Adhere by Smartcomply

Financial Crime Prevention and Compliance

Annual Report

2025

Adhere is Africa's Leading Fraud Detection & Compliance Solution

Leveraging on AI-powered transaction monitoring and fraud detection, engineered from the ground up for the complexities of the African market. We provide a single, intelligent shield that empowers financial institutions to automate KYC/AML processes, monitor transactions in real-time, and prevent financial crime with unparalleled precision.

Note from our Chief Executive Officer

Gbemisola Osunrinde

Building Trust. Defeating Financial Crime. Strengthening the Digital Economy.

To our Valued Shareholders, Esteemed Partners, and the Exceptional Adhere Team,

It is my pleasure to welcome you to the **Adhere Yearly Report**. This year's review captures not just our progress, but the broader evolution of AML, fraud prevention, and digital trust across Africa and the global marketplace.

2025 was a pivotal year. Financial crime grew more sophisticated, digital ecosystems expanded rapidly, and regulatory demands intensified. Through it all, one truth stood firm: **sustainable digital growth depends on strong, adaptive, and intelligent financial crime defense.**

2025 in Review: Key Themes

1. **Strengthened Regulatory Compliance**: Regulators across Africa raised the standard for AML enforcement. We responded with enhanced real-time updates to sanction lists, watchlists, and compliance rules; empowering our clients to remain continuously compliant and audit-ready.
2. **Growth of Digital Payments & Rising Fraud Risk:** The surge in instant payments and cross-border transactions brought new fraud challenges. Adhere's expanded fraud analytics and transaction monitoring capabilities enabled institutions to detect threats faster and respond with precision.
3. **AI-Powered Crime Prevention**: Our strategic investment in machine learning delivered measurable impact. In 2025, Adhere's behavioral and anomaly detection models helped resolve and mitigate **over 35% of complex fraud cases**, reinforcing automation as the future of financial crime defense.

Looking Ahead

1. **Integrated Compliance & Identity Intelligence:** In 2026, we will deepen automation across KYC, AML, and fraud monitoring, while expanding the **Grow** features tailored for emerging markets, including East and Francophone Africa. Our goal is simple: make compliance an effortless, intelligent layer that powers borderless business expansion.
2. **Stronger Global Fraud Defense Through Collaboration**: The next era of financial crime prevention will be built on shared intelligence. We are expanding partnerships, cross-border risk networks, and collaborative data engines to help institutions anticipate threats, not just react to them.

Our Commitment

The fight against financial crime is continuous. But with innovation, collaboration, and the insights shared in this report, we are poised to lead our partners into a more secure, transparent, and trusted digital future.
Thank you for your confidence, partnership, and belief in our mission.

Sincerely,
Gbemisola Osunrinde

Contents

4 **INTRODUCTION**

7 **DIGITAL PAYMENTS GROWTH AND RISE IN FRAUD RISKS**
Digital Payments Geography Analysis
2025 Global Fraud Trends
Analysis of Financial Fraud Trends and Channels in Nigeria

12 **FINANCIAL SERVICES COMPLIANCE & REGULATORY INNOVATIONS**
Real-Time Payments Are Redefining Compliance Standards
The global Impact of Regulatory Measures and Compliance

16 **THE ROLE OF EMERGING TECHNOLOGIES**
The Role of Emerging Technologies

18
Real Time Transaction Monitoring (RTTM)
Identity Verification & Advanced KYC
Device and Geolocation Analysis
Advanced Loan Analysis
Use Cases of Modern Fraud Prevention and Compliance
Traditional fraud monitoring vs Modern fraud monitoring

24 **ARTIFICIAL INTELLIGENCE & MACHINE LEARNING IN FRAUD DETECTION**

25 **FUTURE OF FRAUD PREVENTION**

28 **FORWARD VIEW**

Introduction

2025 has emerged as a pivotal year in the fight against financial crime. Regulatory authorities across the world are responding with unprecedented urgency, introducing stricter AML requirements, strengthening sanctions frameworks, increasing transparency expectations, and intensifying supervisory enforcement. At the same time, criminals are adapting quickly, exploiting emerging technologies, exploiting loopholes between jurisdictions
Compliance is no longer just an operational requirement; it has become a test of resilience, agility, and technological maturity.

