



# INDUSTRY FRAUD REPORT

MARCH - MAY 2025



FOLLOW US

 Ghana Association of Banks  
 @BankersGhana

 @ghanaassociationofbanks  
 Ghana Association of Banks



# INTRODUCTION

While the Bank of Ghana's annual fraud reports remain invaluable for retrospective analysis, our industry requires a more immediate, proactive mechanism for disseminating information about prevalent fraud trends and typologies.

At the Ghana Association of Banks (GAB), supporting a course that safeguards the integrity and resilience of Ghana's banking sector is always on our priority list. Fraud remains a persistent threat, evolving in complexity and impact.

This report provides a synthesized yet confidential review of fraud cumulative 37 incidents recorded between March and May 2025. It highlights dominant fraud typologies, outlines their modus operandi, and presents the financial and operational impact across the industry—deliberately anonymized to ensure institutional confidentiality and customer privacy. This initiative is part of our broader commitment to promoting real-time industry alertness and interbank collaboration to fight fraud. We intend to champion this course going forward, by proactively presenting on at least, a quarterly basis to make the fight against fraud in the industry not just, a conscious act but a very close to a real-time activity.





# MARCH 2025: THE ALARMING RISE OF DIGITAL EXPLOITATION

March marked a notable count in fraud incidents stemming from digital platforms, with mobile-based fraud leading the chart. One prominent case involved a client who shared his Mobile Money PIN with an acquaintance, unaware that it was identical to his USSD PIN. This oversight allowed the acquaintance to swiftly transfer funds to multiple wallets and accounts. The incident, which resulted in a successful theft of over GHS 2,800, underscores the danger of reusing PINs across platforms.

Another case reflected how social engineering continues to flourish. A victim was deceived via WhatsApp by an impersonator posing as a globally recognized tech figure “Elon Musk”. The fraudster introduced a fake investment scheme, tricked the customer into sharing OTPs and account credentials, and swiftly initiated unauthorized transfers via mobile banking apps.

Internal weaknesses were also exposed. An

attempted theft of GHS 400 by a bank teller, uncovered through CCTV, highlighted integrity lapses at the frontline. In another incident, a client was manipulated into handing over funds intended for Treasury Bills to a bank staff (the fraudster) who produced a fake deposit slip.

Elsewhere, ATM fraud manifested through unauthorized transactions affecting 31 customers, suggesting possible systemic flaws. In the digital realm, cyber fraud emerged where customer data was exploited to gain unauthorized USSD access, with illicit transfers quickly initiated to external accounts.

Overall, we have considered in March, six major incidents with a total fraud exposure of nearly GHS 39,000. Five out of the six cases were successful, with minimal recovery, drawing attention to customer behavior, weak authentication practices, and the increasing sophistication of social engineering tactics.

The table below presents the six fraud cases considered for the month

NO	TYOLOGY	AMOUNT INVOLVED (GHS)	STATUS
1	USSD Fraud	2,8601	Successful
2	Mobile App Fraud	2,300	Successful
3	Theft	400	Attempted
4	Cash Suppression	25,000	Successful
5	Card/POS Fraud	6,273.58	Successful
6	Cyber and IS Fraud	2,000	Successful

# APRIL 2025: THE INFILTRATION OF INSTITUTIONAL TRUST

April's trend revealed how fraud is evolving from isolated digital scams into complex, often coordinated schemes exploiting institutional blind spots. A particularly shocking case involved the creation of a shell company with a deceptively similar name to a legitimate business. Through this setup, the fraudster intercepted eight cheques amounting to over GHS 3.1 million intended for a partner firm. Due to minor spelling differences and lack of thorough scrutiny by branch staff, these fraudulent cheques were deposited and cleared without detection.

Meanwhile, compromised devices and poor SIM management continued to drive electronic money fraud. Multiple customers reported unauthorized transfers after losing their phones or failing to secure them properly. In one notable incident, over GHS 132,000 was moved from clients' accounts after they were manipulated into sharing OTPs linked to the MTN MoMo app. The seamless execution of these transfers highlights a deep-rooted problem—customers still do not fully understand or respect digital safety protocols.

Cheque fraud also persisted. One case

involved the presentation of a cloned cheque while the customer was abroad. Though the verification call was placed, the fraudster's convincing tactics led to the transaction being approved, revealing vulnerabilities in customer authentication processes.

