



# INDUSTRY FRAUD REPORT

JUNE - AUGUST 2025



FOLLOW US

 Ghana Association of Banks  
 @BankersGhana

 @ghanaassociationofbanks  
 Ghana Association of Banks

# EXECUTIVE SUMMARY

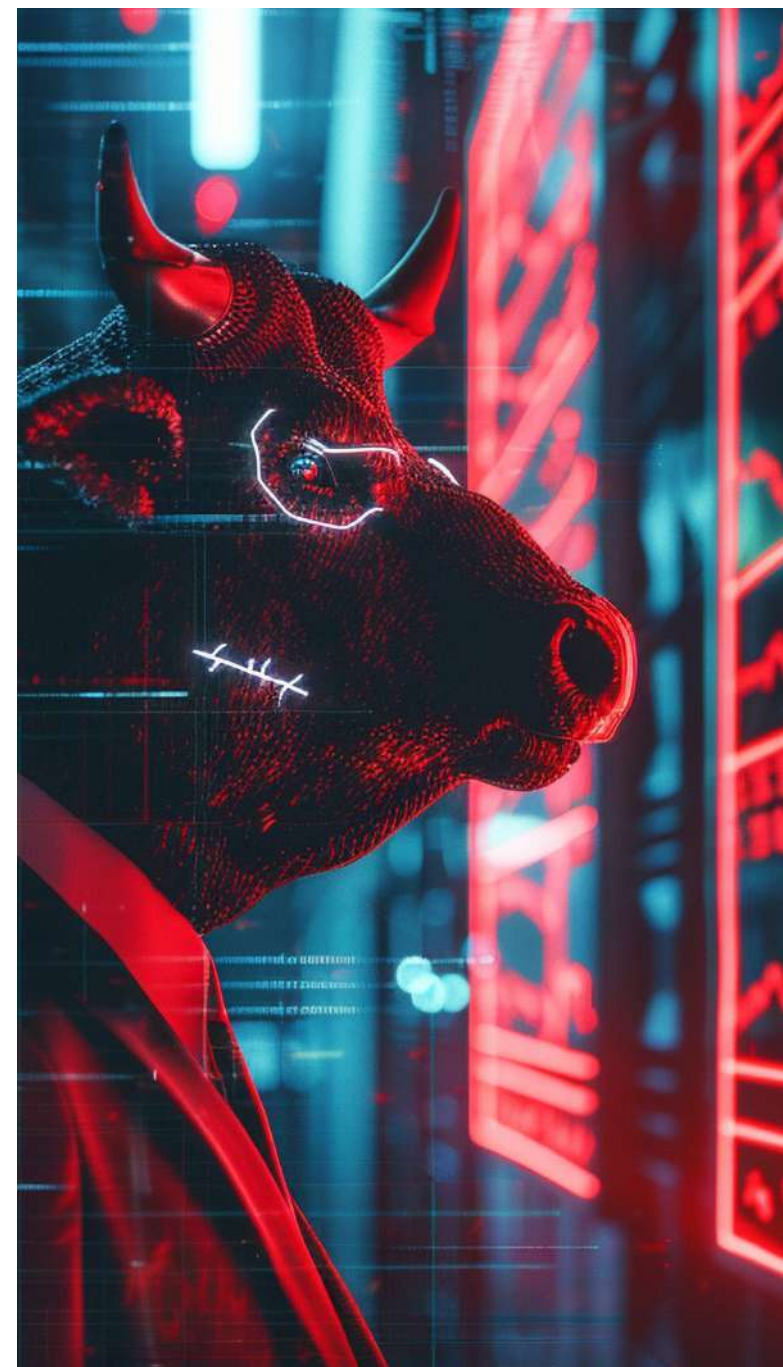
The Ghana Association of Banks' (GAB) Fraud Trend Report for June to August 2025 highlights a critical period in which member banks recorded 44 fraud incidents across nine typologies. The cumulative value of attempted fraud during the quarter amounted to GHS 4.7 million. Out of this exposure, banks recovered GHS 0.9 million resulting in a net industry loss of GHS 3.8 million. These figures underscore both the scale of financial crime and the urgent need for targeted interventions.

Losses during the period were heavily concentrated in cash suppression and cheque fraud, which alone accounted for more than GHS 2.0 million in net losses representing about 43% of the GHS 3.8 million losses recorded per the reported case. making it the single largest driver of industry exposure. Equally concerning was the rise in digital, mobile, and e-money fraud, which together contributed over GHS 1.1 million in exposures. Recovery rates for these channels were almost negligible due to the speed with which fraudsters executed transfers, layered transactions, and withdrew funds through mobile money agents. This trend signals the vulnerability of Ghana's growing digital finance ecosystem, where convenience and accessibility have outpaced the strength of existing security frameworks.

The report also draws attention to internal fraud and insider collusion, which saw notable spikes in August either through internal fraud or / document manipulation recorded close to 50% of the total 7cases recorded. Cash suppression and teller malpractices continue to erode trust in banking operations, despite stronger surveillance and audit systems. In contrast, banks recorded greater success in identifying and blocking document and visa forgeries, with verification systems enabling early detection. This divergence reveals a systemic imbalance: while verification controls on documentation are proving effective, digital authentication and cash-handling protocols remain weak points.

A recurring theme across most cases is the human factor. Customers were deceived through social engineering attacks, where fraudsters impersonated officials and created a sense of urgency to extract One-Time Passwords (OTPs) and credentials. Similarly, device-related vulnerabilities, particularly such as SIM reissuance and stolen phones enabled unauthorized access to bank accounts. The reliance on SMS-based OTPs has proven inadequate, as fraudsters continue to exploit telecom weaknesses and bypass security safeguards.

The implications for the industry extend beyond financial losses. The persistence of forged bank statements and fraudulent visa applications creates reputational risks, both domestically and internationally. Such incidents could invite



increased regulatory scrutiny and diminish trust in Ghana’s financial sector and impugn the integrity of banks’ statements of banks by embassies and high commissions if not addressed decisively.

In response, the report outlines a multi-layered strategy. Immediate measures must focus on strengthening authentication protocols by moving beyond SMS OTPs to phishing-resistant multi-factor authentication, coupled with real-time transaction monitoring across e-money and wallet channels. Operational reforms are equally critical: tighter cash-handling procedures, dual verification, surprise audits, and teller rotation can help mitigate internal fraud. At the industry coordination level, GAB should spearhead partnerships with telecommunications companies, regulators, and law enforcement to establish a central fraud registry, fast-track SIM-change alerts, and promote intelligence sharing.

Finally, sustained customer education remains indispensable. Fraudsters are increasingly exploiting behavioural vulnerabilities rather than technological weaknesses. Targeted campaigns, particularly for vulnerable groups, are essential to reinforce the message that customers must never disclose OTPs or account details under pressure.

