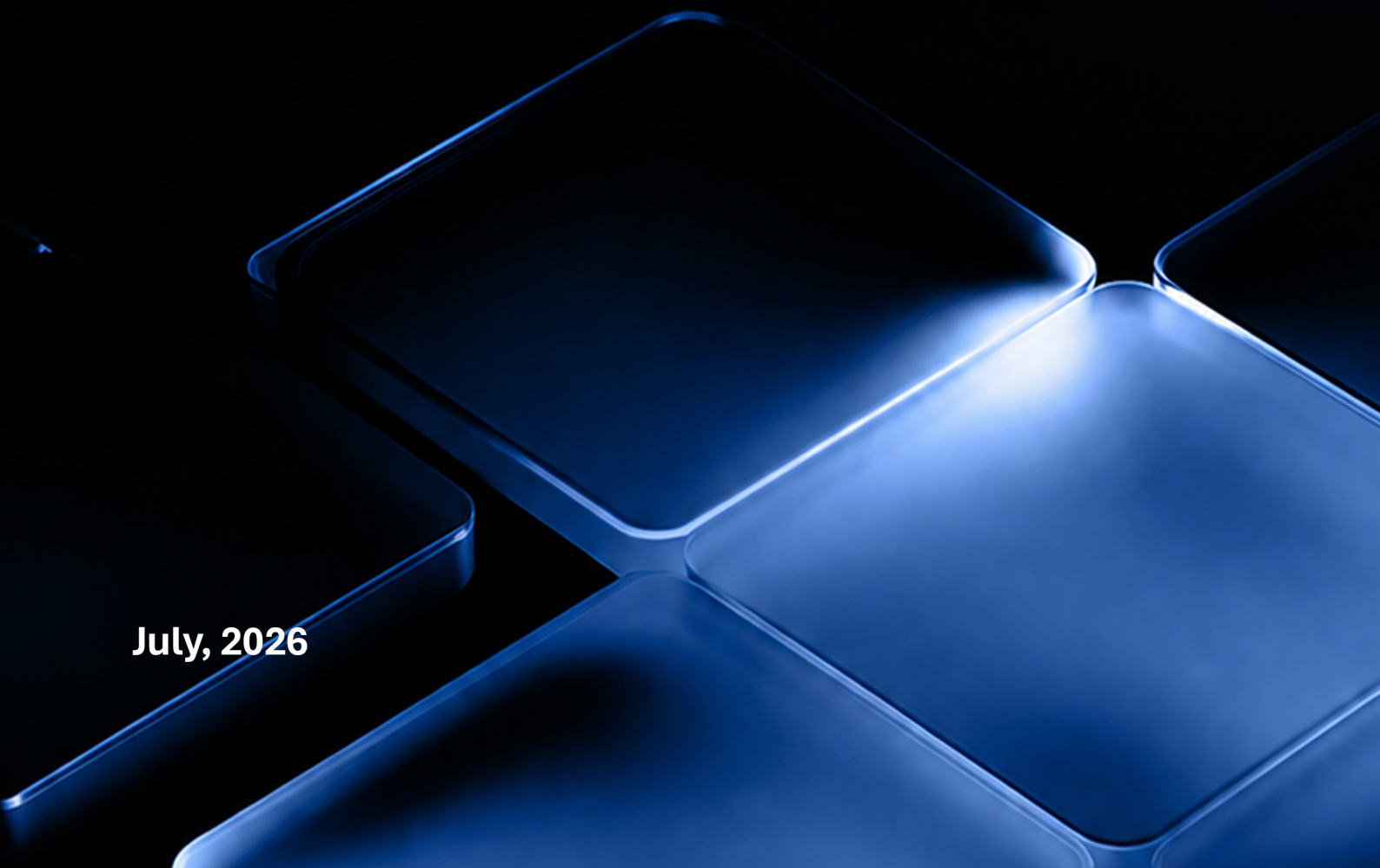
Adhere by Smartcomply

techcabal Insights

The Compliance Reckoning:

Regulating Financial Services in the age of AI



July, 2026

Table of Contents

Foreword

Africa's digital economy is no longer on the cusp of transformation; it is actively living it. Yet, as our digital footprints expand, so does the threat landscape. The frontier of business is no longer defined just by how fast we can scale, but by how securely we can sustain that growth.

Indeed, the financial-crime landscape has shifted. AI has industrialized threat networks, rendering fraud cheaper, faster, and effortlessly scalable. With global fraud losses reaching an estimated $442 billion in 2025, and AI-enhanced fraud proving 4.5 times more profitable than traditional methods, Nigeria stands at a critical inflection point. While we process over 10 billion real-time transactions annually, we rank 110th out of 112 countries for fraud protection, losing ₦52.26 billion to digital-payment fraud in 2024 amid a 90.6% cybersecurity workforce gap.

Despite this, our defense remains fragmented. While 87.5% of Nigerian fintechs report using AI for fraud detection, buying an AI-enabled compliance tool is not the same as building a defensible compliance architecture.

True institutional resilience requires moving beyond isolated software toward an integrated framework built on four capabilities: proactive detection, full-customer risk context, model governance, and cross-institutional collaboration.

As the CBN accelerates automated AML and data-localization deadlines, compliance is a leadership imperative. I urge boards, compliance officers, and tech teams to view this reckoning not as a burden, but as a historic opportunity to build the trust that will secure the future of African finance.

Gbemisola Osunrinde
Group MD, Smartcomply

Executive Summary

Nigeria's fraud landscape has changed shape. Losses fell from ₦52.26 billion in 2024 to ₦25.85 billion in 2025, but the topline decline conceals a 350% rise since 2020, despite a 31% drop in case counts. Successful attacks are now fewer, more targeted, and more costly per incident.

The TechCabal Insights (TCI) incident base documents 30 major cyber and fraud incidents in Nigeria between 2019 and 2026, with over ₦100 billion in disclosed losses. The data shows that the attack surface has migrated in three generations: from institutional perimeters, to payment infrastructure and APIs, to systemic architecture, cloud environments, and national identity systems. Nine of the 30 cases have occurred in the last twenty months.

Nigeria's regulators have moved decisively. The Central Bank has issued seventeen regulatory actions in fourteen months across cyber, data protection, and AML, with six carrying hard compliance deadlines between March 2026 and March 2028. A ₦15.42 billion fine on a leading commercial bank in 2025 signalled that non-compliance now costs institutions their international correspondent relationships alongside the penalty itself.

The operational readiness required to meet those deadlines does not yet exist. The Compliance and Cyber Resilience Index scores three of four readiness pillars below threshold. Only policy and enforcement is at threshold. The infrastructure gap is the sharpest expression of that lag. Nigeria hosts 28 data centre facilities, 75% of them in Lagos. Active load meets under 7% of what a competitive digital economy requires.

Architecture built as one connected system across institutions, regulators, and industry infrastructure is what will meet the mandates. The next eighteen months will resolve the question this report has framed.

01

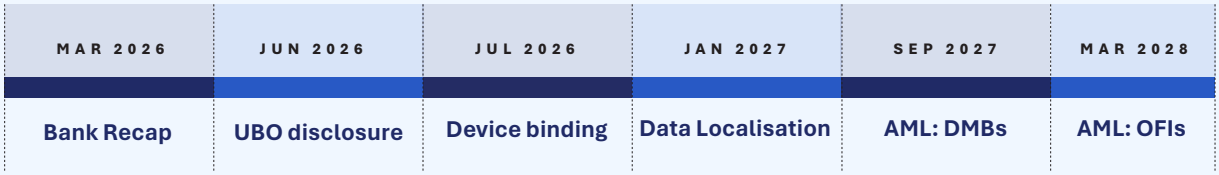
The compliance reckoning

The compliance reckoning

Three strategic currents are converging on Nigerian financial services inside a single eighteen-month execution window: AI as simultaneous threat and defence, seventeen CBN regulatory actions in fourteen months, and operational readiness that has not kept pace.

Three strategic currents

The execution window



Source: CBN

AI has collapsed the cost structure of financial crime and, simultaneously, become the only technology capable of defending against it at machine speed. The CBN has responded with seventeen regulatory actions in fourteen months, six of them carrying hard compliance deadlines between September 2027 and March 2028. The operational foundations required to absorb both currents, spanning talent, data integrity, cloud infrastructure, and model governance, are running materially behind the pace the mandates assume.

What this report argues

The institutions that come through the next eighteen months intact will not be the ones with the best AI tools. They will be the ones with the architecture around those tools. The threat has changed shape. Fraud is now industrialised, automated, and targeted at the verified customer rather than the perimeter. The Central Bank of Nigeria's (CBN) response is a system, not a purchase.

The report measures readiness against that system across four pillars: infrastructure, meaning where data lives and how resilient it is; talent, meaning who can build and govern the models; policy and enforcement, meaning how the rules are tightening and where they bite; and incident response, meaning how fast institutions detect, contain, and recover.

Four Pillars of Readiness

Infrastructure
Data Centres, cloud, resilience

Talent
Cybersecurity professionals, people who build and govern AI,

Policy and Enforcement
How the rules are tightening and enforced

Incident Response
Prevent, detect, contain, recover

Our research approach

This report is built on three evidence streams, each informing every pillar of the compliance and cyber resilience Index.

Quantitative secondary data analysis:	We analysed secondary data across NIBSS annual and quarterly fraud reports, CBN regulatory circulars, sector publications, and institutional disclosures, tracking fraud losses, case counts, channel composition, and the regulatory action calendar to establish the quantitative baseline against which the report's argument is measured.
The empirical case base:	We compiled and analysed 30 major cyber breaches and fraud incidents in Nigeria between 2019 and 2026. The case base tracks how attack vectors migrated from simple website defacements to sophisticated API exploitation, ransomware, cloud misconfigurations, and systemic infrastructure leaks.
Sector interviews:	We conducted semi-structured interviews with technical leaders actively managing risk in the field, including data centre providers on physical hosting capacity and cloud storage architecture, and compliance leaders on live AI-driven countermeasures and modern incident response frameworks, amongst others.