There was also a significant case of internal collusion involving a teller who altered deposit slips to underreport transaction amounts, siphoning off nearly GHS 65,000. Although the amount was eventually recovered, the case illustrates the urgent need for dual verification systems and the importance of real-time alerts.

The April review captured attempted fourteen (14) fraud cases totaling about GHS 4.1 million with successful ones nearing GHS 3.6 million and GHS 500,000 only attempted but prevented. Recoveries remained low, with control breakdowns in both customer-facing and back-office operations. A critical area of concern was the use of saved Ghana card images without proper verification, enabling a fraudulent cheque transaction valued at GHS 83,000.

The table below presents the fourteen (14) fraud cases considered for the month

NO	TYOLOGY	AMOUNT INVOLVED (GHS)	STATUS
1	Online Scam	27,800 (Recovered 4,893)	Successful
2	Forgery of negotiable instrument	3169432.22	Successful
3	Cheque Fraud	4,800	Attempted
4	E-Money Fraud	19,755	Successful
5	E-Money Fraud	8,050	Successful
6	Mobile Money Fraud	132,010	Successful
7	Cheque Fraud	Attempted: 210,550.00	Prevented (unsuccessful)
8	Cheque Fraud	Attempted GHS 143,000.00 GHS 5,000.00 GHS 5,000.00	Prevented Successful Successful
9	Cheque Fraud	4,800.00	Prevented
10	Cash Suppression	1,250	Successful (but recovered)
11	Fraudulent use of a 3rd Party's Ghana card	83, 000	Successful
12	Internal Fraud	Attempted 65,000	Successful (but recovered)
13	Cyber and IS Fraud	149,800	Successful
14	Cyber and IS Fraud	43,000	Successful



# MAY 2025: FRAUD TAKES A MORE ORGANIZED AND SOPHISTICATED TURN

By May, fraud incidents not only grew in number but also in coordination and financial magnitude. A disturbing scheme saw customers recruited into a fake Jumia online work opportunity. These victims unknowingly received and relayed stolen funds through their accounts, ultimately realizing they were part of a larger laundering network only when payments ceased and contact with the fraudsters was lost.

A notable rise in card fraud was observed, particularly involving unauthorized international online transactions. Affected customers reported strange charges from platforms such as Amazon and Walmart, leading to an internal investigation which identified 181 compromised cards across 136 customer accounts. Although over GHS 15,000 was recovered through chargebacks, the cumulative exposure exceeded GHS 268,000.

E-money fraud continued to plague the sector. In one case, over GHS 99,000 was transferred out of a customer’s account after the client shared email and bank details with a fake travel agent. The fraudster gained access to her Gmail, intercepted OTPs, and onboarded her onto the mobile banking app.

Other cases featured victims who delayed reporting phone thefts, allowing fraudsters unimpeded access to USSD and mobile banking services, leading to losses ranging from GHS 3,000 to over GHS 21,000.

The report also captured a resurgence in phishing. Victims were lured into entering card details on spoofed hotel booking platforms and gaming websites, leading to unauthorized debits. In total, phishing-related frauds for May exceeded GHS 70,000.

A major internal fraud case was also recorded involving over GHS 51,000 in policy repayment funds that were never deposited. Staff complicity was suspected and the case has since been escalated to law enforcement.

In terms of financial exposure, the month of May alone recorded frauds exceeding GHS 1 million, with just under GHS 200,000 recovered. Alarminglly, many of these cases showcased fraudsters leveraging loopholes in digital ecosystems, social behavior, and internal controls.