This report examines the forces reshaping financial crime prevention and compliance today, focusing on three critical themes:

1. **Digital payments growth and rise in fraud risks:** As payments become instant and more digital, fraud opportunities increase. Mobile wallets, API-based services, and digital onboarding reduce friction for users while simultaneously creating new entry points for attackers.
2. **Financial Services Compliance & Regulatory Innovations:** New regulations and standards, such as the CBN's AML Baseline Standards and the global adoption of ISO 20022, are forcing financial institutions to embed AI-driven transaction monitoring directly into the payment flow. This not only enhances AML and fraud detection efficiency but also transforms compliance from a post transaction audit function into a proactive, technology driven gatekeeper essential for maintaining the integrity of the fast-paced digital economy.
3. **The role of emerging technologies**: Modern compliance requires modern infrastructure. Tools like Adhere combine Artificial Intelligence (AI) and Machine Learning (ML) to provide an integrated approach to fraud detection, sanctions screening, identity verification, and risk assessment delivering real-time insights that help compliance teams stay ahead of evolving threats.

Digital payments growth and rise in fraud risks

Digital Payments Geography Analysis

Digital Payments Market CAGR(%) Growth rate by region 2025-2030

Source: Mordor Intelligence

Africa’s digital payments landscape continues to scale rapidly, with mobile money agents processing USD 1.68 trillion in 2024, though adoption gaps persist in rural areas due to cash reliance and infrastructure limitations. Across other emerging regions, South America and the Middle East are also accelerating through state backed instant payment rails such as PIX, CoDi, and GCC real-time payroll systems. In Europe, regulatory leadership is shaping market maturity, with MiCA and the 2025 instant-payments mandate driving 24/7 euro transfers and encouraging cross border innovation. Asia Pacific remains the global growth engine, powered by China’s digital yuan, India’s UPI, and widespread QR code standardization such as QRIS, with Indonesia alone recording USD 5.4 billion in QR transactions last year. Meanwhile, North America maintains a strong position with 38.3% revenue share, supported by card network dominance and the rollout of FedNow, as U.S. banks explore stablecoin based settlement to reduce friction across the US, Canada, Mexico corridor.

2025 Global Fraud Trends

Growth in e-commerce, digital wallets, BNPL, and P2P/mobile money services has expanded the attack surface. More access points from apps to APIs mean more potential vulnerabilities. The diversification of payment methods provides fraudsters flexibility, they can switch channels (card, wallet, bank transfer) to evade detection or exploit weaker controls in newer rails.

Social Engineering & APP Fraud

2025 saw attackers shift from technical exploits to human manipulation. Authorised Push Payment (APP) fraud and impersonation scams grew sharply as fraudsters used AI-generated voices, deepfake videos, and cloned identities to deceive customers and staff. Phishing scams were the most common type of fraud, often through deceptive emails and fake banking websites.

Growth of Mule Networks & Synthetic Identities

Account takeover fraud increased by 19%, with criminals accessing legitimate user accounts to siphon funds or execute unauthorized transactions.
Mule accounts, both recruited and synthetic became central to laundering operations.
Synthetic ID fraud grew as criminals combined stolen data with AI-created credentials to bypass onboarding systems

Real-Time Fraud (Speed Exploitation)

The speed of instant payment systems is being leveraged for maximum financial gain; Instead of targeting one massive transaction, fraudsters execute countless small transactions, leveraging the near instantaneous settlement to disperse funds across many accounts before any single alert is triggered.

E-Commerce & Marketplace Fraud

As digital commerce continues to grow globally, businesses are reporting more sophisticated attacks such as:

- Bot-driven card testing
- Fake merchants and marketplace listings
- Inventory and logistics fraud
- Account takeovers targeting loyalty programmes

Fraudsters exploit the scale of online marketplaces, using automation to mask activities across thousands of small transactions.