02

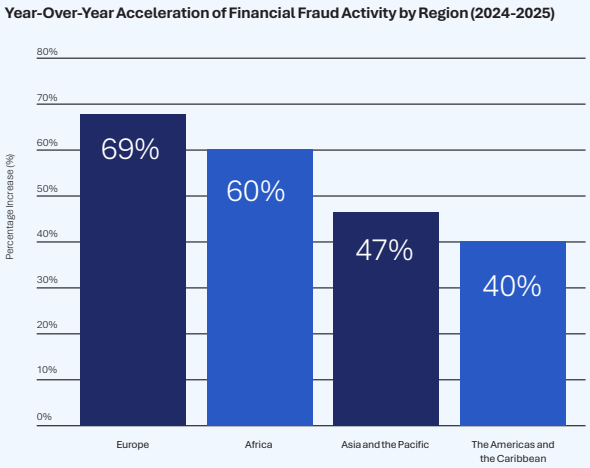
The AI threat landscape

AI has lowered the cost of fraud and raised its scale.

The financial crime confronting Africa's institutions in 2026 is not the same crime they built their defences to stop. Generative AI has collapsed the cost structure of fraud, industrialised identity theft, and introduced attack vectors that most compliance teams have never encountered.

Source: *Interpol*

Africa's fraud acceleration in 2024-2025 was second only to Europe globally



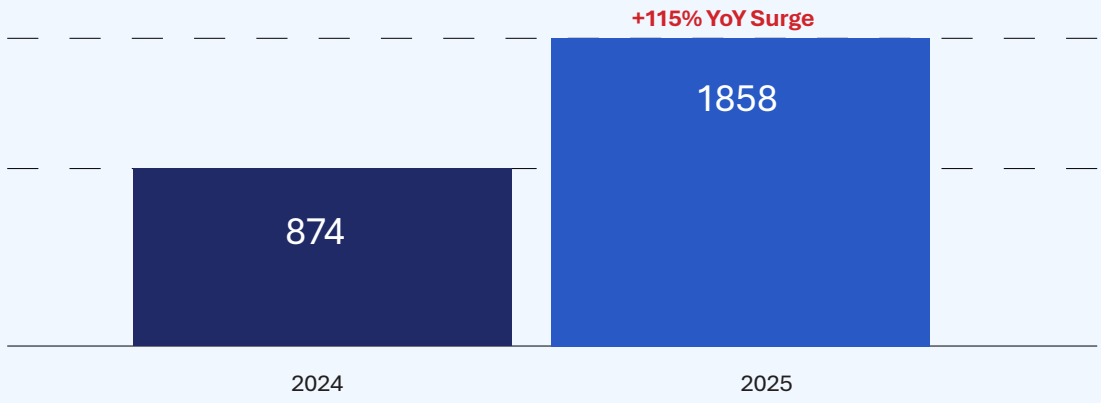
Global financial fraud losses reached an estimated $442 billion in 2025, according to INTERPOL's 2026 Global Financial Fraud Threat Assessment. That figure alone exceeds the nominal GDP of Nigeria in 2025 and of most other African economies. AI-enhanced fraud is now 4.5 times more profitable than traditional methods, and "agentic AI" systems (AI fraud agents) can now autonomously plan and execute entire fraud campaigns, from target reconnaissance through to ransom delivery, without human intervention. Financial fraud now sits among INTERPOL's top five global crime threats, with fraud-related Notices and Diffusions rising 54% between 2024 and 2025.

Institutions are no longer defending against individual fraud attempts, they are defending against automated fraud production systems.

Cyberattacks against financial institutions have more than doubled

Financial services is now a high-value and high-frequency target. The 115% surge reflects a structural shift toward industrialised campaigns with the sector at the centre.

Global CyberattacksTargeting Financial Institutions



Financial Institutions are now both high- value targets and high -frequency attack surfaces

Sources: Check Point 2025 financial threat landscape report

Cyberattacks targeting financial institutions globally more than doubled in 2025, surging 115 per cent from 864 incidents to 1,858, according to Check Point's 2025 Financial Threat Landscape Report. Financial services ranked among the three most attacked industries in Africa throughout the year. The scale reflects a structural shift in how fraud and cyber campaigns are now run: industrialised, automated, and directed at verified customers rather than the perimeter, with the financial sector at the centre.

"The largest gap we see is between AI use for offensive security and AI use for defensive security, with adoption running well ahead on the attack side. A 2026 survey of 1,200 cybersecurity professionals found AI tools deployed at 73 percent of organisations but real-time governance in place at only 7 percent. Trust-building on the defence side is inherently slower than attackers adopting new tools, because a false positive that blocks a legitimate deployment carries real operational cost, while an attacker experimenting with a new technique carries little downside if it fails."

Victor Ikiugu
Head of Security, Paystack

The offence-defence adoption gap is the mechanism through which surging attack volume translates into successful compromise. Closing it is a governance problem before it is a tooling problem.

Africa is absorbing a disproportionate share of the cost

The continental cost signature between 2019 and 2025 places Africa above the global mean on incidence, share of criminal activity, and per-breach cost.

30%
Reported offences in West & East Africa attributed to cybercrime

$3B+
Cumulative African cyber losses 2019-2025

12.9%
African B2B finance organisations affected by ransomware

$2.37M
Average data-breach cost South Africa, 2025

Sources: INTERPOL Africa cyberthreat assessment 2025; Kaspersky security bulletin 2025; IBM cost of a data breach report 2025

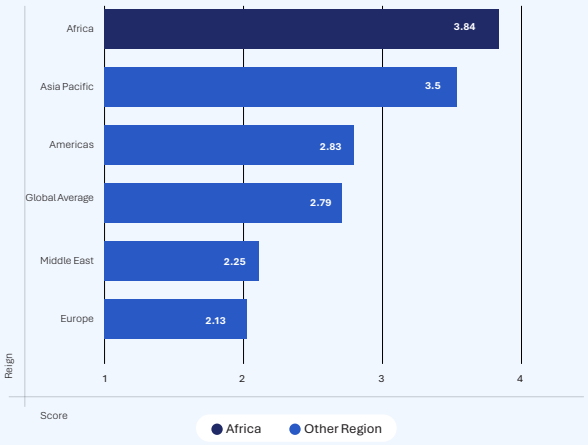
Cumulative continental cyber losses between 2019 and 2025 exceeded $3 billion, according to INTERPOL's Africa Cyberthreat Assessment. Cyber-related crimes now account for approximately 30% of all reported offences in West and East Africa. Kaspersky's 2025 security bulletin found that 12.9% of B2B finance organisations in Africa were affected by ransomware between November 2024 and October 2025, effectively matching the global rate. The average cost of a data breach in South Africa reached $2.37 million in 2025, according to IBM's annual analysis, with financial sector breaches remaining the world's second costliest after healthcare.

Africa is at the centre of global fraud exposure

Africa scores materially above the global average in Sumsub's 2025 fraud exposure index, with several African markets sitting among the least protected countries in the index

Africa is the world's most fraud-exposed region

Sumsub Global Fraud Index Score by Region, 2025. Higher score indicates greater fraud exposure



Sumsub's 2025 Global Fraud Index assessed 112 countries

Country risk strip: bottom six least protected from digital fraud

Least protected countries	Country
112	Pakistan
111	Indonesia
110	Nigeria
109	India
108	Tanzania
107	Uganda

Source: Sumsub 2025 Global Fraud Index.

Africa's fraud exposure is structurally above the global benchmark. Africa's regional fraud exposure score of 3.84 is roughly 38% higher than the global average of 2.79, making it the most exposed region in Sumsub's 2025 index. Nigeria, Tanzania and Uganda sit inside the global bottom six for fraud protection, showing that Africa's exposure is regional, not just country-specific .

Sub-Saharan Africa also reported the highest regional exposure to cyber-enabled fraud in the World Economic Forum's 2026 survey. 82% of respondents reported direct or network-proximate exposure in the prior 12 months.

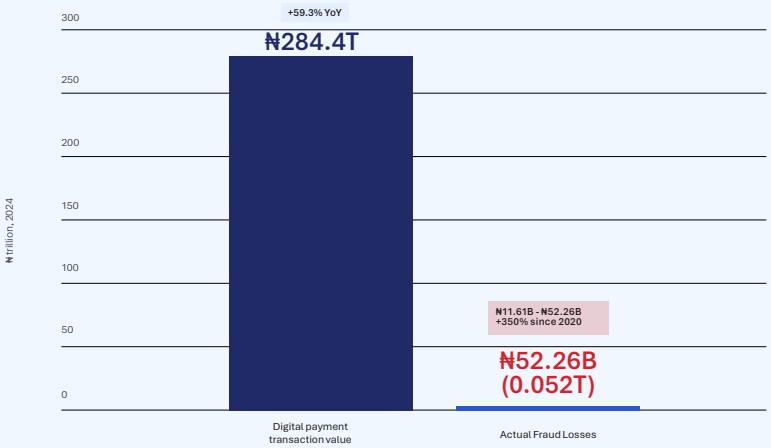
Africa's fraud challenge reflects a protection gap: digital and financial adoption are outpacing the institutional, regulatory and verification systems built to secure them.

Nigeria's payment scale has grown faster than its fraud-protection architecture

Nigeria combines the continent's highest digital transaction volume with one of the world's weakest fraud protection scores, creating the highest-value, and lowest-friction target for AI-driven financial crime in Africa.

Nigeria is at the Epicentre of Africa's Fraud Exposure

The continent's largest real-time payments market is also one of the world's least fraud-protected



What the scale gap shows

Fraud losses equal just 0.018 per cent of transaction value, so the bar for losses almost disappears on a true scale. The absolute loss figure is nonetheless staggering and has grown 4.5 times since 2020.

The mismatch between payments growth and defensive architecture, not fraud volume itself, is where the exposure sits.

4,622
Cyberattacks per week, per organisation

110th of 112
Global fraud protection rank (Sumsub 2025)

10B+
Annual real-time payment transactions.

$6B
Projected fintech GDP contribution, 2026.