In conclusion, the June–August 2025 fraud trends reveal a financial ecosystem under significant strain from both technological threats and internal control lapses. Without decisive

action, the growing digitization of financial services will continue to magnify losses. For the Board and executive leadership, the priority must be clear: invest in stronger fraud-resistant authentication, enhance operational discipline

in cash management, and deepen cross-industry collaboration. These interventions will not only reduce financial losses but also safeguard the reputation and stability of Ghana’s banking industry.

Typology	Number of Cases	Total Amount Involved	Amount Recovered	Net Loss
Social Engineering	4	GHS 371,900	GHS 10,000	GHS 361,900
Unauthorized Account Access / Transfers	4	GHS 73,900	GHS 0	GHS 73,900
Cash Suppression and Cheque Fraud	9	GHS 2,191,828.50	GHS 177,639.50	GHS 2,014,189
Document Forgery / Bank Statement	7	GHS 287,868.00	GHS 279,868.00	GHS 8,000
Mobile / Digital Banking Fraud	7	GHS 768,787.95	GHS 0	GHS 768,787.95
Card / POS / ATM / USSD Fraud	6	GHS 298,857.76	GHS 150,250.53	GHS 148,607.23
E-Money Fraud	3	GHS 370,572	GHS 0	GHS 370,572
Internal Fraud	2	GHS 306,687.18	GHS 271,200	GHS 35,487.18
Account Takeover Fraud	2	GHS 18,130	GHS 18,130	
Total	44	GHS 4,687,530.39	GHS 888,958.03	GHS 3,798,572.36



# INTRODUCTION

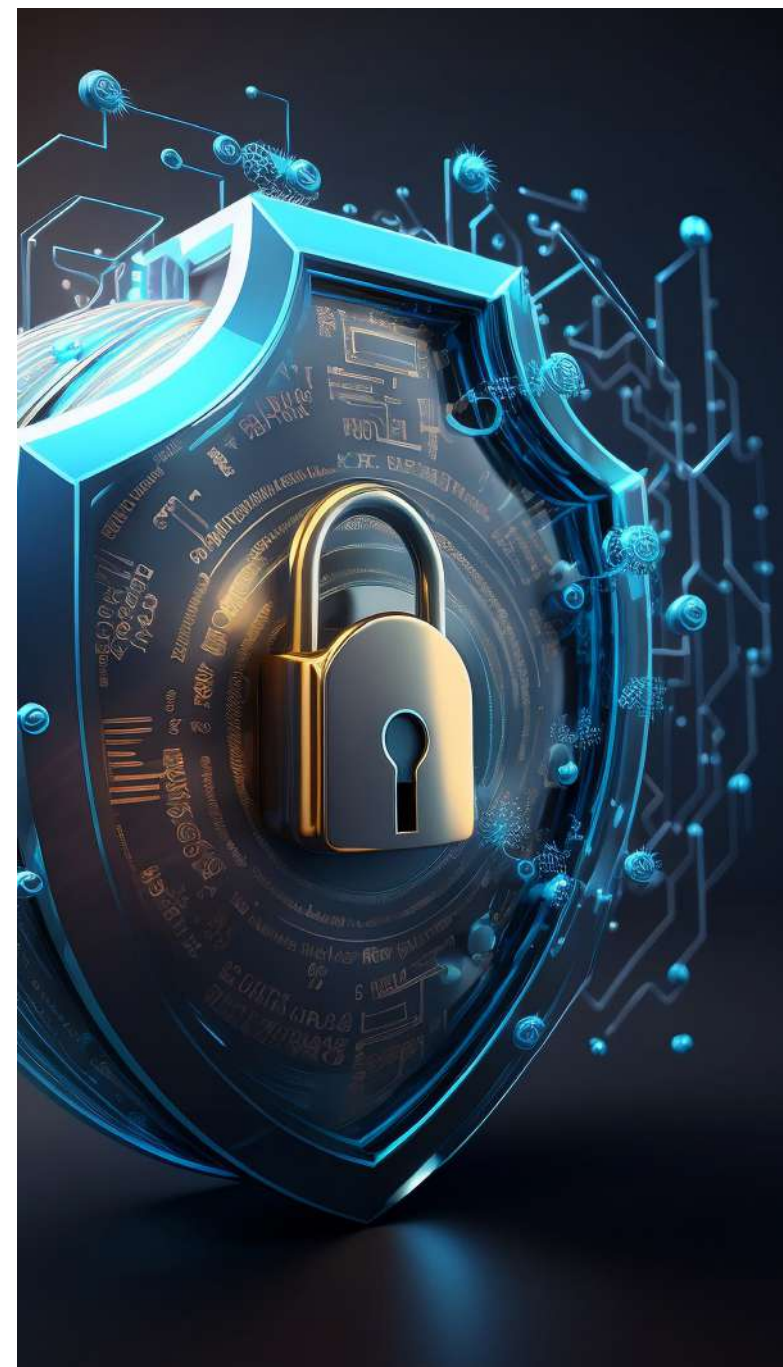
At the Ghana Association of Banks (GAB), supporting a course that safeguards the integrity and resilience of Ghana's banking sector is always on our priority list acknowledging that the soundness and integrity of the financial sector are critical pillars of economic stability and public trust. In Ghana, the rapid expansion of digital financial services has increased convenience and broadened access, but it has also created new entry points for fraud. Both the Bank of Ghana (BoG) and the Ghana Association of Banks (GAB) have consistently highlighted the evolving nature of financial crime, emphasizing its implications for operational resilience, consumer confidence, and systemic stability.

The Bank of Ghana's 2024 Annual Fraud Report, published in April 2025, provides a national benchmark for understanding these dynamics. It revealed that fraud cases across banks, Specialized Deposit-Taking Institutions (SDIs), and Payment Service Providers (PSPs) rose by 5% in 2024, from 15,865 cases in 2023 to 16,733 cases in 2024. This increase corresponded to a 13% rise in value at risk, from GHS 88 million in 2023 to approximately GHS 99 million in 2024. The data further showed divergent sectoral patterns: while banks and SDIs experienced a decline in

the number of attempted fraud cases, the PSP sector recorded a notable increase. Importantly, forgery and manipulation of documents surged seven-fold to GHS 53 million, accounting for 67% of the total value at risk in banks and SDIs. At the same time, declines were observed in cyber/email fraud, fraudulent withdrawals, and cash suppression. The report also underscored the persistent challenge of low recovery rates, largely due to prolonged legal proceedings that discourage financial institutions from pursuing restitution.

