GAB
GHANA ASSOCIATION OF BANKS

POLICY BRIEF

Financial Crime, Fraud Trends and Regulatory Expectations in the Digital Era: Evidence from the Ghanaian Banking Industry

GAB RESEARCH
March 2026
PB/005/26

GHANA ASSOCIATION OF BANKS

POLICY BRIEF

GAB RESEARCH

FINANCIAL CRIME, FRAUD TRENDS AND REGULATORY EXPECTATIONS IN THE DIGITAL ERA: EVIDENCE FROM THE GHANAIAN BANKING INDUSTRY

Author:
Collins Boamah
Head of Regulatory, Ethics, Forensics & Special Duties
Ghana Association of Banks
Email: Collins.Boamah@gab.com.gh

Executive Summary

The acceleration of digital financial services in Ghana has transformed the country's banking landscape while simultaneously reshaping its financial crime risk profile. Drawing on insights from the Bank of Ghana (BoG) Annual Fraud Reports, Ghana Association of Banks (GAB) Quarterly Fraud Reports, Financial Intelligence Centre (FIC) data, and law enforcement sources including the Ghana Police Service, EOCO, and OSP, this paper examines evolving fraud typologies, systemic vulnerabilities, and regulatory expectations within Ghana's banking sector.

The findings reveal a structural shift from traditional branch-based fraud to digitally enabled, identity-driven, and cross-border financial crime. The paper argues that regulatory compliance alone is insufficient; instead, a resilience-based, intelligence-led, ecosystem-wide response is required to safeguard financial stability in the digital era.

****The author is a staff member of the Ghana Association of Banks. The views expressed in this policy brief are solely those of the author and do not necessarily reflect the official position of the Ghana Association of Banks.****

1. Introduction

Ghana's financial sector has experienced significant digital transformation over the past decade. The expansion of mobile banking platforms, integration of mobile money, internet banking solutions, fintech partnerships, instant domestic and international payment systems, agent banking networks, and the integration of the Ghana Card as a primary identification instrument has deepened financial inclusion and significantly improved transactional efficiency.

However, digitization has simultaneously expanded institutional attack surfaces across interconnected digital channels, accelerated transaction velocity, reducing detection and recovery windows, increased anonymity through complex, layered transaction chains, enabled rapid cross-border dissipation of illicit funds and reduced reliance on physical presence, thereby weakening traditional control points

The Bank of Ghana's Annual Fraud Reports consistently highlight a rise in reported fraud attempts, particularly through electronic channels. Complementary data from GAB and FIC demonstrate

increasing sophistication and complexity in suspicious transaction patterns, while law enforcement agencies report greater involvement of organized and sometimes transnational criminal networks.

This paper explores the intersection between digital banking growth and financial crime risk in Ghana and assesses regulatory expectations in this evolving supervisory landscape.

2. Regulatory Context

Globally, digital transformation correlates with shifts in fraud typologies (Levi,2023; FATF, 2022). Emerging markets face heightened vulnerability due to rapid digital adoption outpacing regulatory evolution, cross-border remittance exposure and foreign exchange pressures, informal sector interfaces with formal banking channels, and weak cross-jurisdiction enforcement mechanisms among other related concerns.

In Ghana, the regulatory framework governing financial crime includes:

- **Banks and Specialised Deposit-Taking Institutions Act, 2016 (Act 930)** providing prudential oversight authority to the Bank of Ghana, including enforcement powers relating to governance failures and risk management deficiencies and providing high level regulation to the application of risk and governance structures in impacted financial institutions.
- **BOG/FIC AML/CFT&P Guideline, 2026** clearly provides operational guidance on policy framework, governance, due diligence, STR filing, transaction monitoring, sanctions screening, and risk-based supervision.
- **Anti-Money Laundering Act, 2020 (Act 1044)** which establishes comprehensive AML/CFT obligations, including customer due diligence, beneficial ownership identification, reporting of suspicious transactions, and enhanced monitoring of politically exposed persons (PEPs) and applicable sanctions.
- **Payment Systems and Services Act, 2019 (Act 987)** which regulates electronic money issuers, payment service providers, and fintech participants. This is critical, given the increasing fraud exposure within digital payment ecosystems.
- **Cybersecurity Act, 2020 (Act 1038)** also Introduces obligations relating to cyber incident reporting, critical information infrastructure protection, and digital evidence preservation.
- **The Guidelines on Operations of Electronic Payment Channels** provides a framework for the management of an efficient and secure transmission of electronic transactions across various payment channels, specifically point of sales and Automated Teller Machines.

In addition several applicable regulations, guidelines and notices deployed by competent authorities such as the applicable Ghana Card notices from BOG and SEC make reference to due diligence measures as well as the requirement to biometrically verify third parties via the Ghana card for onboarding, ongoing due diligence and transactions.