The table below presents the seventeen (17) fraud cases considered for the month

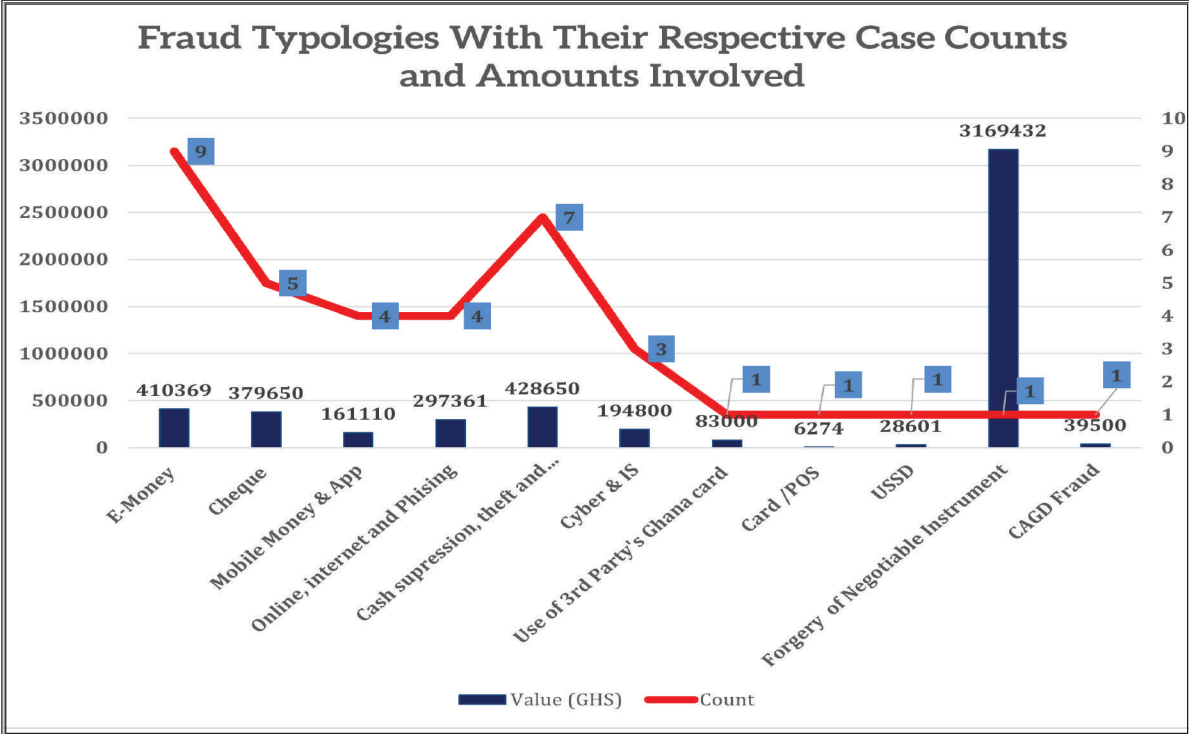
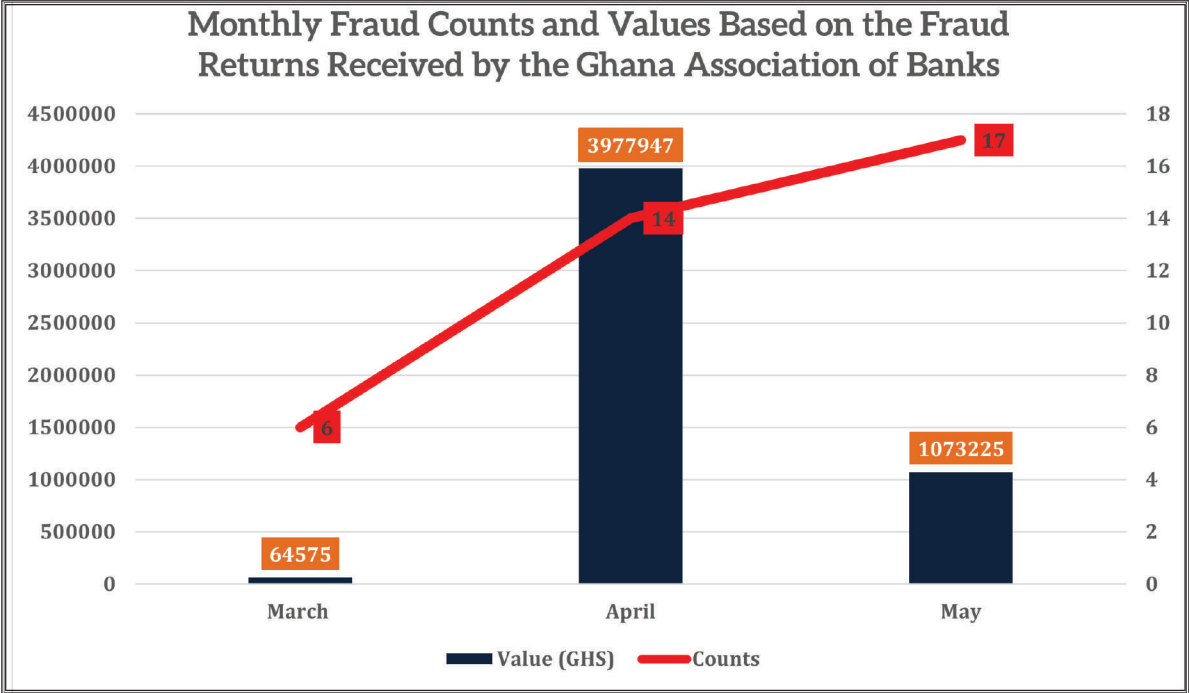
NO	TYOLOGY	AMOUNT INVOLVED	STATUS
1	Online Scam	GHS27,800 (Recovered GHS 4893)	Successful
2	External Fraud (E-Money)	Attempted: GHS 268364 Recovered: GHS15017.13 Loss: 253,347.06	Successful
3	Cyber and IS Fraud	GHS 2000	Successful
4	External Fraud (E-Money)	GHS4,580.00	Successful
5	Internet Banking Fraud	GHS199,640	Successful
6	E-Money Fraud	GHS 99,700.00	Successful
7	CAGD Loan Fraud	Attempted: 39,500.00 Recovered: 39,500.00	successful
8	Mobile money fraud	GHS 5,800.00	successful
9	Mobile money fraud	GHS 21,000.00	Successful
10	Phishing	GHS 58,000.00	Successful
11	Phishing	GHS 11,921.16	Successful
12	Misappropriation of funds	GHS 274,000.00 Recovered: GHS 170,760.53	Successful
13	Cash Theft	GHS 51,000.00	Successful
14	E-Money Fraud	GHS 3000	Successful
15	E-Money Fraud	GHS 4300.00	Successful
16	E-Money Fraud	GHS 2000	Successful
17	E-Money Fraud	GHS 620	Successful