It is against this national backdrop that the GAB Fraud Trend Report for June to August 2025 must be understood. While the BoG report provides an annual, sector-wide perspective, the GAB report offers a quarterly, industry-specific analysis of fraud typologies and losses among member banks. During this three-month period, 44 incidents were reported across nine typologies, with a total exposure of GHS 4.7 million. Recoveries were modest, amounting to GHS 0.9 million a net industry loss of GHS 3.8 million. The GAB findings mirror several of the BoG's broader trends, particularly the rising threat of digital fraud and impersonation and the ongoing risks of internal collusion and cash-handling lapses.

The alignment between the BoG and GAB reports illustrates two key realities. First, fraud in Ghana's financial sector is no longer confined to traditional methods such as cheque manipulation and cash theft; it has

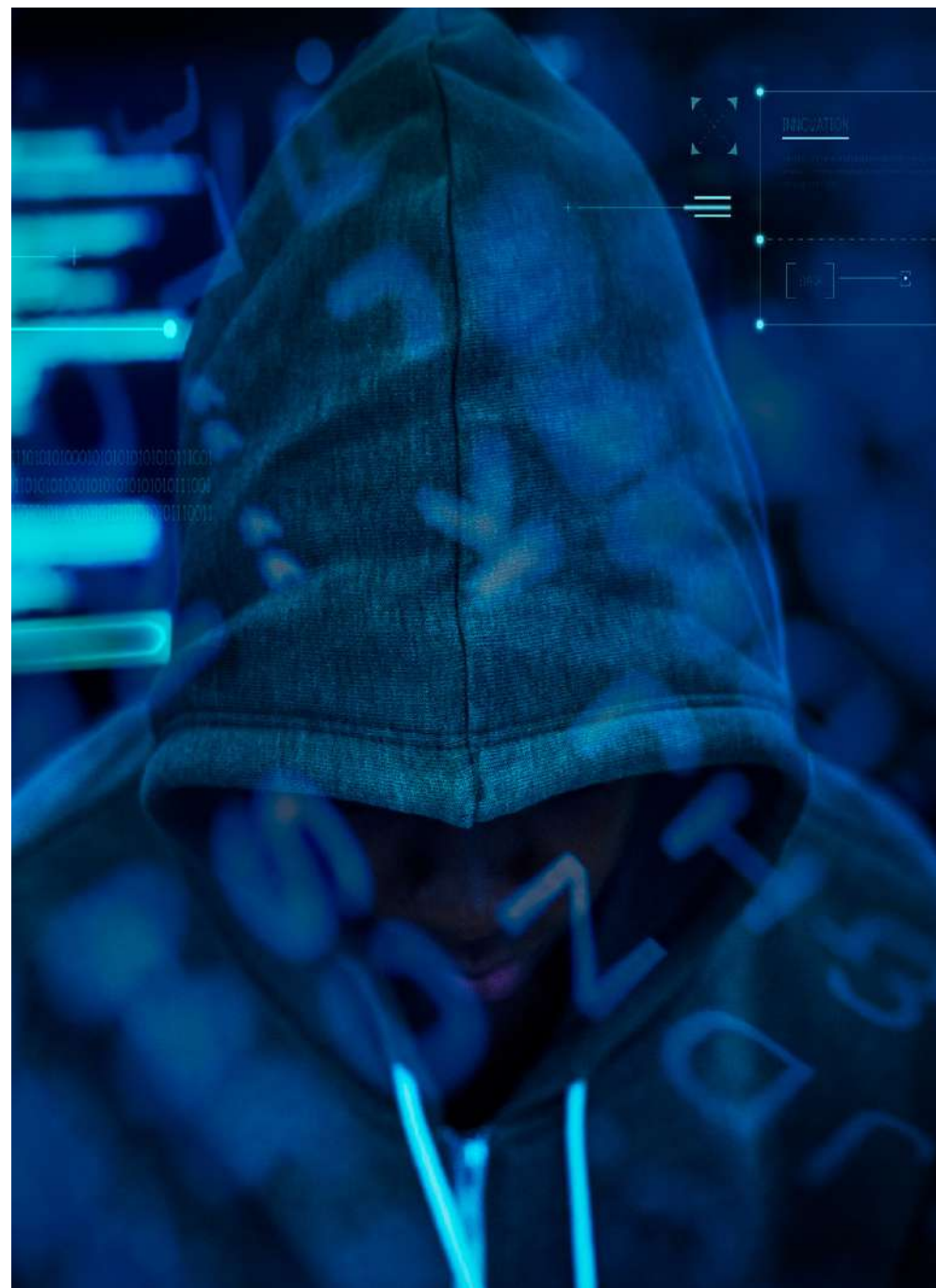


shifted decisively toward digital platforms and document forgery, where detection is harder and recoveries are lower. Second, the persistent role of human behaviour—whether through social engineering of customers or insider collusion, remains central to fraud risk, underscoring the need for stronger operational controls and customer sensitization.

While the Bank of Ghana’s annual fraud reports provide invaluable retrospective insights, the evolving nature of fraud requires a more immediate and proactive industry mechanism for information sharing. Our aim is to complement the BoG’s work by offering quarterly, forward-looking intelligence that highlights emerging fraud typologies, documents their modus operandi, and illustrates their operational and financial impacts in real time.

Our maiden publication, covering March to May 2025, reviewed 37 reported incidents and provided actionable insights to guide fraud prevention strategies. In this second report, we present 44 new and more complex cases, analyzed with the same rigor and presented with detailed narratives of the surging schemes observed. As with previous editions, all identifying information has been anonymized to preserve institutional confidentiality and customer privacy.