Corporate & SME Vulnerabilities

Small and medium enterprises (SMEs), in particular, are heavily targeted due to limited security budgets. Trends include:

- Business Email Compromise (BEC)
- Invoice manipulation and supplier fraud
- Payroll redirection scams
- Insider collusion, often driven by economic strain

The use of malware and spyware to steal sensitive banking credentials rose by 22%, particularly targeting small businesses.

Cross-Border & Crypto Enabled Fraud

Scams involving cryptocurrency wallets escalated, with $3 billion in stolen assets, primarily through fake investment platforms. Consumers and businesses using cross-border payment services face added risks from:

- Layering across multiple jurisdictions
- Crypto-to-fiat laundering
- Cross-chain obfuscation using mixers and bridges

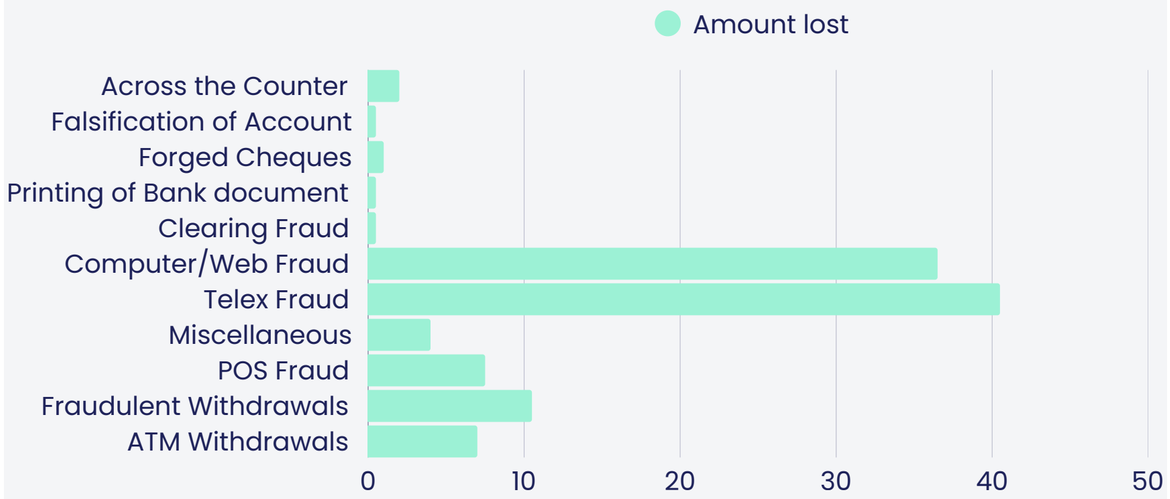
Fraudsters exploit regulatory gaps between countries and weak KYC controls in certain digital asset platforms.

Analysis of Financial Fraud Trends and Channels in Nigeria

In the third quarter of 2025 in Nigeria, a total of 14,697 fraud cases were reported, reflecting a substantial 38.8% increase from the 10,589 cases recorded in Q2. Most fraud was driven by external actors, with outsider led incidents jumping 39.2%, while staff related fraud and staff terminations both fell notably.

The highest impact channels were Computer/Web (₦2 billion; 39.5%), Mobile (₦1.23 billion; 23.5%), and POS (₦595 million; 11.3%), together accounting for over 74% of the value involved. In terms of losses, Computer/Web and Mobile fraud made up 77% of the total. Channel specific trends showed broad increases across ATM (103%), Web (68.5%), Branch (35%), and POS (20.7%) fraud. Card fraud surged by 40%, cash-related fraud by 15%, while cheque fraud fell by 37% and mobile fraud declined by 9.7%.

Percentage Distribution of Amount lost to Frauds and Forgeries (Third Quarter 2025)



FITC Reports on Fraud and Forgeries in Nigerian Banks

Financial Services Compliance & Regulatory Innovations

Real-Time Payments Are Redefining Compliance Standards

1. The Central Bank of Nigeria's (CBN) Baseline Standards for Automated AML Solutions

The CBN exposure draft released in May, 2025 directly addresses the challenges posed by real-time payment systems. Traditional, manual compliance methods cannot keep pace with the instantaneous movement of funds, which facilitates high-speed financial crime. The new standards mandate a paradigm shift, requiring financial institutions to adopt automated, AI/ML-driven AML solutions capable of real-time transaction monitoring, screening, and alert generation. This integration embeds compliance directly into the payment process, transforming it from a slow, post-transaction audit function into a proactive, technological gatekeeper necessary to maintain the integrity of Nigeria’s fast-paced digital financial ecosystem.