Sources: NIBSS, Check Point Research, Sumsub, CBN , Chambers and Partners Fintech

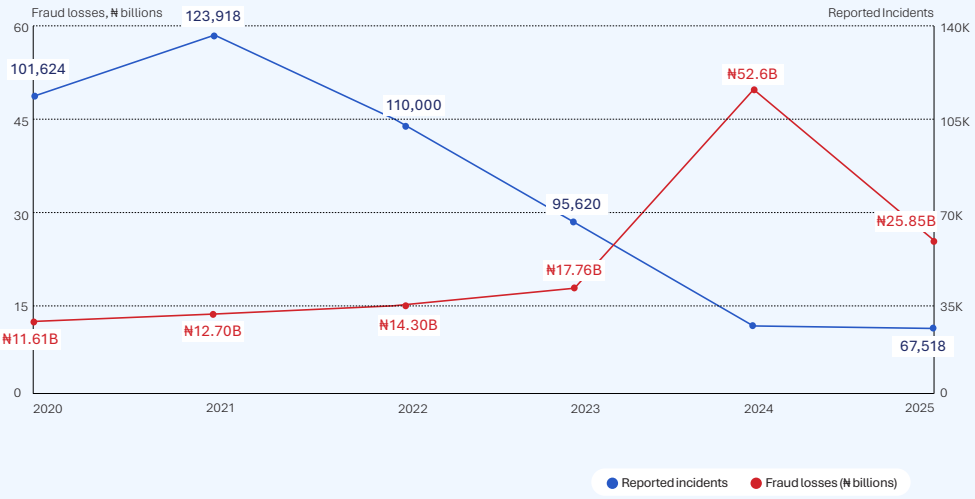
The value of electronic payment transactions in Nigeria surged 59.3% in 2024 to reach ₦284.4 trillion. Against a market that ranks 110th of 112 countries for fraud protection and where organisations face 4,622 cyberattacks per week, this scale creates the highest-value and lowest-friction target on the continent. NIBSS data makes the cost visible: Nigerian financial institutions lost ₦52.26 billion to digital payment fraud in 2024, a 350% increase over four years even as reported case counts fell 31%.

Nigeria's fraud paradox: fewer incidents, higher severity

The decline in fraud losses reflects a change in the shape of the threat.

Digital payment fraud losses vs reported incidents

Nigeria, 2020 to 2025



NIBSS 2025 industry data identifies social engineering, SIM swap, account compromise, and phishing as the fastest-evolving techniques driving these losses, all of which target the verified customer rather than the institutional perimeter.

Source: NIBSS, TechCabal

Digital payment fraud losses fell to ₦25.85 billion in 2025, a 51% decline from ₦52.26 billion in 2024, according to NIBSS. The 2024 figure was distorted by a single ₦31.1 billion incident. Stripped of that distortion, underlying 2024 losses would have been closer to ₦21 billion, meaning 2025 losses exceed the underlying 2024 baseline by roughly 23%.

The topline decline conceals a rising underlying trend rather than evidence of stronger fraud resilience.

Nigeria's cyber threat has moved from the institutional perimeter to the financial system itself

Our analysis of 30 major Nigerian cyber and fraud incidents between 2019 and 2026 shows the attack surface has migrated from perimeter breaches to payment infrastructure exploitation and, more recently, verified customer journeys.

Structural weakness account for 60% of documented incidents

Attack taxonomy accross 30 major Nigerian cyber and fraud incidents, 2019 to 2026

Systemic vulnerabilities and cloud misconfigurations	9 Cases	30%
Data leakage and database breaches	9 Cases	30%
Direct operational fraud and monetary siphoning	5 Cases	16.7%
Phishing, identity theft, and access hijacking	3 Cases	10%
Ransomware and destrutive extortion	2 Cases	6.7%
Web surface disruptions	2 Cases	6.7%

₦100B+
Disclosed losses across 10 of 30 cases.

Note: Cases are assigned to the primary attack vector. Some incidents involve multiple techniques and are categorised by the mechanism that produced the primary impact. Rounding may cause totals to differ from 100% by 0.1.

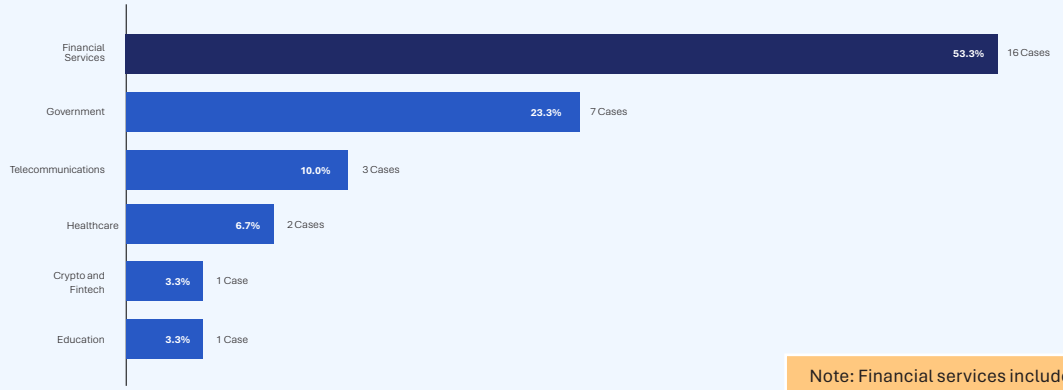
Source: TechCabal Insights 30-case incident base, 2019 to 2026.

The incident base tracks three generations of attack, each a response to the defensive posture of the one before. Generation one (2019 to 2021, six cases) targeted the institutional perimeter through database leaks and website breaches. Generation two (2022 to 2024, fifteen cases and half the dataset) shifted to payment infrastructure and API exploitation as institutions hardened their perimeters. Generation three (2025 to 2026, nine cases) has moved further inward to identity and infrastructure attacks, and it has produced nearly a third of the six-year dataset in under two years. Financial services and government together account for 77% of all cases, meaning the exposure is concentrated in the two sectors most central to national infrastructure.

Individual institutional readiness is a necessary but insufficient condition for sector resilience, because weakness in one node creates risk across the connected nodes.

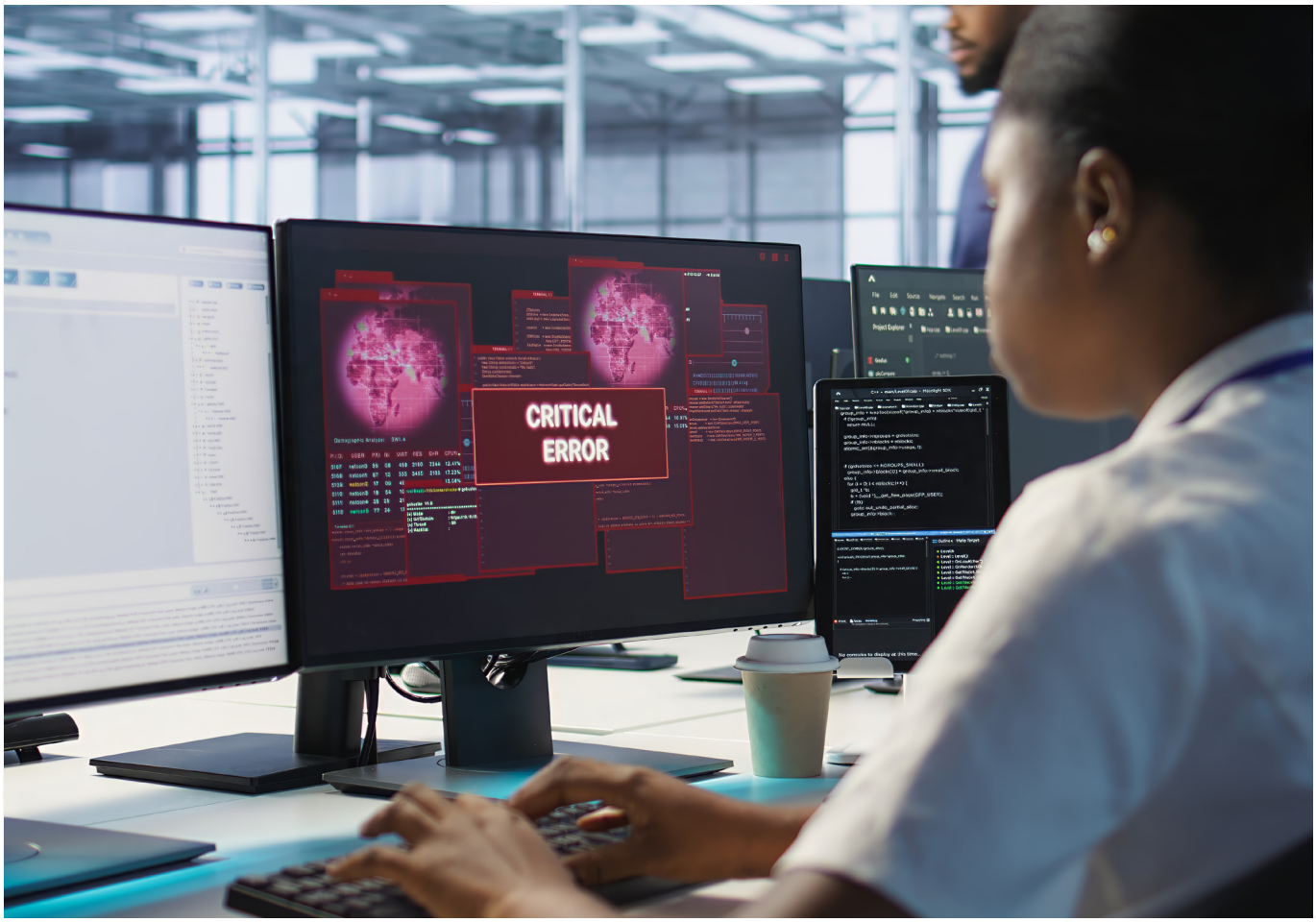
Financial services carries more than half of documented incidents

Sector distribution across 30 major Nigerian cyber and fraud incidents, 2019 to 2026



Note: Financial services includes commercial bank, fintechs, and payment infrastructure. Rounding may cause totals to differ from 100% by 0.1.

Source: TechCabal Insights 30-case incident base, 2019 to 2026.