The Bank of Ghana has progressively strengthened supervisory oversight, emphasizing risk-based supervision, governance accountability, cyber resilience, and enhanced fraud reporting requirements. The supervisory shift has increasingly focuses on effectiveness rather than mere policy existence.

3. Methodological Approach

This study employs a qualitative and documentary analysis approach based on:

- Bank of Ghana Annual Fraud Reports used to assess multi-year fraud trend trajectories, typology evolution, and sectoral exposure levels.
- GAB Quarterly Fraud Reports which provide near-real-time industry intelligence and interbank fraud movement patterns.
- FIC Annual Reports and STR/SAR Trend Summaries used to evaluate suspicious transaction growth, typology shifts, and money laundering layering patterns.
- Public Reports from EOCO, OSP, and Ghana Police Service which offer enforcement insight into prosecution challenges, asset recovery constraints, and organized crime patterns.
- Industry Consultations and Observed Enforcement Patterns to supplement documentary evidence with practitioner-level perspectives.

The objective is to identify structural patterns and systemic vulnerabilities rather than isolated case incidents.

4. Emerging Fraud Trends in Ghana's Banking Sector

4.1. Digital Channel Fraud

Recent BoG reports indicate increasing fraud attempts through mobile banking platforms, internet banking portals, card-not-present (CNP) transactions, and agent banking ecosystems

The most dominant techniques include Phishing campaigns targeting login credentials, Vishing schemes exploiting customer trust, SIM swap fraud enabling account takeover, Malware-assisted credential harvesting, and Business Email Compromise (BEC) targeting corporate clients.

The defining characteristic of digital fraud is velocity. Funds can be transferred across multiple institutions and borders within minutes, often structured into smaller amounts to evade threshold detection. This significantly reduces the recovery window and increases reliance on real-time monitoring systems.

4.2. Identity-Driven Fraud and Ghana Card Vulnerabilities

The Ghana Card has materially strengthened KYC integrity and reduced certain forms of identity misrepresentation. However, fraud cases reveal new vulnerabilities, including forged or digitally altered identity documentation, fraudulent acquisition of Ghana Cards using false foundational data, synthetic identities combining legitimate and fabricated data elements, exploitation of remote onboarding processes with limited physical and biometric verification and use of intermediaries or agents to bypass enhanced due diligence controls

Additionally, operational uncertainty regarding photocopying restrictions has introduced compliance tension between identity protection and documentation retention requirements. Financial institutions must balance data privacy considerations with audit trail obligations and fraud investigation needs.

The increasing reliance on digital onboarding without biometric revalidation presents a structural vulnerability that requires stronger API-based verification and liveness detection technologies.

4.3. Cross-Border Debit Card and FX Arbitrage Abuse

Industry data indicate coordinated use of debit cards outside Ghana to exploit foreign exchange differentials. These schemes typically involve high-frequency transaction bursts within short time intervals, fragmented withdrawals across multiple ATMs or POS terminals, deployment of mule accounts for transaction routing, collusion with foreign merchants or payment intermediaries, and exploitation of system latency in FX repricing

This typology extends beyond institutional fraud losses and introduces macroeconomic implications, particularly regarding foreign currency outflows and FX reserve pressure. In periods of currency volatility, such coordinated arbitrage can exacerbate systemic liquidity stress adversely impacting the Net Open Position (NOP) of financial institutions and negatively impacting the regulator's FX management strategies.

4.4. Insider-Enabled Fraud

Although this is less frequent than customer-driven fraud, insider cases produce significantly higher per-case losses. Common patterns include manipulation of dormant or inactive accounts, overriding internal system controls, suppression or deletion of transaction alerts, collusion with external fraud syndicates and unauthorized privilege escalation within core banking platforms.

Insider fraud exposes governance and tone-at-the-top deficiencies. It often reflects weak internal control structures including a lack of segregation of duties, inadequate system access reviews, and ineffective whistleblower mechanisms.

BoG supervisory expectations increasingly place responsibility on Boards to ensure robust internal control environments, regular audit testing, fit and proper processes for employee onboarding and cybersecurity assurance frameworks.

4.5. Money Laundering and Proceeds Concealment

FIC data show rising Suspicious Transaction Reports linked to rapid layering of fraud proceeds across multiple banks, use of digital wallets and fintech payment rails, conversion into high-value movable assets, structured transactions below reporting thresholds, and emerging exposure to cryptocurrency exchanges.

A key structural challenge is the compression of time between predicate offense and laundering activity. In digital fraud cases, funds may be fully dissipated before formal reporting and freezing orders are executed. This places pressure on regulatory reforms to enable provisional freezing mechanisms.

5. Law Enforcement and Institutional Challenges

Data from Police CID and EOCO suggest increasing sophistication of organized financial crime networks as well as the use of cross-border facilitators and shell accounts. Despite this, limitations continue in the form of jurisdictional limitations in asset tracing and recovery, procedural delays in obtaining court-issued freezing orders and high evidentiary thresholds prior to intervention.