2. EU Instant Payments Regulation Fully in Effect

As of January, payment service providers have been required to accept euro instant payments within 10 seconds, and from October onward, they must also send payments under the same timeframe. This shift goes far beyond operational efficiency; it is a major compliance pressure point. Traditional batch based screening can no longer keep up, as sanctions and fraud checks now need to run at transaction speed. Institutions without real-time screening engines, fallback workflows, and immediate alert-handling mechanisms are already feeling the strain, and regulators are expected to closely examine early failures.

3. ISO 20022: The Foundation for Next-Gen Compliance

More than half of all cross-border messages now use ISO 20022, and with the coexistence period ending in November, structured data is becoming mandatory. The richer data set such as purpose codes, LEIs, and extended address fields can significantly enhance sanctions, AML, and fraud monitoring accuracy. But this also raises expectations for data quality and governance. Poorly structured or incomplete data can now cause instant payment rejections and potential compliance breaches.

Treating ISO 20022 as a mere system upgrade rather than a transformation in data standards may leave institutions exposed just as regulatory scrutiny intensifies.

4. FATF's Enhanced Payment Transparency

In June, the Financial Action Task Force (FATF) updated Recommendation 16 to significantly tighten standards for payment transparency. This revision mandates that complete and accurate originator and beneficiary information must accompany funds throughout the entire payment chain, regardless of whether the transfer uses traditional cross-border systems or newer digital platforms. In essence, incomplete or inconsistent data is now a clear violation.

For financial institutions, this means a critical need to upgrade and strengthen data validation systems to prevent rejected transfers, ensure seamless transactions, and avoid intense regulatory scrutiny for non-compliance.

The global Impact of Regulatory Measures and Compliance

- Regulatory frameworks like GDPR and CCPA prompted 65% of financial institutions to overhaul their data protection strategies.
- The US Office of the Comptroller of the Currency (OCC) issued $1.2 billion in fines to banks for insufficient fraud prevention in 2023.
- KYC compliance violations led to penalties exceeding $800 million globally.
- CBN's new fraud detection laws significantly impact Nigerian banks by enforcing strict, rapid accountability, mandating faster customer refunds (within 16 days), tightening reporting (72-hour customer limit), and imposing severe penalties for negligence, forcing banks to invest heavily in stronger tech.
- Anti-Money Laundering (AML) regulations helped recover $4.5 billion in fraudulent funds through coordinated efforts.
- Cross-border fraud prevention agreements among 15 countries facilitated real-time fraud alerts, reducing losses by 20%.
- Banks investing in compliance training programs saw a 25% improvement in staff adherence to fraud detection protocols.
- Regulatory sandboxes, which allow controlled testing of anti-fraud technologies, expanded by 18%, enabling innovative approaches to fraud prevention.

Despite the heightened scrutiny and tougher requirements, these regulatory measures are ultimately shaping a stronger and more resilient financial ecosystem. Each intervention pushes institutions toward higher standards of transparency, accountability, and technological maturity. As banks invest in better tools, tighter controls, and more capable teams, the industry is steadily moving toward a future where fraud is identified faster, losses are minimized, and consumer trust is reinforced.

Source: Techcabal, Coinlaw

The Role of Emerging Technologies

The Role of Emerging Technologies

Emerging technologies are reshaping the future of financial crime prevention by enabling faster, smarter, and more adaptive detection. Artificial intelligence, behavioural analytics, machine learning, biometrics, blockchain intelligence, and identity orchestration platforms are transforming how institutions identify suspicious patterns, authenticate users, and monitor risk signals across vast data streams. These tools are reducing false positives, streamlining investigations, and providing the real-time visibility needed to operate safely in instant payment environments.