The attack surface has moved from institutional systems into payments, identity and critical infrastructure

The three-generation pattern is not just a chronology. Each generation shows attackers moving one layer deeper into the systems that enable identity, trust, and payments.

Source: TechCabal Insights analysis

The evolution in attack objectives matters more than the evolution in technique. Generation one attackers pursued data. Generation two pursued money. Generation three pursues operational control of the systems that enable both. A successful breach no longer just exposes information. It can compromise payment integrity, customer trust, and operational continuity across sectors that depend on the same identity and payment infrastructure.

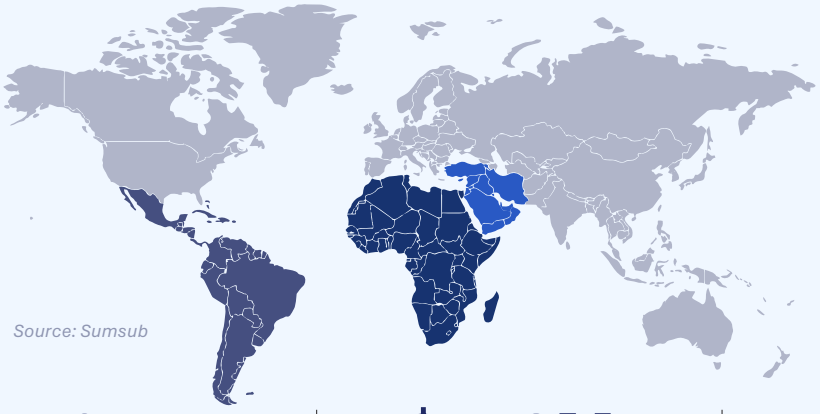
Customer journeys, payment rails, identity systems, and cloud infrastructure now function as one connected risk environment.

Deepfake fraud is no longer an emerging risk. It is a production-scale threat.

The single most consequential development in financial crime over the past 18 months is the weaponization of deepfake technology against identity verification systems. Deepfake incidents in Africa rose 393% year-on-year in 2025, acoording to Sumsub,

Deepfake incident growth is concentrated across three exposed regions

YoY growth indicators from Sumsub reporting



Source: Sumsub

+643% Fasted growing region
Middle East

+393% High-exposure digital markets
Africa

+255% Rising verification pressure
Latin America

11%
of top first-party identity fraud schemes are deepfakes

$410M
global reported deepfake fraud losses, H1 2025 (Surfshark)

+40%
financial professionals have encountered deepfake fraud (Deloitte)

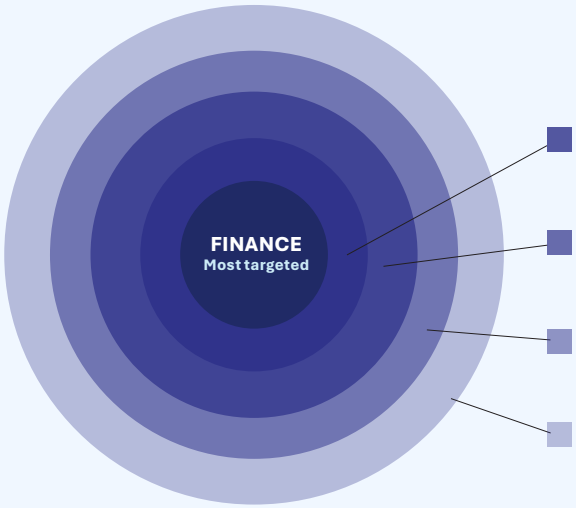
Sources: Sumsub, Surfshark, Deloitte

Deepfake fraud is no longer an experimental threat. Smile ID's 2025 Digital Identity Fraud in Africa Report documented a single syndicate using 100 stolen faces to launch 160,000 verification attacks in a single month, and the marginal cost of producing a convincing synthetic identity has fallen to near zero. The global map matters to Nigerian institutions because these attack patterns travel. A synthetic identity tactic proven in one high-volume market becomes deployable against banks, fintechs, wallets, and agent networks in every other. Nigeria's scale makes it a proving ground.

The evidence indicates that deepfake detection now sits inside the core financial-crime infrastructure question rather than adjacent to it.

Social engineering at scale

Finance is the most targeted sector across Africa, and AI has lowered the cost, raised the speed, and reduced the detectability of every attack vector.



PHISHING
80% AI-assisted
ENISA, Sep 2024 - Feb 2025

BEC ATTACKS
11 African countries
As principal hubs

SIM-SWAP FRAUD
R5bn annual cost
In South Africa alone

BANKING TROJANS
196% global surge
In smartphone attacks

Nigeria specific indicators

66%
Increase in password stealing attacks

53%
Rise in spyware detections

46%
Rise in finace-targeted phishing

Sources: ENISA, Kasperky, COMRiC

AI has changed how both humans and machines are deceived. Over 80% of phishing emails analysed by ENISA between September 2024 and February 2025 used AI in some capacity. Kaspersky's data shows a 66% year-on-year increase in password-stealing attacks in Nigeria in the first half of 2025, alongside a 53% rise in blocked spyware and a 46% increase in finance-targeted phishing.

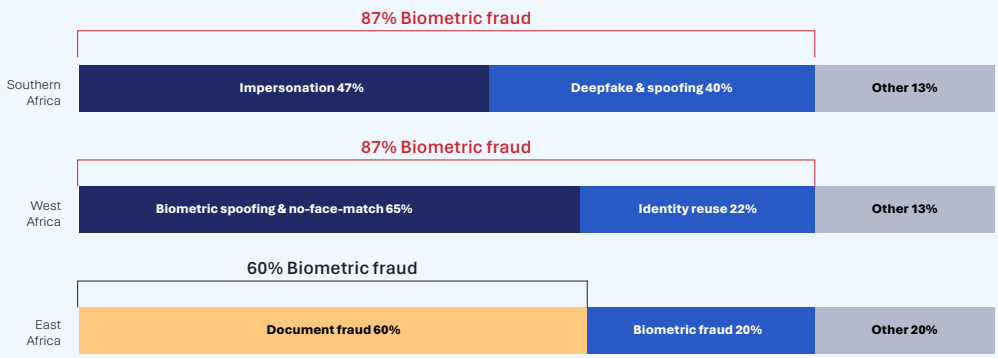
Across Sub-Saharan Africa, 42.4 million web attacks and 95.6 million on-device attacks were detected in the first six months of 2025. Finance is the most impacted sector by BEC attacks in Africa, according to Kaspersky, with Nigeria, Ghana, Côte d'Ivoire, and South Africa among the principal hubs.

AI has made every phishing email more personalised, voice clone more convincing, and campaign execution costs materially lower. The human layer, not the technical stack, remains the most exploited vulnerability in Africa's financial infrastructure.

Biometric fraud tracks the verification method

The dominant fraud vector tracks the underlying verification method. Fraudsters attack the method that dominates the market.

Verication rejection composition by region, 2025



200M+

Identity checks analysed across 35 African countries (Smile ID)

Sources: Smile ID's 2026 Digital Identity Fraud in Africa Report

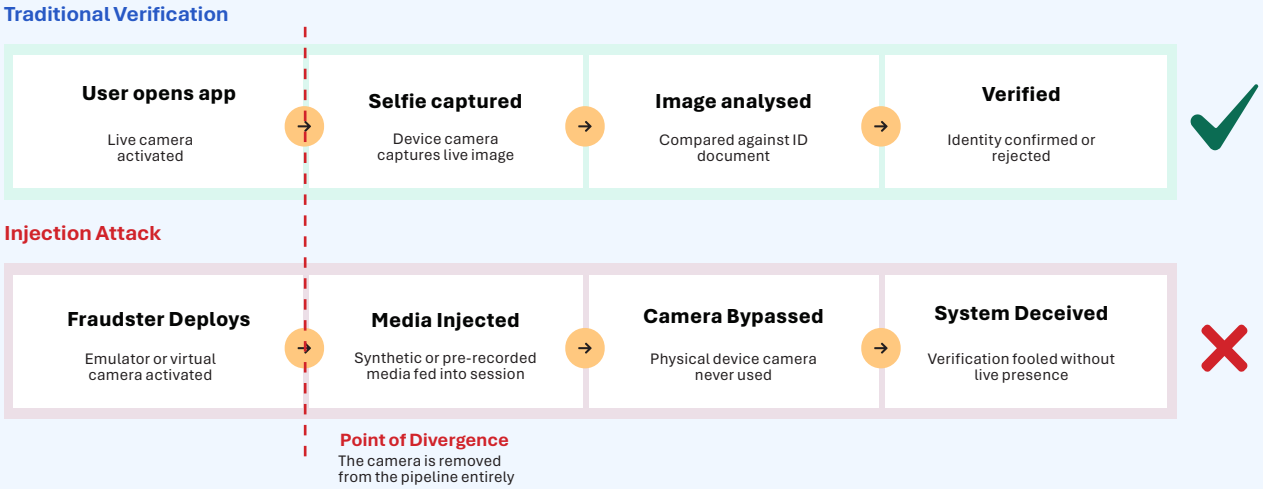
In Southern and West Africa, where biometric verification dominates, 87% of rejected verifications in both regions are linked to AI-assisted biometric fraud. In East Africa, where ID card-based verification still leads, document fraud accounts for 60% of rejections. East Africa is not less targeted: Kenya recorded 4.5 billion cyber threat events in 2025 and Tanzania saw deepfake fraud surge 317%. The attack surface shifts with the verification method.

As Nigeria's verification stack moves further towards biometric and signal-based systems under the CBN's mandates, the evidence indicates the fraud composition will shift with it.

The battleground has shifted from onboarding to authentication

How injection attacks Bypass Verification

The traditional pipeline assumes a live camera. Injection attacks remove the camera entirely



5x
more authentication fraud than onboarding

90%
of fraud blocked by mobile SDK signals, not image analysis

100,000+
Injection attacks per month (2025)

Sources: Smile ID's 2026 Digital Identity Fraud in Africa Report

Authentication fraud attempts now exceed onboarding fraud by more than five times. Attackers are operating within verified accounts, targeting login flows, account recovery, and high-value transactions. Nearly 90% of fraud blocked in 2025 was triggered by mobile SDK signals rather than by image analysis, indicating the defensive layer that catches most contemporary attacks is device signal telemetry. Injection attacks, which bypass the device camera entirely, now exceed 100,000 per month.