The time-sensitive nature of digital fraud often outpaces legal processes, resulting in low asset recovery ratios relative to reported fraud values.

There is also fragmentation in data exchange across agencies, citing data privacy issues, lack of technology and adequate archiving systems and processes, hence creating intelligence silos that weaken coordinated enforcement responses.

6. Regulatory Expectations in the Digital Era

The Bank of Ghana's supervisory posture increasingly emphasizes the following:

6.1. Effectiveness Over Formal Compliance

Institutions must demonstrate measurable fraud mitigation outcomes rather than merely policy documentation. This includes reduction in successful fraud ratios, timely STR filing, demonstrable alert-to-investigation turnaround time, and independent validation of AML system effectiveness.
Supervisory reviews increasingly assess control performance metrics rather than procedural existence.

6.2. Board-Level Oversight

Fraud and cyber risk must be embedded within enterprise risk governance. Boards are expected to regularly review fraud dashboards, approve fraud risk appetite statements. ensure management investment in technology and skills, oversee cybersecurity stress testing, demand independent internal audit validation and ensure the formation of dedicated fraud department managed by highly trained and skilled professionals.

Regulatory expectations increasingly treat fraud risk as a governance issue rather than an operational anomaly. Greater attention must be focused on creation of a fully functional and independent fraud department with direct reporting lines to either the Managing director or a board sub-committee for effective and efficient fraud detection, prevention and deterrent mandate.

6.3. Real-Time Monitoring Capabilities

Delayed batch monitoring is no longer sufficient in a real-time payment ecosystem.

Real time AI-driven transaction monitoring, behavioral analytics, anomaly detection systems, and automated alert escalation frameworks are increasingly expected.

Financial Institutions should be required to monitor transaction velocity and geolocation anomalies, deploy multi-factor authentication mechanisms, integrate sanctions screening into payment workflows and establish 24/7 fraud response centers.

6.4. Collaborative Intelligence Sharing

Regulators must encourage structured engagement across institutions and agencies. This includes cross-bank fraud alert sharing, joint typology development forums, data-sharing frameworks with FIC, dedicated liaison desks with law enforcement, and industry-wide fraud awareness campaigns.

Financial crime defense must transition from isolated institutional response to ecosystem-wide intelligence integration.

7. Strategic Policy Recommendations

1. Establish an Industry-Wide Fraud Intelligence Unit with a centralized platform under GAB coordination to enable real-time fraud signal sharing, mule account flagging, and typology dissemination.
2. Develop Standardized Rapid-Freezing Protocols pre-agreed inter-agency templates to reduce legal delays in freezing suspicious funds during the critical early hours of fraud detection.
3. Strengthen API-Based Ghana Card Integration with Direct biometric and liveness verification integration with the National Identification Authority to reduce synthetic identity risk.
4. Enhance ECOWAS-Level Cooperation structured cross-border information exchange and asset recovery frameworks to address transnational fraud syndicates.
5. Invest in AI-Enabled Detection Platforms and Shift from rule-based monitoring to predictive analytics and behavioral anomaly detection systems.
6. Reform Procedural Bottlenecks in Asset Freezing by Introducing provisional administrative freezing mechanisms subject to judicial confirmation to preserve assets during investigations.

8. Conclusion

Ghana's banking sector stands at a critical juncture. Digital innovation has deepened inclusion, efficiency, and competitiveness. However, financial crime has evolved in parallel, becoming faster, more organized, cross-border in nature, and technologically enabled.

The transition required is from reactive fraud management to predictive, intelligence-led resilience frameworks.

Sustainable financial stability in Ghana's digital era depends on coordinated regulatory enforcement, institutional accountability, technological investment, and ecosystem-wide collaboration.

Compliance is necessary but resilience is indispensable.

REFERENCES

Adzakor, W. K. (2024). The new economy: Impact of financial digitalization on Ghana's public sector. Jurnal Pengelolaan Keuangan Publik, 3(2), 68-78.

Financial Action Task Force (FATF), (2022). Annual report 2021–2022: Strengthening global action to tackle money laundering and terrorist financing. Paris: FATF. Available at: https://www.fatf-gafi.org/en/publications/Fatfgeneral/Annual-Report-2021-2022.html

Levi, M. (2023). Frauds in digital society. The SAGE Handbook of Digital Society. London: Sage, 480-500.

Republic of Ghana, (2016). Banks and Specialised Deposit-Taking Institutions Act, 2016 (Act 930). Accra: Government of Ghana.

GHANA ASSOCIATION OF BANKS

Contact Us:

No. 12 Tafawa Balewa Avenue,
GA-029-4444, North Ridge Accra.

+233-0302-667-138 / 0302-670-629

info@gab.com.gh

P.O. Box 41, Accra, Ghana

www.gab.com.gh

FOLLOW US

Ghana Association of Banks
@BankersGhana
@ghanaassociationofbanks
Ghana Association of Banks