This section examines the technologies powering modern financial crime prevention and the reasons they've become essential in today's high velocity payment and risk environment. We also show how Adhere applies these technologies across its platform to help organisations detect threats before they cause harm.

Real Time Transaction Monitoring (RTTM)

RTTM engines analyse thousands of variables per second to block suspicious activity before settlement. Machine learning is now central to financial crime detection, enabling systems to learn from historical patterns and dynamically adjust to new attack behaviors.

Detects anomalies invisible to static rule engines: ML Models use Behavioral Analytics to establish a unique, dynamic profile of "normal" behavior for every customer, account, and device. An anomaly is then detected not by breaking a pre-set limit, but by any statistically significant deviation from that individual's learned pattern. This allows the system to identify subtle, non linear risk signals, such as a user logging in from an unfamiliar device, immediately changing a password, and then making a low value payment to a new beneficiary a combination of actions that no static rule would flag as highly suspicious.

Learns evolving fraud patterns such as device switching or mule-network behaviour: They achieve this by analyzing millions of data points across the network, automatically identifying the hidden common features of successful fraud attacks known as feature engineering. For example, the model can quickly recognize a new mule-network pattern where many different new accounts receive identical small transfers from multiple victims before simultaneously clearing the funds, or recognize a specific pattern of device switching used to test stolen credentials. This adaptive learning allows the system to detect and block new fraud waves before they are explicitly known or coded into a rule set

Reduces false positives with adaptive risk scoring: By comparing the transaction against the user's detailed normal profile and the patterns of known fraud, the ML model provides a score that reflects the true probability of risk. For instance, a large payment made to a known business partner that fits the user's historical spending is not flagged, whereas a smaller, unusual payment showing three minor deviations from the norm receives a high-risk score. This precision dramatically cuts down the investigative queue, allowing compliance teams to focus their resources on the genuinely suspicious activities.

Identity Verification & Advanced KYC

Identity verification is moving beyond document checks. Modern systems combine multiple signals to create a holistic identity risk profile.

1

Facial Matching Algorithms: Facial matching algorithms use advanced computer vision techniques and machine learning models to verify that a person's face matches a trusted source such as a government-issued ID, selfie, or previously registered biometric record. Advanced platforms compare the face to records, ensuring continuity over time and detecting account takeover attempts and helps institutions meet identity verification standards required by regulators.

2

Digital Identity Validation: ensures the authenticity and validity of key national identity credentials in real time. Systems are built to interface with authoritative government databases, such as Nigeria's NIN (National Identity Number) database, the Kenyan Alien ID, and many other registries. This simultaneous digital verification is vital during customer onboarding, as it prevents the use of forged, manipulated, or synthetically generated identity documents, establishing a foundational level of trust and compliance from day one.

3

Real time Sanctions and PEP Screening The convergence of sanctions lists (like OFAC and EU), PEP (Politically Exposed Person) global watchlists, and modern technology forms the backbone of adaptive compliance. This integration utilizes fuzzy matching technology that account for variations in spelling, transliteration, and name order to accurately screen new and existing customers against high-risk entries, drastically reducing both false positives. This check is transformed into a dynamic process via continuous monitoring.

4

Biometric and Liveness Verification: is a crucial, non-repudiable security feature used during digital onboarding to verify that the person presenting an identity document (ID) is physically present and not an imposter using a static image, video replay, or deepfake mask. The process typically requires the user to perform a specific action, such as nodding, turning their head, or blinking. This effectively combats synthetic identity fraud and deepfake attacks, creating a high level of assurance during the initial KYC authentication phase.

Device and Geolocation Analysis

This technology creates a digital fingerprint of the device and monitors the location from which a customer is accessing services.. As a user initiates a transaction, the agent assesses hundreds, if not thousands, of parameters including IP address, device fingerprint, transaction history, geo-location in milliseconds. If an anomaly or suspicious pattern is detected, the transaction can be immediately flagged for review, put on hold, or outright blocked before it completes.