Institutions still relying on selfie-based liveness checks alone are defending against yesterday's threat. And even where liveness verification holds, the most material escalation practitioners now observe goes around it entirely.

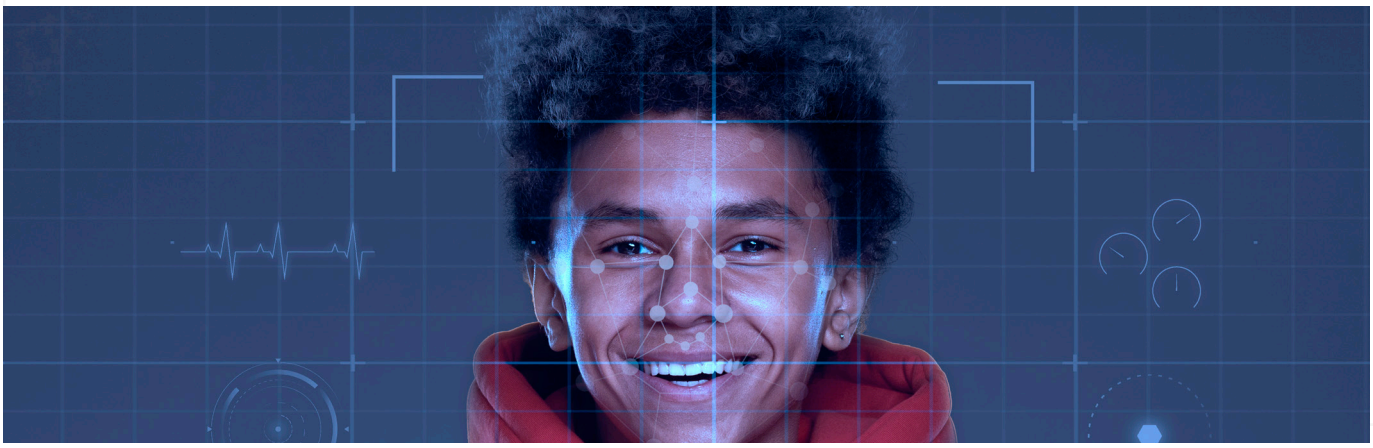
Attackers have stopped trying to defeat biometric verification. They have started using it.

The most material escalation practitioners now observe does not attempt to defeat biometric verification. It goes around it.

"Our experience over the past 12 to 18 months points to a hybrid vector we internally term Corporate Money Muling, where fraud networks bypass biometric verification entirely by using genuine human proxies to onboard corporate entities. A legally registered business is onboarded with a real, on-record director who completes liveness checks cleanly, after which operational control of the account is assumed by an undisclosed third party. Front-end biometric liveness verification, however sophisticated, cannot detect this vector, because the check is being performed by a real human rather than a spoofed or synthetic one. Generative AI has lowered the coordination cost of recruiting and managing these proxies at scale, particularly by removing the language and cultural-fluency barriers that previously limited how quickly foreign-linked networks could operate."

David Samson
Fraud Investigation Manager, Paystack

The evidence indicates that biometric defences and behavioural monitoring are now complementary requirements, not sequential ones.

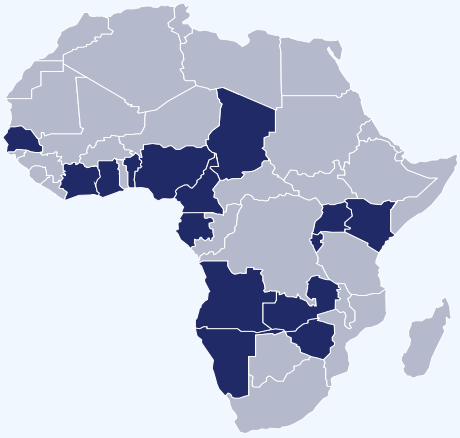


African financial fraud operates at syndicate scale

Operation Red Card 2.0 confirmed that financial fraud in Africa is no longer the work of individual actors. It is organised, networked, and sufficiently capitalised that syndicate leaders are investing in physical infrastructure to house their operations.

Operation summary: 8 December 2025 - 30 January 2026

High- yeild investment scams, mobile money fraud and fraudulent mobile-loan applications



16 Participating Countries

Angola, Benin, Cameroon, Chad, Côte d'Ivoire, Gabon, Gambia, Ghana, Kenya, Namibia, Nigeria, Rwanda, Senegal, Uganda, Zambia, Zimbabwe.

Nigeria
Investment Fraud ring

Côte d'Ivoire
Predatory mobile loan fraud, 58 arrests

Kenya
27 arrests, fake investment dashboards

651	2,341	1,442	+$45M	1,247
arrests	devices seized	malicious IPs, domains and servers taken down	losses exposed	victims identified

Source: Interpol

Between December 2025 and January 2026, INTERPOL's Operation Red Card 2.0 dismantled fraud networks across 16 African countries, exposing scams linked to over $45 million in losses. The operation confirmed what the data in this report shows: financial fraud in Africa is organised, networked, and sufficiently capitalised that syndicate leaders are investing in physical infrastructure. In Nigeria, an investment fraud ring had constructed a residential property as its operational hub; a separate syndicate infiltrated a major telecom provider through compromised staff credentials. In Kenya, 27 suspects ran fraudulent investment dashboards

through messaging apps and fabricated testimonials. In Côte d'Ivoire, 58 arrests targeted predatory mobile loan schemes exploiting vulnerable populations. The evidence indicates a consistent pattern across cases: structured operations, physical infrastructure, recruited personnel, and cross-platform reach.

03

Regulation has moved from prescriptive rules to evidence-based, real-time compliance

Nigeria's regulatory posture has moved from cybercrime statute to automated, evidence-based compliance.

2015

Cybercrimes Act 2015

Nigeria's first comprehensive cybersecurity law, criminalizing cyber fraud, hacking, identity theft, and mandating financial institutions to implement cybersecurity measures.

2018

CBN AML/CFT Administrative Sanctions Regulations

Introduced penalties for non-compliance with AML/CFT obligations, strengthening enforcement.

2019

NDPR 2019

Nigeria's first data protection regulation, issued by NITDA. Introduced consent requirements, data subject rights, and restrictions on cross-border transfers.

2022

CBN Cybersecurity Framework for OFIs

Mandated OFIs to establish cybersecurity units, conduct penetration testing, and report incidents.

2023

Nigeria Data Protection Act (NDPA)

Established the Nigeria Data Protection Commission (NDPC). Codified lawful processing, data subject rights, and localisation rules for sensitive data.

2025

CBN Cybersecurity Framework for OFIs

Introduced AI/ML-based suspicious activity monitoring, mandated 24-hour reporting to NFIU, enforced MFA for foreign card transactions, and made banks liable for APP fraud.

2026

CBN AML Baseline Standards

Requires automated AML/CFT/CPF solutions across all financial institutions. Compliance deadlines: Sept 2027 (DMBs), March 2028 (OFIs). Includes real-time risk assessment, sanctions screening, fraud detection, and case management

2026

CBN Data Localisation Directive

Circular mandating all payment transaction data generated in Nigeria to be stored locally by Jan 1, 2027. Introduced beneficial ownership disclosure and market share caps.

Four overlapping mandates have turned compliance into a concurrent enterprise transformation

Institutions can no longer address regulatory obligations sequentially. Between March 2026 and March 2028, the CBN requires them to automate financial-crime monitoring, localise payment data, strengthen identity and device controls, and demonstrate cybersecurity resilience. Changes that depend on the same data, technology, governance and talent foundations.

Four CBN mandates in effect between March 2026 and March 2028

Key deadlines and requirements financial institutions must meet

Mandate	Deadline/Status	Key Requirements
1. Cybersecurity Self-Assessment & Resilience	Immediate Evidence Requirement **DBs: Within 3 Weeks** **Other FIs: within 5 Weeks** **From 30 March, 2026**	• CBN Cybersecurity Self-Assessment Tool (CSAT) launched 30 March 2026. • Assesses governance, risk, technology, third-party, incident response and resilience • Evidence of controld required
2. Device Binding & Authentication (Instant Payments)	**Effective 1st July, 2026**	• Real-time enterprise fraud monitoring • Stronger identity verification for digital account opening & reactivation • One device per customer for mobile financial services •New device activation: ₦20,000 limit for the first 24 hours
3. Payment - Data Localisation	**Compliance by 1st January , 2027** **Circular Issued 15 June, 2026.**	• Payment - transaction data generated in Nigeria must be stored and managed domestically. • Review data flows, hosting, backups, DR, Vendor contracts and admin access
3. Automated AML/CFT/CPF Solutions	**Full Implementation** **DBs: By 10 Sept, 2027** **Other FIs: By 10 March, 20228**	• Automated systems across customer ID, risk assessment, sanctions screening, transaction & fraud monitoring, case mgmt, reporting and governance • Implementation Roadmaps due 10 June, 2026

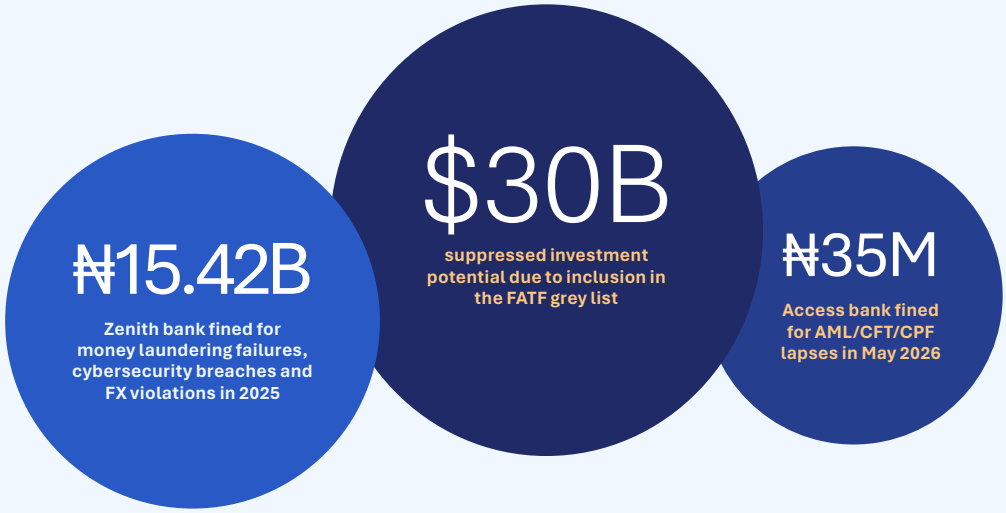
The mandates are operationally interdependent. Automated AML depends on integrated and reliable data; device binding depends on identity and real-time

fraud monitoring; localisation changes the infrastructure supporting both; and the CSAT tests whether the surrounding governance and resilience controls are effective. Treating each mandate independently could lead to duplicated investment, incompatible systems and gaps between compliance, technology and risk teams.