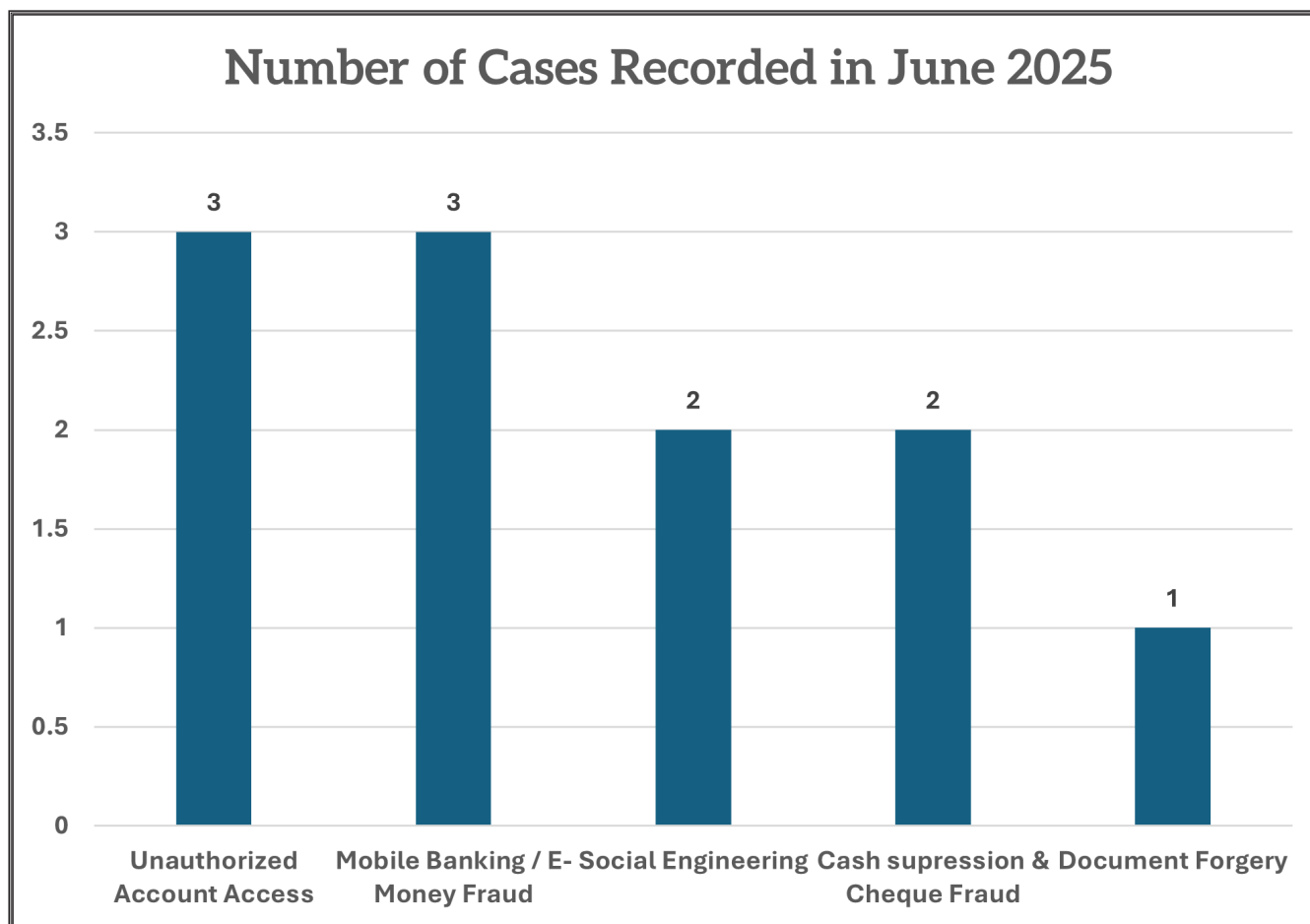
This initiative reflects our broader commitment to promoting real-time industry alertness and interbank collaboration. By publishing these reports quarterly, we seek to transform fraud management from a reactive exercise into a continuous, near real-time defensive practice. We encourage our member banks to incorporate these insights into their day-to-day strategies and urge our customers to remain vigilant. Together, through shared responsibility and proactive engagement, we can foster a safer and more resilient banking environment in Ghana.



# THE NARRATIVE IN JUNE 2025

The fraud landscape in June revealed how diverse and persistent criminal methods have become, ranging from external social engineering to insider collusion within banking halls. A recurring pattern throughout the month was the exploitation of mobile and digital channels. Fraudsters took advantage of the banking sector's integration with telecom operators, using carefully scripted phone calls to impersonate support staff. By instilling fear and urgency, they tricked customers into revealing one-time passwords, which were then used to authorize transfers from bank accounts into Mobile wallets. Once the funds landed in these wallets, they were layered across several accounts and quickly withdrawn at agent points. This form of social engineering proved particularly effective because customers were often convinced they were dealing with legitimate officials.

Closely related to this were incidents involving device theft and number reassignments. In some cases, stolen smartphones gave fraudsters immediate access to mobile banking applications because credentials were saved on the devices or auto-login was enabled. In other instances old phone numbers belonging to customers had been reissued by telecom operators whilst the numbers were linked to the mobile banking applications of the previous owners, allowing





fraudsters to reset banking credentials and gain unauthorized access. These incidents highlighted the vulnerabilities created when customers do not secure their devices and when banks and telecom operators fail to coordinate adequately on SIM reassignments. Email compromise added another layer of risk, as fraudsters infiltrated customer inboxes, redirected OTPs, and quietly authorized transactions without the knowledge of the victims. Together, these cases showed that customers' personal habits around digital security are often the weakest link in the chain.

Card fraud was also evident in June, with fraudsters exploiting online merchant platforms to carry out card-not-present transactions. They frequently executed small, repeated debits, which allowed them to bypass detection while still accumulating sizeable sums. These incidents led to chargeback requests and refunds, but they reminded the industry that global card fraud trends remain a local risk, especially when merchants do not enforce secure protocols like 3-D Secure. Traditional methods of fraud also persisted, particularly in the form of forged cheques and falsified supporting documents. In some cases, goods were supplied against cheques that later bounced, leaving victims exposed. This reaffirmed that while digital fraud is on the rise, analogue methods still pose significant threats when verification is lax.

Internal fraud contributed its own share of cases. Instances of cash suppression were reported, where tellers or relationship officers accepted

deposits but failed to credit customer accounts. Some engaged in deliberate miscounting, while others suppressed funds until reconciliation exposed the shortfalls. Although recoveries were made in several of these cases, the repeated nature of such incidents emphasized weaknesses in cash-handling oversight. Mandatory dual verification at the counter, real-time reconciliations, and CCTV monitoring emerged as critical measures to close these gaps. Overall, the June incidents painted a picture of a fraud environment that is increasingly multi-layered. External actors relied heavily on

social engineering, exploiting customers' trust and the convenience of telecom integration, while internal staff misused their positions to divert funds. Whether through a stolen phone, a reissued SIM card, a forged cheque, or suppressed cash at the counter, the fraudsters' central strategy was speed – moving funds quickly before detection could occur. The month's lessons were clear: banks and telecoms must strengthen their joint controls, customers must be educated to guard their credentials, and institutions must maintain strict oversight of staff handling cash and sensitive processes.

Summary of the fraud cases as reported in June 2025

Typology	Number of Cases	Amount Involved (GHS)	Amount Recovered (GHS)	Net Loss (GHS)
Social Engineering	2	172,000	0	172,000
Unauthorized Account Access	3	23,900	0	23,900
Cash suppression & Cheque Fraud	2	408,105	0	408,105
Mobile Banking / E-Money Fraud	3	329,241	0	329,241
Document Forgery	1	147,100	147,100	0
Card / POS Fraud	1	39,046.14	0	39,046.14
Total	11	1,509,392.14	147,100	1,362,292.14

# TPOLOGY-WISE INSIGHTS IN JUNE 2025

During June 2025, member banks of the Ghana Association of Banks (GAB) reported a range of fraud cases across multiple typologies, highlighting both operational and digital vulnerabilities in the sector.