Device Fingerprinting: Analyzes hundreds of attributes (OS version, browser type, device ID, installed fonts) to uniquely identify a user's device, Combats Account Takeover (ATO) Instantly flags a login attempt from a new or unrecognized device, triggering multi-factor authentication (MFA).

Geolocation Analysis: Uses IP addresses, GPS, and Wi-Fi triangulation to pinpoint a user's physical location during a transaction. Detects Impossible Travel; alerts are raised if a user attempts a transaction in London minutes after logging in from New York, signaling a credential compromise. Also restricts access from known high-risk geographical areas (geo-fencing).

Advanced Loan Analysis

Advanced loan analysis has become one of the fastest-growing technologies redefining risk management, fraud detection, and credit decisioning. In 2025, financial institutions are shifting toward AI-powered loan analytics, which evaluate borrowers using real-time behavioural, transactional, and identity signals to detect inconsistencies before a loan is approved.

Fraud Detection: ML models analyze patterns in application data, device fingerprints, and document metadata to identify red flags associated with synthetic identity fraud or loan stacking (applying to multiple lenders simultaneously).

Income-to-Debt Matching (The DTI Ratio): Income-stability models analyse transaction flows, employment history, and spending behaviour to detect inflated income claims or hidden liabilities. This ratio calculates the percentage of the applicant's gross monthly income that goes toward servicing all existing debt obligations.

Collateral risk engines estimate liquidation value in real time, identifying overvalued or recycled collateral a common fraud tactic. Instead of simply checking documents, modern systems detect fraud at the intent stage pinpointing anomalies in behaviour, documentation, financial flows, or identity signals that indicate elevated risk.

Use Cases of Modern Fraud Prevention and Compliance

AI and machine-learning are no longer experimental technologies; they now drive real, measurable impact across fraud prevention, KYC/AML, and regulatory compliance, enabling institutions to detect risks earlier, respond faster, and operate with greater precision. Here we will look at some use cases of these tools in action.

1. Behavioural Analysis & real time detection

Use case: Detect suspicious or abnormal payments in milliseconds.

A customer normally makes ₦15,000–₦30,000 transactions. Suddenly, a ₦850,000 transfer is initiated from a new location at 2 AM.
The ML model flags the transaction as high risk due to:

- unusual amount
- abnormal time of activity
- location mismatch

The payment is automatically held for review or blocked until verified.

2. Sanctions & PEP Screening Optimization

Use case: Reduce false positives by using intelligent name matching.

The name “Olawale J. Badmus” matches 42 similar profiles on a sanctions list or pep, instead of flagging all profiles.
AI/ML uses:

- fuzzy matching technology
- linguistic models
- scoring accuracy

System narrows it down to the true match which results to 80–95% false positive reduction.

3. Customer Risk Profiling (Adaptive Risk Scores)

Use case: Continuously adjust a customer’s risk level using behaviour algorithms.

If a previously low-risk customer, Is now

- on a watchlist
- transacting in high-risk corridors
- sending larger, more frequent transfers

AI increases their risk score enabling enhanced monitoring and EDD .

Traditional fraud monitoring vs Modern fraud monitoring

Aspect	Traditional Fraud Monitoring	Modern Fraud Monitoring
Detection Approach	Static Rules & Thresholds	Adaptive, Self-Learning Models
Alert Accuracy	High False Positives	Significant Reduction in False Positives
Speed & Processing Method	Limited Ability	Real time risk scoring in milliseconds
Data Utilization & Behaviour Analysis	Limited to transaction fields	Uses behavioural, contextual, device & network intelligence
Fraud Coverage & Cross-Channel Visibility	Single Channel Monitoring	Cross-Channel Fraud Detection

Artificial Intelligence & Machine Learning in Fraud Detection

As financial crime grows in speed and sophistication, institutions are responding with a new generation of detection and prevention technologies designed to stay ahead of emerging threats. These innovations ranging from real-time analytics and behavioural intelligence to biometrics and blockchain, are reshaping how financial institutions secure transactions, protect customer identities, and mitigate operational risk. The following insights highlight how these technologies are strengthening fraud defences across global banking.

+92%

Deep-learning models detected new and evolving fraud schemes with 92% accuracy, especially in high-risk transactions.