The mandates converge on one operational requirement: an integrated architecture across monitoring, data, identity controls, and infrastructure that carries all four simultaneously..

Compliance is expensive. Non-compliance is existential

Non-compliance now carries costs that extend beyond fines into Nigeria's restored market credibility.



Source: TechCabal, ThisDay

The enforcement trajectory removes any ambiguity about what non-compliance cost.. The ₦15.42 billion fine imposed on Zenith Bank in 2025 was a signal. Correspondent banking relationship closures, de-risking by foreign partners, and reduced access to international capital are the downstream consequences of non-compliance. Monetary penalties only begin to capture them.

Nigeria's removal from the FATF grey list in October 2025, achieved after two years of coordinated reform, was won at what Governor Cardoso has estimated as **$30 billion in suppressed investment potential** during the listing period. Underinvestment in automated AML compliance now triggers the very reputational and systemic consequences that the grey-list exit was designed to close.

04

The compliance mandate is advancing faster than institutional readiness

The compliance & cyber resilience index

The Compliance and Cyber Resilience Index assesses Nigeria's cyber resilience terrain across four pillars, infrastructure, talent, policy and enforcement, and incident response, using the three evidence streams set out in the methodology and scoring each pillar on a five-point scale.

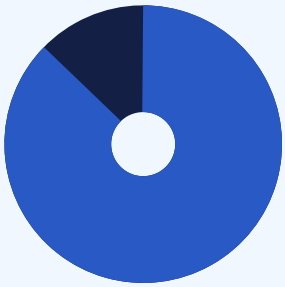
The compliance & cyber resilience index

Pillar	Status/Score	Index Rationale & Key Benchmark Metrics
1. Infrastructure Capacity	 (1.8/5.0) Below threshold	• 28 data centers for 250M+ people (Global Deficit) • 21 of 28 facilities locked in a single state (Lagos) • Insufficient local hosting capacity for 2026 laws
2. Talent Gap	 (2.1/5.0) Below threshold	• 100-firm mapping shows heavy junior/mid-level • Acute senior brain drain ("Japa") crippling leadership • Lack of data science capability to manage AI models • 90.6% cybersecurity workforce deficit
3. Policy, Regulation & Enforcement	 (3.0/5.0) At threshold	• Strong policy intent (CBN Baseline, NDPA, Localisation) • High regulatory involvement & active oversight • Enforcement lagged by regulator's own tech gap
4. Incident Response	 (2.0/5.0) Below threshold	• Financial services accounts for majority of 30 attack cases • Response pace lags the machine-speed profile of contemporary attacks • Automated real-time detection capability remains under-built

Scoring scale. 1.0 indicates absent or nascent operational capability. 3.0 indicates readiness broadly aligned with current regulatory expectations. 5.0 indicates mature capability that exceeds current regulatory expectations across all sub-components. Sub-components within each pillar are equally weighted, and composite pillar scores are the simple mean of the sub-components. Scores are directional composites, precise to one decimal place.

AI adoption has not translated into integrated defence

High AI adoption has not translated into lower fraud severity because most deployments remain point solutions, not integrated security and compliance architecture.



87.5%

of Nigerian Fintechs use AI for fraud detection

Institutions have adopted detection technology faster than they have redesigned their financial-crime operating architecture.

Source: CBN FINTECH Report (2025)

87.5% of Nigerian fintechs use AI for fraud detection. Yet Nigerian financial institutions lost ₦25.85 billion to digital payment fraud in 2025, and losses have grown 350% since 2020, even as reported case counts fell 31%. Nigerian banks now block the large majority of attempted fraud at their perimeter, but the successful attacks that penetrate appear to be more severe per incident than at any point in the recent record.

"The gap in compliance architecture is not confined to cybersecurity. Most private sector organisations do a great deal in cybersecurity while neglecting data privacy, and the pattern is the same in nearly every case we investigate: strong investment on the security side and neglect on the adjacent one. You can do a great deal in cybersecurity without doing data privacy, but you cannot do data privacy without doing cybersecurity. Many organisations will tell you that the CISO is also their DPO, but the CISO is the information security officer and the DPO is the data protection officer. The two roles are not interchangeable, and neither are the two disciplines."

Dr. Vincent Olatunji

National Commissioner, Nigeria Data Protection Commission

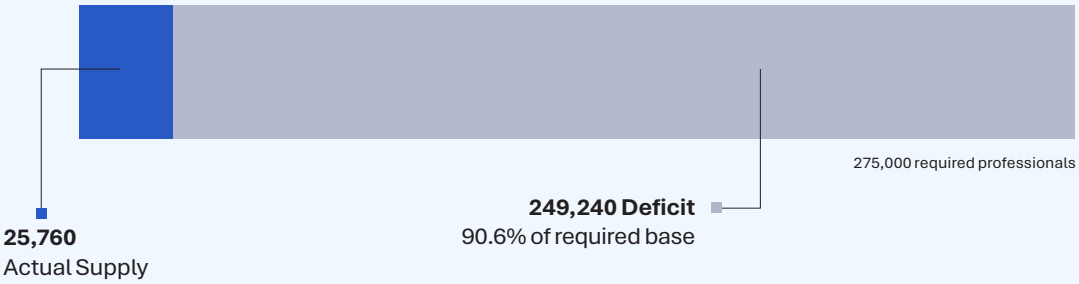
The pattern is now consistent across cybersecurity, privacy, and fraud detection. Institutions have adopted the tools. The architecture question is still open.

The talent required to build and govern automated compliance does not exist at scale

The CBN's compliance mandates assume institutional capacity that, at current talent supply, does not exist at scale.

Nigeria's cybersecurity workforce meets 9% of national demand

Certified professionals vs required base at global density benchmark, 2026



Density Ratio, Nigeria 1 expert per 8,000 citizens, against global benchmark of 1 per 800

Source: NITDA, compTIA

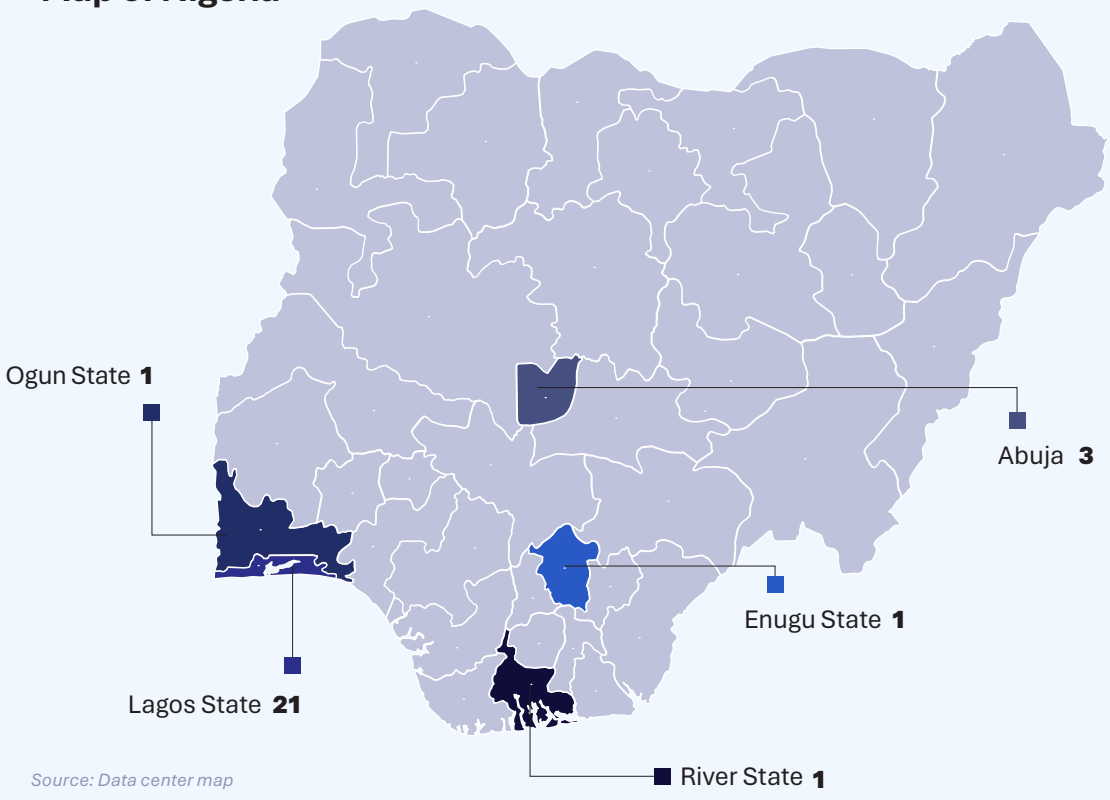
Nigeria has 25,760 certified cybersecurity professionals for a population exceeding 220 million, one tenth of the workforce the global density benchmark requires. Demand is not the constraint. Nigeria's tech sector is projected to generate 225,000 new job openings, many in cybersecurity. Supply is. Senior cybersecurity architects now earn ₦12 million to ₦25 million annually, salary bands most mid-tier banks and fintechs cannot match. The CBN's automated AML standards assume institutional capacity to build, validate, and govern AI-driven compliance systems.