Social Engineering Fraud led the reported cases, with two successful incidents totaling GHS 172,000 and no recovery. Fraudsters employed psychological manipulation and digital impersonation to deceive staff and customers, underscoring the persistent sector-wide vulnerability to human-targeted attacks. This highlights the need for continuous staff training and customer education.

Closely linked to this, Unauthorized Account Access was recorded in three cases totaling GHS 23,900, all successful and unrecovered. These incidents exposed weaknesses in account authentication and transaction monitoring across member banks, emphasizing the importance of multi-factor authentication, real-time alerts, and anomaly detection systems.

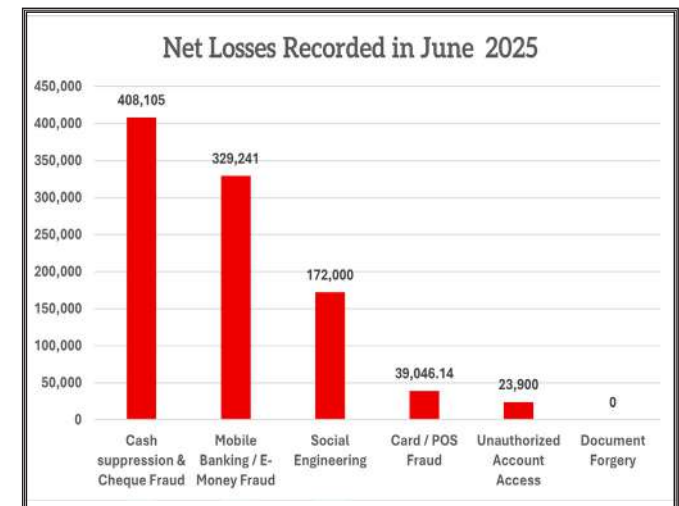
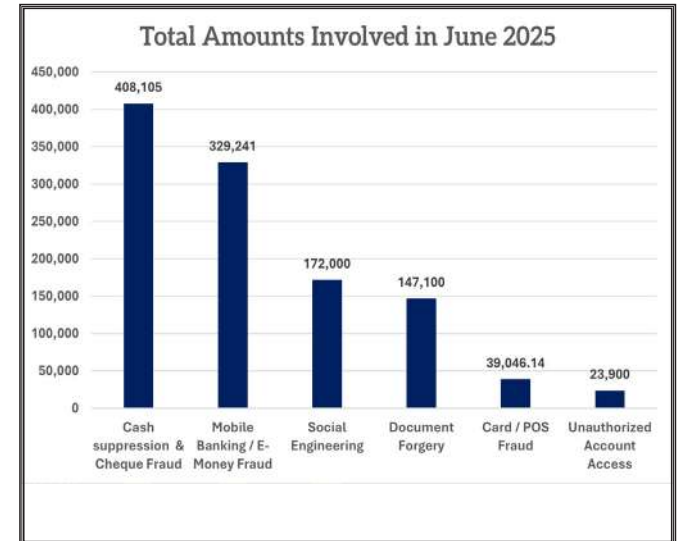
Cash suppression and Cheque Fraud followed, with two cases—including cash suppression and cheque fraud—amounting to GHS 408,105. The absence of recoveries in these cases highlights

operational vulnerabilities in cash handling and cheque processing, reinforcing the need for rigorous internal controls, segregation of duties, and regular audits.

The growing prominence of digital channels was evident in Mobile Banking and E-Money Fraud, where three successful cases totaling GHS 329,241 were reported with no recoveries. The trend demonstrates that fraudsters are increasingly targeting electronic banking platforms, emphasizing the critical need for enhanced cybersecurity, transaction monitoring, and customer awareness initiatives.

In contrast, Document Forgery showed a successful recovery. One case totaling GHS 147,100 was fully recovered, reflecting the effectiveness of verification processes and internal controls. Nevertheless, continued vigilance is essential, especially for high-value or visa-related transactions.

Finally, Card / POS Fraud accounted for one case totaling GHS 39,046.14, which was unrecovered. This indicates ongoing sector-wide exposure to electronic payment fraud and underscores the need for real-time monitoring and proactive fraud detection mechanisms.