+40%

Automated anomaly detection platforms cut the need for manual reviews by 40%, freeing teams to focus on complex investigations.

+$25b

AI-powered fraud systems helped financial institutions avoid over $25 billion in losses globally in 2025, reinforcing their impact on risk reduction.

Source: Coinlaw Banking Fraud detection statistics, 2025

Global adoption of Emerging Technologies in Fraud Prevention

Europe Leads with Regulation Driven AI Adoption

The EU's instant payments regulation, ISO 20022 migration, and tightening AML standards have accelerated adoption of real-time AI monitoring, behavioural biometrics, and advanced sanctions engines.

North America Expands AI & Real-Time Payments Security

The launch of FedNow and continued RTP growth pushed U.S. banks to deploy ML-based fraud scoring, mule-account analytics, and behavioural biometrics to stop real-time APP fraud.

Asia-Pacific Accelerates Biometric Identity & Transaction Security

APAC is the fastest adopter of real-time fraud orchestration. Markets like India, China, Singapore, and Indonesia integrate biometrics, QR-based security, and AI monitoring into digital payment ecosystems.

Africa Adopts Instant Payment and Mobile Money Safeguards

With mobile-money volumes exceeding USD 1.6 trillion, African regulators and banks are investing in real-time AML engines, device intelligence, and cross-border fraud controls through PAPSS, EAPS, and SADC RTGS.

Middle East & Gulf Region Invest in AI Identity & AML

GCC countries implement facial biometrics, AI-powered KYC onboarding, and advanced AML analytics as digital banking and instant payroll systems expand.

Latin America Strengthens Real-Time Controls as PIX, CoDi Grow

Brazil's PIX and Mexico's CoDi have driven adoption of behavioural analytics, bot detection, and graph-based AML systems to counter immediate fraud risks.

Sources: Various news articles and reports

Examples of companies using AI to detect fraud, automate compliance, and enhance customer experiences

JPMorganChase

Uses thier internal AI platform Omni AI with Large Language Models (LLMs) and ML to identify suspicious transactions, cutting account validation rejection rates by 15-20% and reducing false positives.

MasterCard

Master card records $50b in potential losses from fraud prevented in past three years, they proactively block fraudulent payments using AI and processes insights from billions of global transactions to secure transactions.

stripe RADAR

Stripe is transparent about its use of a global, multi-trillion dollar transaction network to train its AI. Utilizes machine learning models trained on vast global data to cut card-testing attacks by an estimated 80% and reduce fraud losses.

paystack

Employs AI/ML to detect anomalies in payment patterns, block fraudulent transactions, and protect merchants and customers.

carbon

Leverages AI for smarter income verification and fast-track loan underwriting, enabling the platform to disburse large volumes of loans more efficiently.

HSBC

Using AI broadly across fraud detection, transaction monitoring, and compliance. Their recent commitment to generative-AI underscores a drive toward automation and advanced risk-detectio

BudPay

In 2025, Budpay invested in next-generation fraud-prevention tools with ML-powered detection engines to block suspicious activity instantly, backed by upgraded encryption and data-protection systems that keep customer information safe.

absa

Absa Digi Account and Digi Loan; industry-first 100% digital products that use facial and voice recognition, document intelligence, and machine learning to automate onboarding and credit decisioning.

Sources: Various news articles and reports

Future of Fraud Prevention

The future of fraud prevention is being shaped by rapid advances in artificial intelligence, increasingly real-time payment ecosystems, stronger global regulation, and the shift toward hyper connected digital identities. Below are the key developments that will define the next generation of fraud-prevention strategies:

Embedded Fraud Prevention Across User Journeys

Financial institutions are shifting from "monitor at the end" to embedding fraud controls at every step:

- Login
- Authentication
- Transaction initiation
- Transaction execution
- After transaction

This end-to-end intelligence is especially critical for APIs powering open banking, wallets, merchant payments, and B2B transfers.