The deepest capability is likely to remain concentrated among the largest institutions, while mid-tier banks, fintechs, and lenders face a more acute talent constraint.

Nigeria's data-centre capacity is expanding, but resilience remains constrained by concentration and limited redundancy

Domestic hosting capacity is expanding, but concentration in Lagos and limited active IT load could constrain secure migration ahead of the January 2027 localisation deadline.

Map of Nigeria



Source: Data center map

Nigeria has 28 data centre facilities across five states, but 75% of that capacity sits in Lagos. Active IT load capacity is less than 40 megawatts, meeting under 7% of the

600 megawatts required to support a fully competitive domestic digital economy, according to Digital Realty Nigeria. Expansion is underway, with OADC investing $240 million in a 24MW Lekki facility, Airtel's Nxtra building a 34MW site in Lagos, and total capacity potentially exceeding 150 megawatts by 2027. The CBN's data localisation directive requires all payment transaction data to be stored domestically by January 2027. The capacity is growing. The geographic redundancy that disaster recovery requires is not.

"Relocalisation is not about prioritising one aspect. Latency, redundancy, disaster recovery and security architecture all need to be considered, as they constitute the platform to offer the quality of services offered today. The focus is the migration plan, assuring like-for-like service offering.."

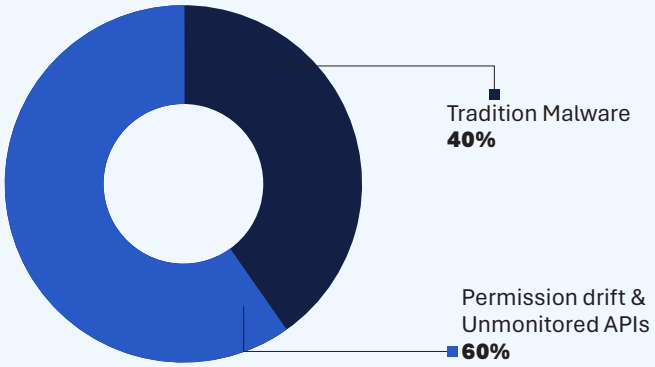
Lars Johannisson
CEO, Rack Centre

Data localisation without secure cloud architecture could create new exposure

60% of cyber incidents in Africa's cloud environments originate from permission drift and unmonitored APIs. Nigerian institutions are about to migrate workloads into precisely these environments under the CBN's January 2027 deadline.

Configuration failures, not malware, drive the majority of cloud incidents in Africa

Share of cyber incidents in African cloud environments, by attack vector, 2024–2025



Nigeria NBS
Data Breach

Kenya M-Tiba
2.15 TB, 4.8M people

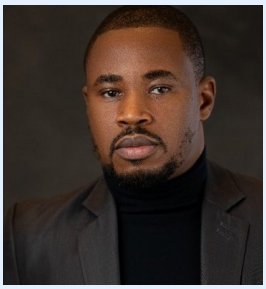
South Africa DoD
1.6TB, including presidential contacts

The CBN's data localisation directive requires all payment data stored domestically by January 2027. For institutions running critical workloads on offshore or hyperscale cloud environments, that means migrating critical workloads within months. The question now is whether institutions will migrate securely. In Africa's hybrid cloud environments, 60% of incidents stem from permission drift and unmonitored APIs, not malware. The evidence is already on the continent: Kenya lost 2.15 terabytes of health data affecting 4.8 million people, South Africa's Department of Defence lost 1.6 terabytes, and Nigeria's own National Bureau of Statistics was breached. Nigeria recorded 3,459 ransomware detections in 2025, third highest on the continent.

Even the best architecture inside a single institution will not be enough.

The architecture question does not stop at the institution's perimeter. Cross-institutional intelligence-sharing is the layer the sector has invested in least, and the layer that switch operators see the cost of most clearly.

"The biggest gap is that we keep working in silos. Bad actors are used against one financial institution, and the same situations happen at other institutions, and some of them succeed, but it is one ecosystem. Institutions, in an attempt to protect their reputation, do not report all the activities that happen, and the overall effect is that we are all worse off for it. If all the key organisations put their data on fraud attempts, compromised IP addresses, devices, and BVNs into one central intelligence base, successful attacks would drop by close to 50 percent, because some of this data is not really ours to hold. It concerns everybody, especially where it is tied to security."



Mudiaga Umukoro
CEO, Chams Switch

The evidence indicates that individual institutional readiness, however well built, converges on a ceiling that only sector-wide intelligence architecture can lift.

05

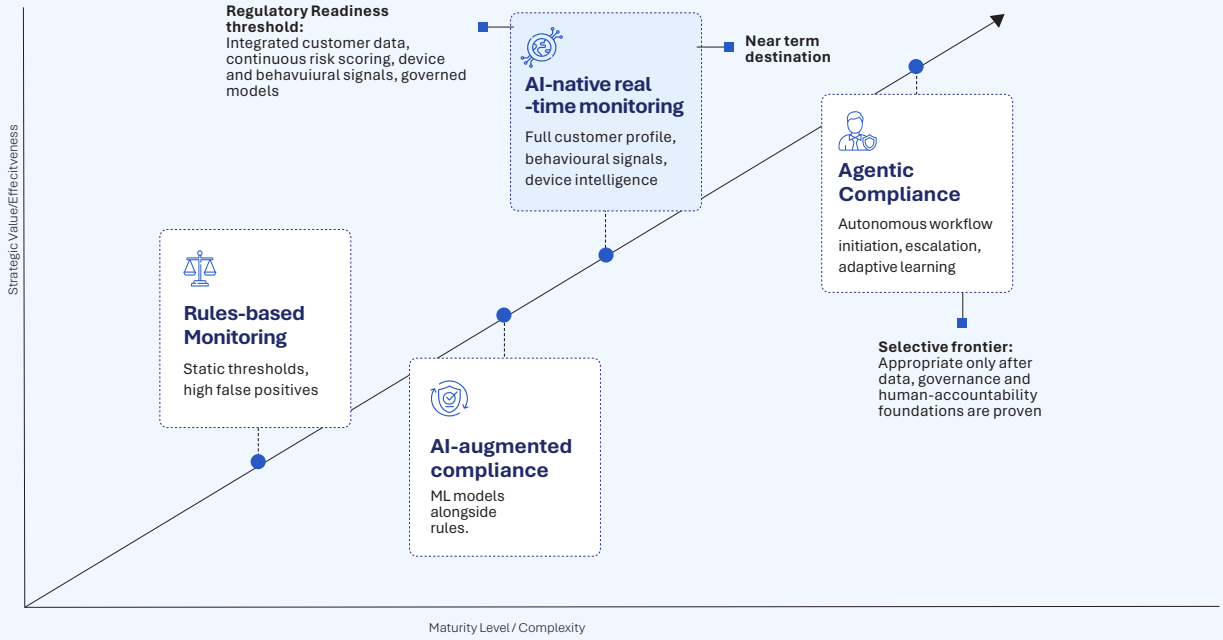
Passing regulatory scrutiny requires architecture, not just AI tools

Institutions should prioritise the move from AI-assisted tools to integrated, real-time compliance

Compliance maturity framework

The maturity journey from rule-based monitoring to autonomous, intelligent compliance

The regulatory readiness threshold sits at integrated, real-time compliance.



Source: TechCabal Insights analysis, informed by CBN Baseline Standards for Automated AML/CFT/CPF Solutions and industry research on AI-enabled financial crime compliance

Most institutions appear to remain between rules-based and AI-augmented compliance, with relatively few operating at integrated, AI-native monitoring at production scale. The transition from Stage 2 to Stage 3 is where the CBN's Baseline Standards land the regulatory threshold. It requires unified financial-crime data, connected fraud and AML systems, continuous customer-risk scoring, and independent model validation.

CBN compliance will be judged on architecture, not tool adoption

The CBN's baseline standards mandate four integrated capability layers across the full financial services perimeter, including digital asset infrastructure.

"Wallet governance, on-chain transaction monitoring and policy-based approval workflows are becoming institutional requirements rather than specialist capabilities. As digital assets integrate more deeply into regulated financial services, compliance is becoming part of the infrastructure itself rather than a function layered on afterwards."

Francis Ogbuka
Head of Africa, Utila

Detection

SDK signals, behavioral biometrics, device intelligence, anomaly detection.
CBN link: credible detection, monitoring investigation and measurable outcomes

Context

Full profile risk scoring, cross-channel and cross-product monitoring
CBN link: consolidated real time or near real time customer risk view

Governance

Annual validation, bias/drift testing, explainable alert logic
CBN link: defensibility, audit rails, model validation and explainable decisions

Collaboration

Federated learning, NIBSS ISO 20022 integration, cross-institution intelligence
CBN link: integrated control environment and collaborative intelligence

Together, these capabilities allow institutions to detect, decide, explain and respond at the speed of the threat.

The CBN's Baseline Standards do not mandate a technology purchase. They mandate an architecture. Detection alone, where most spending is concentrated, will not pass regulatory scrutiny without the three layers that make it defensible: context (risk-scoring against the full customer profile, not raw transaction data), governance (annual independent validation of AI models for accuracy, bias, and performance drift), and collaboration (cross-institutional intelligence sharing through frameworks like NIBSS's ISO 20022 migration).

The institutions most likely to pass regulatory scrutiny will be those that build all four layers. Buying an AI tool is not the same as building a defensible compliance architecture.