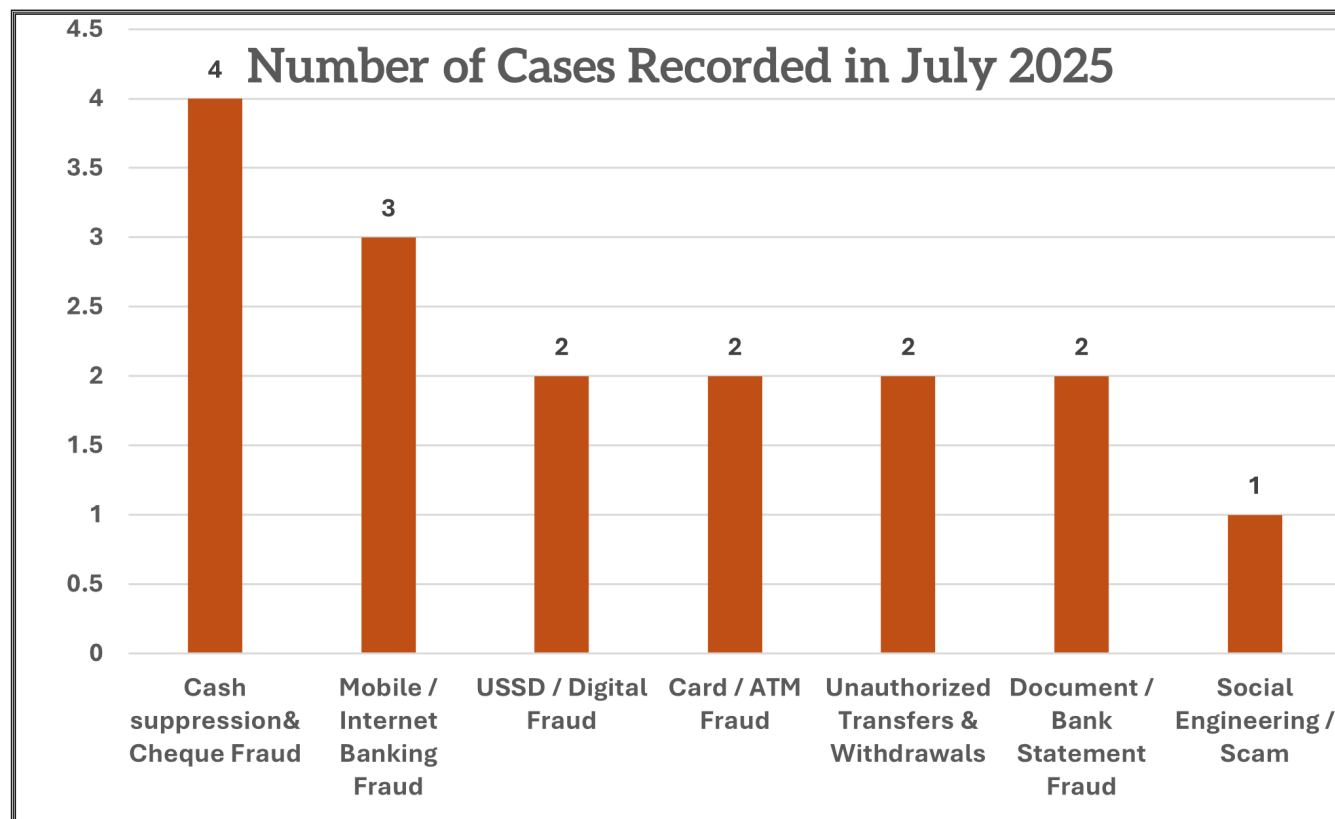




# THE NARRATIVE IN JULY 2025

Fraud activity in July continued to mirror the dual challenge facing the banking industry: sophisticated external attacks on digital channels and persistent insider collusion that erodes trust within institutions. Social engineering remained a strong theme, as customers once again received convincing calls from impostors posing as bank representatives.

By claiming that irregular activity had been detected, the fraudsters persuaded victims to share sensitive login credentials or one-time passwords, which were then used to initiate mobile transfers. These attacks relied on urgency and authority, demonstrating how psychological manipulation remains one of the most effective fraud tools.



Device-related fraud was also present. Stolen phones were quickly turned into gateways for unauthorized transactions, with fraudsters taking advantage of saved credentials and auto-login features to access accounts. In other cases, reissued phone numbers gave fraudsters the ability to reset mobile banking credentials and take control of accounts. These incidents exposed the continuing vulnerability in the relationship between banks and telecom operators, where the reassignment of SIM cards is not always flagged promptly. They also reminded institutions that digital fraud is not only about advanced hacking but often about exploiting basic gaps in everyday processes.

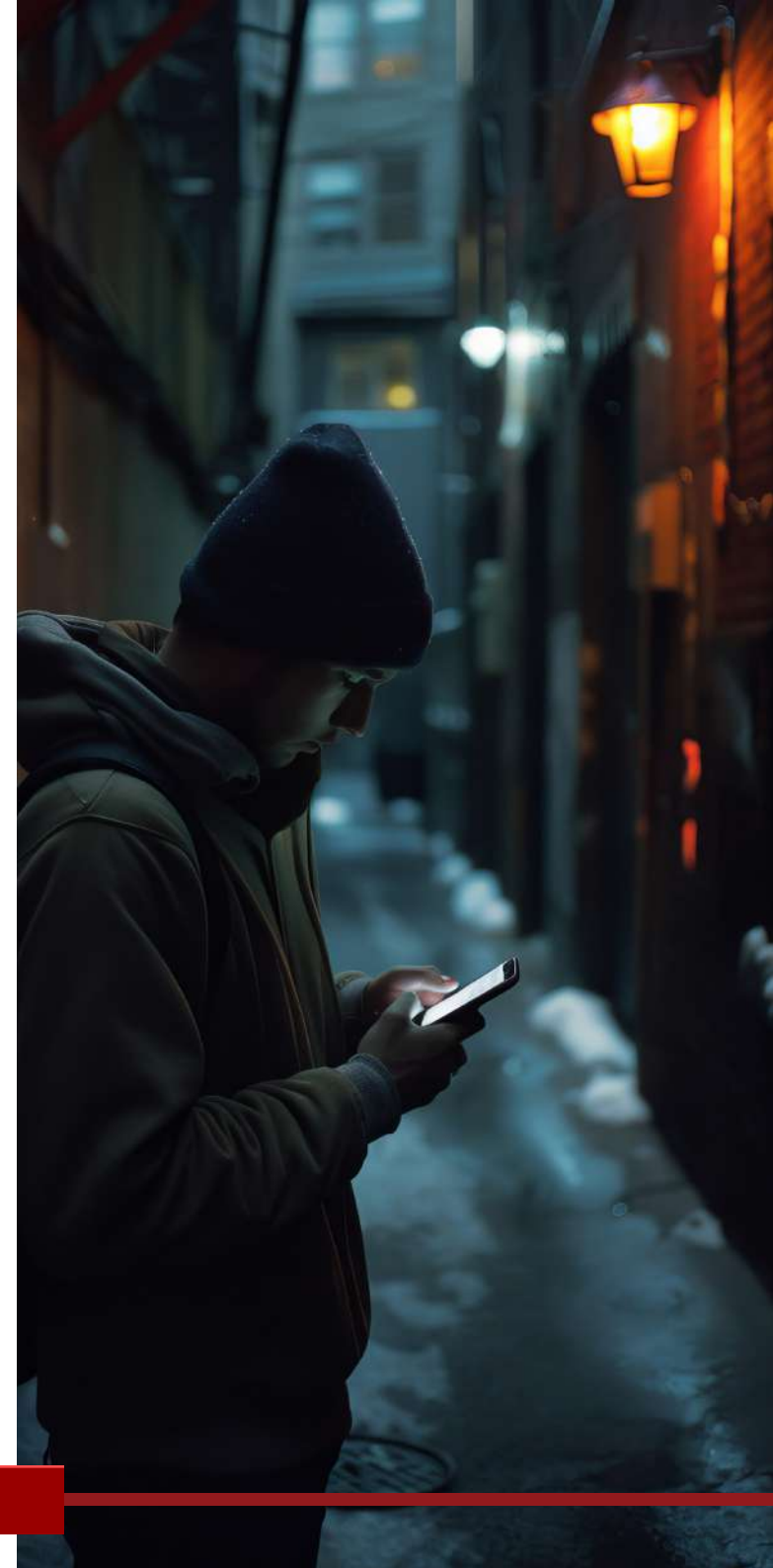
Alongside external schemes, insider fraud played a prominent role in July. Multiple cases of cash suppression were reported, where tellers or staff members deliberately withheld part of customer deposits. Some acted alone, while others colluded with external parties to divert funds. In one notable case, recovery was possible when the shortfall was traced during reconciliation, but the repeated nature of such cases throughout the month revealed a systemic weakness. These incidents showed that while banks have invested heavily in digital controls, lapses in basic cash-handling oversight still create significant exposure. Surprise audits, dual control at cash points, and continuous CCTV reviews emerged as essential countermeasures.