Self-Learning, Autonomous Fraud Engines

As financial crime becomes faster, the next generation of fraud detection systems will go far beyond with tools such as:

- Deep learning
- Graph neural networks
- Sequential pattern models
- Federated learning across institutions
- Large scale anomaly detection engines

These models will identify fraud rings, mule networks, synthetic IDs, and collusive behavior across channels and institutions.

AI Co-Pilot Systems for Analysts

Instead of separate rule engines, case tools, and monitoring dashboards, future fraud teams will use AI copilots that:

- Auto-triage alerts
- Perform first level investigations
- Generate case summaries & reports
- Suggest risk scores and recommended actions
- Reduce investigation time by 50–70%

These copilots will dramatically reduce manual workload and operational cost.

Forward View

The year 2026 marks an inflection point where compliance and fraud defense transform from necessary friction into a strategic engine for business expansion. Adhere is deepening its commitment to smarter, faster, and more automated financial crime defence.

Adhere is strategically expanding its global defense posture to proactively tackle the rising complexity of financial crime. This expansion is centered on establishing robust cross-border intelligence networks and collaborative, privacy preserving, data sharing frameworks.

In 2026, we are giving financial institutions deeper visibility into merchant risks, enabling organisations to detect risky devices, behavioural anomalies, repeat offenders, and cross platform fraud patterns with far greater precision. These capabilities form part of a broader multi-layer fraud detection architecture combining AI-powered anomaly detection, behavioural intelligence, network level risk scoring, and real-time monitoring. This unified framework ensures that fraud is intercepted at multiple points simultaneously, reducing blind spots and limiting attack surfaces.

Looking ahead, Adhere will advance in a smarter, more resilient, and deeply collaborative approach to fraud prevention also making compliance effortless for businesses scaling across Africa’s high growth digital economies.

About Adhere

The Engine of Secure Financial Growth.

We are the trusted compliance and fraud prevention partner for the fintechs, banks, and payment processors shaping the future of African finance. Our platform delivers measurable results, protecting revenue and enabling our clients to scale with confidence.

Monitoring over $1B in transactions every month, delivering a 70% reduction in manual compliance workload and a significant decrease in false positives for our clients.

Our Core Strengths

- **Real-Time Transaction Monitoring:** Our AI-powered engine analyzes every transaction in real-time, detecting anomalies and suspicious patterns with incredible speed and accuracy.
- **Automated KYC/AML Screening**: Seamlessly screen customers against global and local watchlists, sanctions lists, and Politically Exposed Persons (PEP) databases to ensure full regulatory compliance.
- **Customizable Rule Engine**: Go beyond out of the box solutions. Create and fine-tune sophisticated, custom rules that reflect your unique business logic and risk appetite.
- **Comprehensive Case Management**:Adhere centralizes all compliance and fraud workflows, making it easier to triage, assign, and resolve alerts. This improves collaboration, and speeds up investigations while maintaining regulatory auditability.

Adhere by Smartcomply

Trusted by

Glossary and notes

AI
Artificial Intelligence

AML
Anti-Money Laundering

API
Application Programming Interface

BEC
Business Email Compromise

BNLP
Buy Now, Pay Later

CAGR
Compound Annual Growth Rate

CCPA
California Consumer Privacy Act

CBN
Central Bank of Nigeria

CODI (CoDi)
Cobro Digital (Mexico's digital payments platform by Banco de México)

DTI
Debt-to-Income Ratio

EAPS
East African Payment System

EDD
Enhanced Due Diligence

FATF
Financial Action Task Force

FedNow
Federal Reserve's Real-Time Payments System

GDPR
General Data Protection Regulation

Geo-fencing
A location-based boundary used in apps, risk management, fraud detection, etc.

ISO 20022
A global payment messaging standard providing structured, richer data to improve fraud detection and cross-border transparency.

KYC
Know Your Customer

LLM
Large Language Model

ML
Machine Learning

OFAC
Office of Foreign Assets Control

OCC
Office of the Comptroller of the Currency

PAPSS
Pan-African Payment and Settlement System

PEP
Politically Exposed Persons

RTP
Real-Time Payments

RTTM
Real-Time Transaction Monitoring

Adhere
by Smartcomply

info@smartcomply.com adhere.smartcomply.com