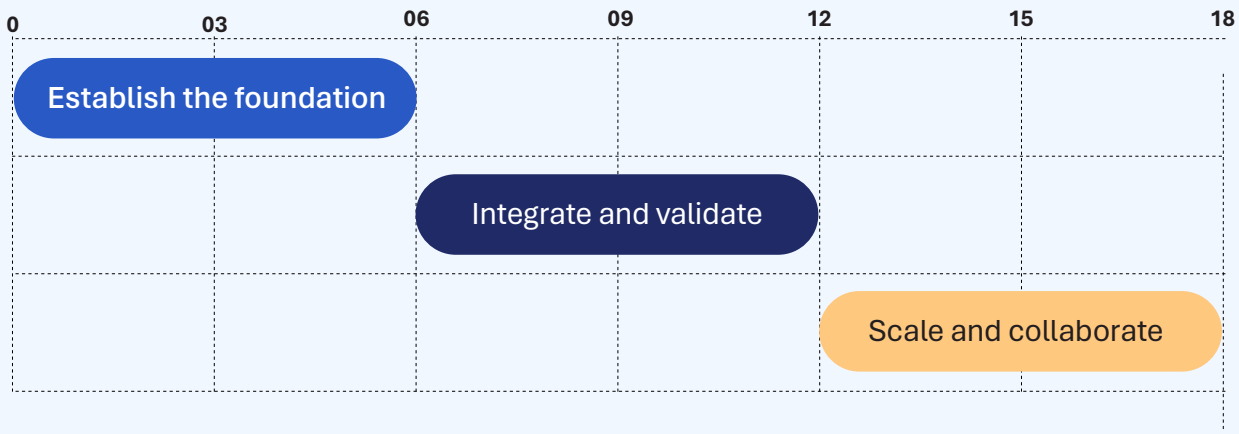
The CBN standards require one connected compliance system across the four capability layers.

Integration across the four capability layers cannot be built simultaneously, but it can be built in a defensible order under the mandate window.

"The most effective compliance systems are the ones fully integrated across the customer lifecycle: onboarding, transaction monitoring, screening, and ongoing due diligence, all working off the same intelligence rather than as separate checkpoints. What breaks first is the opposite model, where a customer can pass onboarding once and drift into entirely different risk territory months later without anyone connecting the dots. This is precisely the gap the CBN's baseline standards are designed to close: the expectation is not that institutions run good screening and good monitoring side by side, but that these functions operate as one connected system."

Ugonna Akah
Chief Compliance Officer, Moniepoint MFB

The roadmap below sets out how financial institutions subject to the CBN Baseline Standards can build the connected system Akah describes across the eighteen-month mandate window between March 2026 and March 2028



First 0–6 months:

Establish the foundation

Inventory fraud and AML systems.
Map data gaps and integration dependencies.
Define ownership and governance.
Prioritise high-risk customer journeys.
Assess localisation and resilience exposure.

Next 6-12 months:

Integrate and validate

Connect fraud, AML, identity and transaction data.
Introduce continuous customer-risk scoring.
Establish model documentation and validation.
Improve device and behavioural signal coverage.

Next 12-18 months:

Scale and Collaborate

Expand cross-product monitoring.
Automate selected investigation workflows.
Participate in shared fraud-intelligence mechanisms.
Test operational resilience and regulatory evidence.

06

What the evidence shows

What the last eighteen months have made clear

Nigeria's financial system faces a reckoning that procurement alone cannot resolve. AI has collapsed the cost structure of financial crime and become the only defence capable of matching its speed. The CBN responded with seventeen regulatory actions in fourteen months, six of them carrying hard deadlines between March 2026 and March 2028.

Nigerian financial institutions absorbed ₦52.26 billion in disclosed fraud losses in 2024 and ₦25.85 billion in 2025, a topline decline that conceals a 350 per cent underlying rise since 2020 while reported case counts fell 31 per cent. The TCI incident base documents over ₦100 billion in disclosed losses across 30 major cases and six sectors between 2019 and 2026. The Compliance and Cyber Resilience Index scores three of the four pillars below threshold, with only policy and enforcement at threshold. The operational foundations required to meet the mandates are not yet in place at Tier-1 scale, and are materially further behind at the mid-tier and OFI level. The reckoning will be survivable through an effective security and compliance architecture, and only when institutions, regulators, and industry infrastructure move as a coordinated system.

Four things the data tells us

On infrastructure.

The evidence indicates that data localisation is achievable within the CBN's deadline, but the concentration of national data centre capacity in a single city introduces a resilience question that will shape how institutions design their cloud posture for the next decade.

On talent.

A widening distance separates the seniority profile required to govern AI-driven compliance systems from the seniority profile currently in place, a gap the market is now pricing into compensation and mobility.

On policy and enforcement.

Nigeria has issued seventeen regulatory actions in fourteen months across cyber, data protection, and AML. The evidence indicates that policy intent has moved ahead of enforcement capacity, and institutions best positioned are those aligning their compliance architecture with the direction the regulators are travelling.

On incident response.

The evidence suggests the attack surface has migrated from institutional perimeters to payment infrastructure and identity systems, which is a shift the reporting frameworks and threat intelligence arrangements of the sector are beginning to catch up with.

Adhere
by Smartcomply

Compliance and Security, **Built into every Transaction.**

Adhere helps you monitor activity in real time, detect risks early, and stay compliant—without slowing down your business.

Partners

ISO 27001 NDPC mastercard

Appendix

The four pillars of our methodology

Pillar	Technical Focus	Core Research Imperative
Infrastructure	Evaluating domestic vs. foreign data hosting footprints, the density of state-capital edge data centers, and structural capacity limitations.	— Physical Infrastructure Check: Moving beyond software to analyze Nigeria's operational data centers. — The Lagos Concentration Risk: Assessing why a 75% concentration in Lagos creates an industry-wide single point of failure. — Data Localization Viability: Mapping the reality of storing financial data locally within compressed 2026/2027 timelines by CBN.
Talent Gap	Quantitative and qualitative census of specialized cybersecurity, risk engineering, and automated AML talent density.	— The hollow middle phenomenon: A large percentage of firms show an abundance of mid personnel but severe senior executive vacancies. — The Japa effect: Hyper-inflation of senior architect compensation pricing out mid-tier banks and fintechs. — Skillset Mismatch: Compliance teams are structured for legacy rules-based monitoring rather than modern data science and model calibration.
Policy, Regulation & Enforcement	Deconstructing institutional execution of the CBN Baseline Standards, the NDPA, and regional global alignment.	— The Enforcement Gap: Regulatory bodies lack the technical personnel necessary to continuously audit and enforce automated systems. — Low Baseline Compliance: Uneven regulatory visibility results in paper-shuffling compliance until historic, multi-billion naira fines hit. — Model Explainability Mandates: Operationalizing the strict requirement for independent annual audits on machine learning algorithms.
Incident Response & AI Speed Latency	Analysing active threat-response protocols, API exploitation vulnerabilities, and real-time automated mitigation capabilities.	— Traditional detection systems are blind to machine-speed API micro-transaction chaining and automated injection attacks. — Authentication over Onboarding: Tracking why defensive priorities must shift as live threats move past the front gate into verified customer flows. — AI-on-AI Countermeasures: Moving away from human-centric end-of-day batch processing to automated, millisecond signal networks.

Endnotes

1. The incident base underpinning this report tracks 30 major cyber and fraud incidents in Nigeria between 2019 and 2026, spanning financial services, government, telecommunications, healthcare, education, and crypto/fintech. Scan to explore the full dataset, filterable by sector and year. The 30-case incident base (2019–2026).
2. TechCabal. (2025–2026). Reporting on Nigerian financial-sector cyber incidents and enforcement penalties.
3. Central Bank of Nigeria. Baseline Standards for Automated Anti-Money Laundering, Counter-Financing of Terrorism and Counter-Proliferation Financing Solutions for Financial Institutions in Nigeria. CBN, 2026.
4. Central Bank of Nigeria. Circular on Data Localisation for Payment Transactions. Ref. PSM/DIR/PUB/CIR/001, 15 June 2026.
5. Central Bank of Nigeria. Cybersecurity Self-Assessment Tool (CSAT) for Deposit Money Banks and Other Financial Institutions. CBN, March 2026.
6. Central Bank of Nigeria. Guidelines on Device Binding and Strong Customer Authentication for Instant Payments. CBN, 2026.
7. Central Bank of Nigeria. Anti-Money Laundering and Combating the Financing of Terrorism Regulations for Banks and Other Financial Institutions in Nigeria. CBN, 2025.
8. Central Bank of Nigeria. Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions. CBN, 2022.
9. Central Bank of Nigeria. AML/CFT Administrative Sanctions Regulations. CBN, 2018.
10. Central Bank of Nigeria. Nigeria Fintech Landscape and Regulatory Report. CBN, 2025.
11. Federal Republic of Nigeria. Nigeria Data Protection Act. Official Gazette, 2023.
12. Federal Republic of Nigeria. Cybercrimes (Prohibition, Prevention, etc.) Act. Official Gazette, 2015.
13. National Information Technology Development Agency. National Cybersecurity Workforce Assessment. NITDA, 2026.
14. Nigeria Inter-Bank Settlement System (NIBSS). Annual Fraud Landscape Report, 2020–2025 (annual and quarterly editions).
15. INTERPOL. Africa Cyberthreat Assessment Report 2025.
16. INTERPOL. (2026, February). Operation Serengeti 3.0 and African Joint Operation against Cybercrime (AFJOC): Summary of results, 8 December 2025 – 30 January 2026.
17. Kaspersky Security Bulletin 2025: Statistics and Threat Landscape.

18. IBM Security and Ponemon Institute. Cost of a Data Breach Report 2025.
19. Sumsub. Global Identity Fraud Report 2025 (including the Global Fraud Index and deepfake incident tracking). Sumsub, 2025.
20. Financial Action Task Force. Jurisdictions under Increased Monitoring: Nigeria Delisting Statement, October 2025.
21. Digital Realty Nigeria. Nigeria Data Centre Capacity and Load Assessment. Digital Realty, 2025.
22. Open Access Data Centres (OADC). Lekki Facility Development Disclosure. Corporate release, 2025.
23. Airtel Africa. Nxtra Data Centre Investment Disclosure, Nigeria. Corporate release, 2025.
24. ThisDay. Coverage of Zenith Bank ₦15.42 billion regulatory fine and Nigeria's FATF grey-list exit, 2025. Lagos: Leaders and Company Ltd.
25. Central Bank of Nigeria. Remarks by Governor Olayemi Cardoso on the cost of FATF grey-listing to the Nigerian economy. Public statements, 2025.


Brought to you by:
techcabal
Insights
Adhere
by Smartcomply