Card fraud also surfaced during the month, with cloning and unauthorized foreign transactions detected on international cards. Customers discovered charges they had not authorized,

and investigations traced the activity back to compromised card details. While some funds were recovered through chargebacks, these cases highlighted the ongoing global nature of card fraud and the need for stronger controls such as 3-D Secure and more effective monitoring of unusual foreign transactions.

Among the cases in July were incidents where falsified bank statements were submitted, particularly for visa applications. Fraudsters either altered genuine statements or produced entirely fabricated documents to support their applications. In one such case, the attempt was detected during the verification process, preventing its use. While no funds were lost, the matter highlighted another dimension of fraud: reputational exposure. When fraudulent documents bearing a bank's name are circulated, even outside direct financial transactions, they undermine trust in the institution and create regulatory concerns. This reinforced the need for banks to maintain strong document security features and controls together with verification mechanisms for any documents issued in their name and to collaborate with external agencies, such as embassies, to authenticate customer financial records.

Not every attempted fraud succeeded in July. A handful of cases were detected and blocked by fraud monitoring systems before any funds were lost. Suspicious mobile banking transactions were intercepted after system rules flagged them, and falsified documents submitted for non-cash purposes were spotted during verification.



## Summary of the fraud cases as reported in July 2025

These prevented incidents demonstrated that well-calibrated detection systems and diligent verification procedures can play a crucial role in reducing losses.

Taken together, the July incidents reflected a familiar but worrying pattern. External fraudsters continue to exploit customer trust, telecom channels, and digital vulnerabilities, while insider threats contribute heavily through cash suppression and collusion. The recurrence of both categories in the same month emphasized that the fraud threat is not one-dimensional. Institutions must therefore invest in layered defenses: strengthening collaboration with telecom operators to address SIM reissue and mobile wallet fraud, educating customers to resist social engineering, and tightening internal oversight to make it harder for staff to manipulate cash or systems. In the end, July reinforced that the fight against fraud must be fought simultaneously on both external and internal fronts.

Typology	Number of Cases	Amount Involved (GHS)	Amount Recovered (GHS)	Net Loss (GHS)
Mobile / Internet Banking Fraud	3	56,330	0	56,330
Social Engineering / Scam	1	120,000	0	120,000
USSD / Digital Fraud	2	360,577	0	360,577
Cash Suppression & Cheque Fraud	4	206,884.50	165,639.50	41,245
Card / ATM Fraud	2	587,975.79	150,204.39	4,571.4
Unauthorized Transfers & Withdrawals	2	57,500	0	57,500
Document / Bank Statement Fraud	2	n/a	n/a	n/a
<b>Total</b>	<b>16</b>	<b>966,310.78</b>	<b>315,685.89</b>	<b>650,624.89</b>





# TYPOLGY-WISE INSIGHTS IN JULY 2025

In July 2025, the Ghana Association of Banks (GAB) collated fraud returns from its member banks, revealing 16 cases across multiple typologies, including digital/mobile banking, cash and cheque handling, card/ATM fraud, and social engineering. The reported incidents highlight the continued sector-wide exposure to both operational and technological vulnerabilities.

Mobile and Internet Banking Fraud remained prominent, with three cases totaling GHS 56,330 (Internet banking, mobile banking, and Momo fraud), all successful and unrecovered. These incidents underscore the ongoing risks associated with electronic banking channels and the critical need for enhanced cybersecurity, multi-factor authentication, and customer awareness campaigns.

Closely related, Social Engineering/Scam accounted for a high-value case of GHS 120,000, which was successful with no recovery. The persistence of such scams reflects the sector-wide susceptibility to human-targeted attacks, reinforcing the need for regular staff training and customer education.

Incidences of fraud via the USSD and digital platforms were also significant, with two successful cases totaling GHS 360,577 and no recoveries. The targeting of digital platforms demonstrates that fraudsters are increasingly exploiting electronic channels, requiring proactive monitoring,

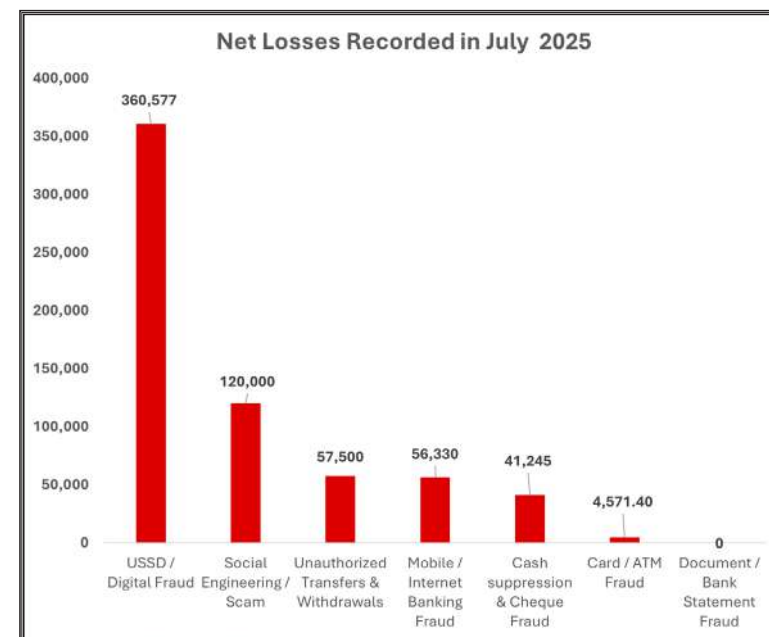
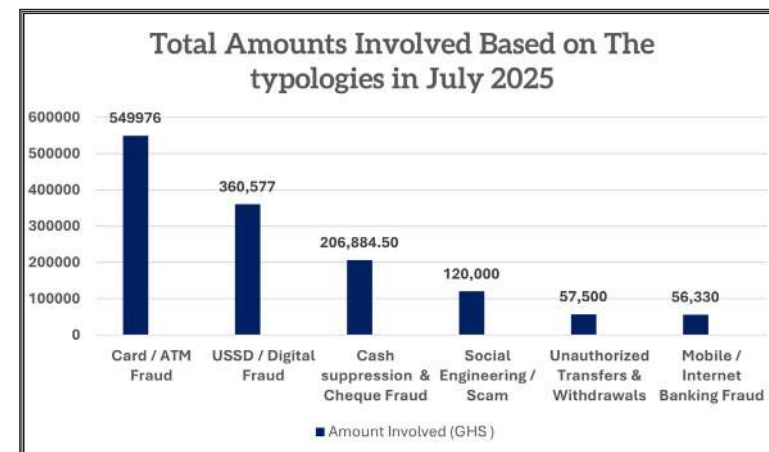
transaction alerts, and fraud detection mechanisms across member banks.