# CROSS-MONTH ANALYSIS: THE TRENDS, THREATS, AND TAKEAWAYS

Between March and May 2025, the total fraud-related value reported by member institutions exceeded GHS 5.1 million with a recovery rate of only 5.10% (GHS 260,000 across these months). Surprisingly only GHS 570,000 (representing 11.18%) worth of fraud was prevented due to timely detection and interbank collaboration.

## The most prevalent fraud vectors were:

- **E-Money & Mobile Banking Fraud:** Often initiated through device theft, SIM hijacking, or customer negligence.
  - **Cheque & Forgery Schemes:** Involving cloned or intercepted instruments and fraudulent corporate setups.
  - **Card & Internet Banking Fraud:** Capitalizing on weak cybersecurity postures and customer naivety.
  - **Phishing & Social Engineering:** Growing rapidly through WhatsApp, spoofed websites, and digital impersonation.
  - **Internal Collusion:** Persistent cases involving tellers, sales agents, and administrative insiders.
- Key enabling factors include widespread sharing of OTPs and PINs, unreported SIM or phone losses, weak staff scrutiny, and outdated system access protocols. While most frauds were successful due to social engineering and compromised security, a few were averted due to prompt client feedback and institutional vigilance. Below is a summary of the prevailing typologies with case counts and values involved from March to May 2025.





# STRATEGIC RECOMMENDATIONS FOR BANKS

## 1. Customer Education Must Intensify:

Campaigns on device encryption, phishing detection, and reporting protocols should be relentless.

## 2. Real-Time Alerting Systems:

SMS, email, and app notifications should be configured for immediate delivery with enhanced fraud markers.

## 3. Staff Integrity and Ethics Training:

Continuous education on conduct, especially for frontline and back-office staff.

## 4. Chequebook and Ghana Card Protocol Reviews:

Introduce stronger ID verification and double confirmation procedures.

## 5. Industry-wide Data Sharing (confidential):

Promote cross-institution collaboration through anonymized intelligence like this report. The Ghana Association of Banks remains a committed facilitator to collectively fight fraud.

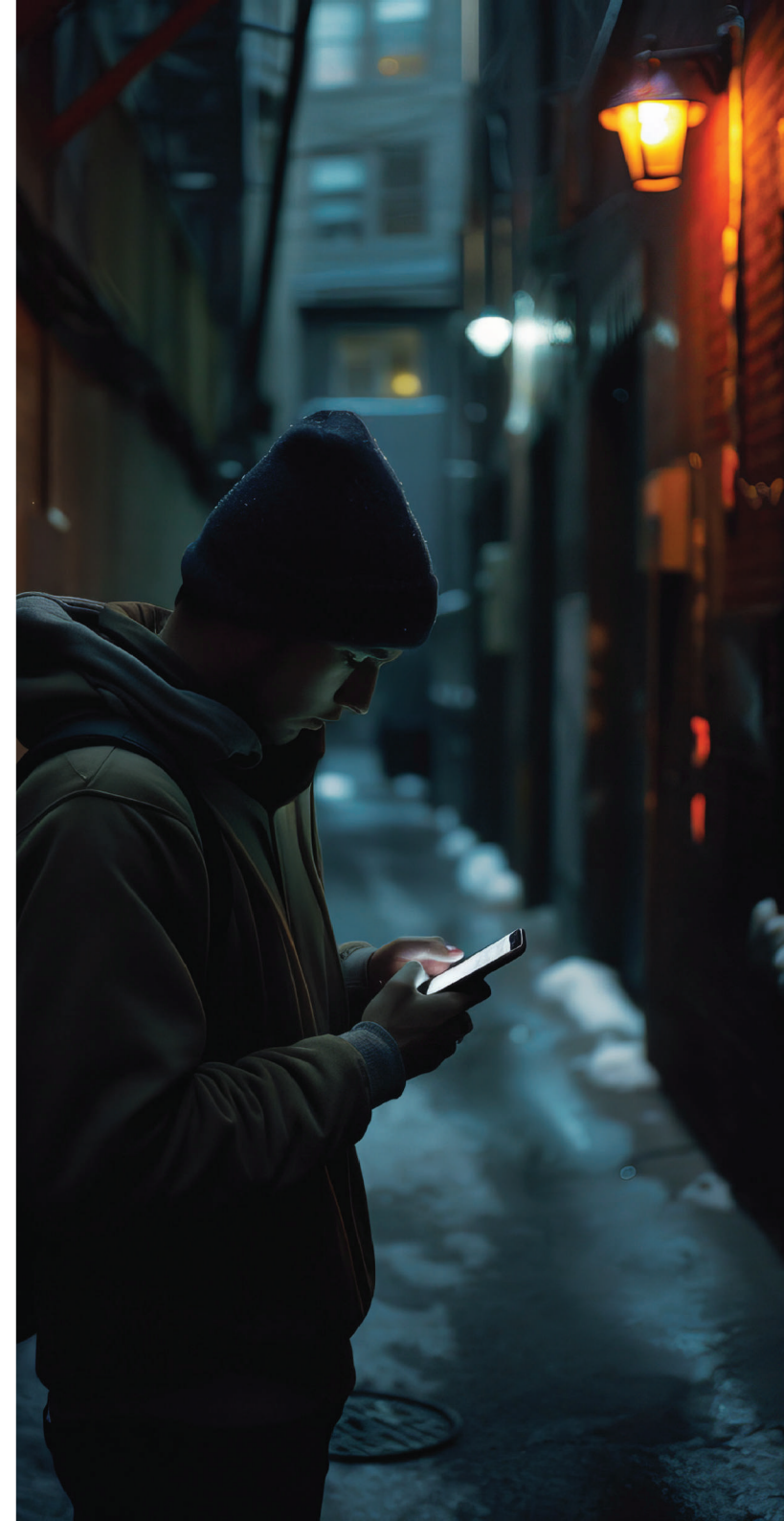
## 6. Digital Access Control Audits:

Restrict admin privileges, implement stronger Multi-Factor Authentication (MFA) enforcement, and continuously monitor system logs.

# CONCLUSION

Fraud is no longer a sporadic event; but rather it is a coordinated, adaptive threat that requires industry-wide collaboration, constant vigilance, and proactive education. The Ghana Association of Banks reaffirms its commitment to leading a coordinated response that places early detection, swift reporting, and preventative education at the heart of its fraud risk strategy.


This report is a call to collective action. By sharing these insights confidentially and acting upon them, we can create a more secure and resilient financial sector for Ghana.[td](https://ghana.gov.gh)






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



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