Cash suppression and Cheque-Related Fraud was reported in four cases, including cash suppression (GHS 24,245 and GHS 105,639.50) and cash theft (GHS 60,000), with partial recovery in some cases. These incidents highlight vulnerabilities in operational procedures, cash handling, and internal controls. Regular audits and strengthened oversight remain essential to mitigate such risks.

Online card and ATM Fraud included one card fraud case (GHS 116,775.79 with GHS 112,204.39 recovered) and one ATM fraud case (GHS 38,000, fully recovered). These cases indicate ongoing exposure in card-based and ATM channels while also demonstrating that recoveries are possible when internal controls and monitoring are effective.

Unauthorized Transfers and Fraudulent Withdrawals contributed additional losses, totaling GHS 57,500, reflecting weaknesses in transaction verification processes and monitoring.

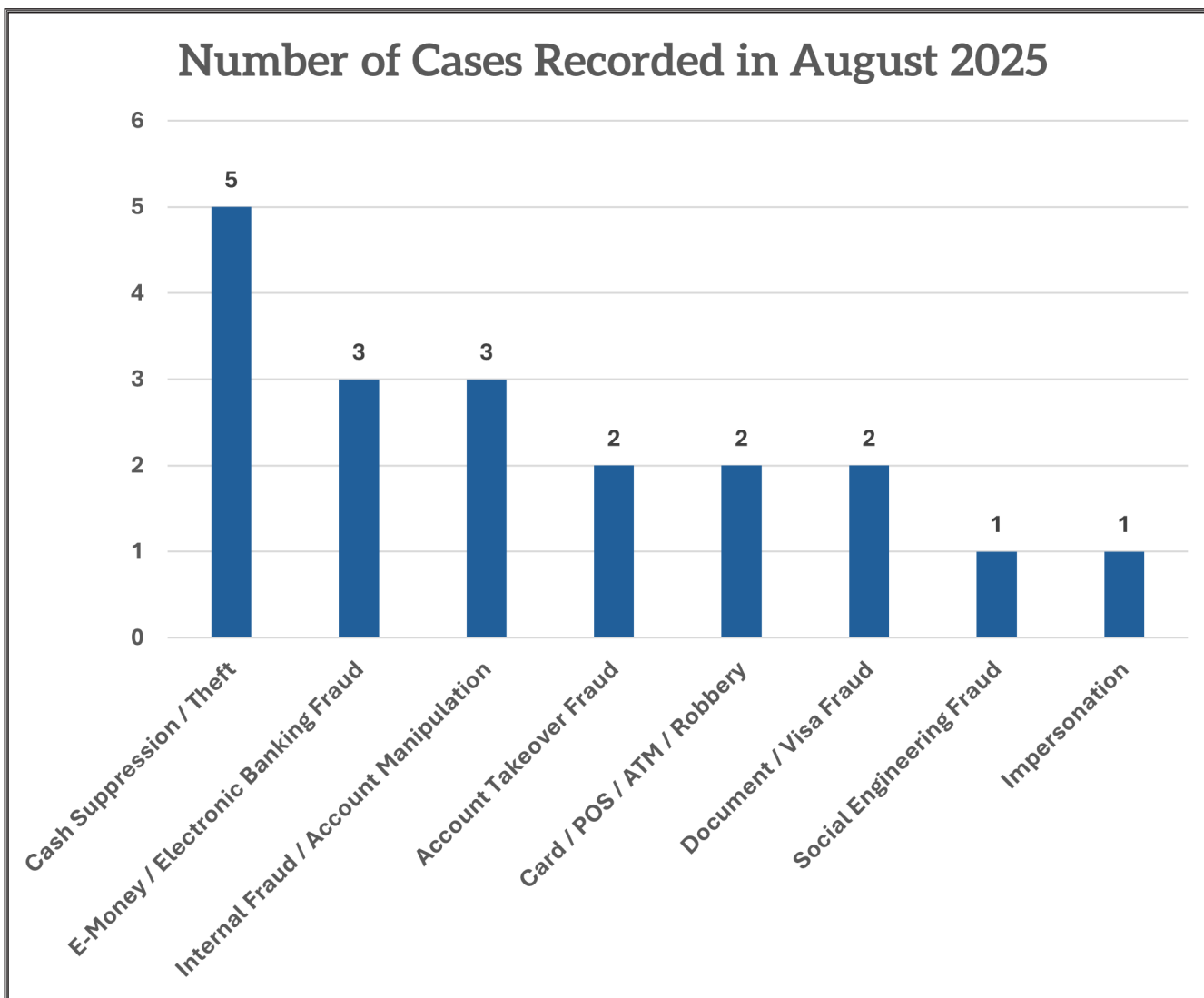
Finally, Bank Statement Falsification and other document-related fraud were reported, though amounts were not disclosed, highlighting the continued relevance of document verification and internal checks



# THE NARRATIVE IN AUGUST 2025

The month of August exposed just how varied and persistent fraud risks have become, with incidents ranging from organized digital takeovers to large-scale internal fraud. Once again, digital channels were a major target. Fraudsters compromised customer devices, often through theft or malicious applications, and used them to access accounts. In some cases, they paired devices to intercept one-time passwords and session tokens, enabling them to authorize multiple transactions without the customer's knowledge. These technical compromises revealed how fraudsters are increasingly moving beyond simple tricks to more sophisticated device-level attacks. The lesson was clear: reliance on SMS-based authentication is no longer sufficient, and stronger, phishing-resistant authentication methods must be adopted.

Social engineering continued to play a role, with impostors contacting customers under the guise of support staff to extract sensitive information. By creating urgency and posing as trusted officials, they convinced victims to release details needed to authorize fraudulent transactions. Vulnerable groups, particularly elderly customers, were targeted with these tactics, underlining the need for tailored awareness campaigns that address the unique risks faced by different customer segments. Fraudsters also attempted impersonation for foreign transfers,



submitting requests that mimicked genuine customers. Fortunately, some of these efforts were intercepted during verification, preventing losses.

Card and account compromise cases also appeared, with fraudsters using phishing and stolen credentials to gain unauthorized access. Once inside, they executed transfers through USSD and wallet channels, capitalizing on the relatively weaker controls in those systems. Email compromise once again featured, as attackers redirected banking notifications into junk folders and quietly approved new device registrations. These cases reinforced the growing importance of protecting not only the bank’s systems but also the wider digital ecosystem that customers rely on, including their emails and mobile devices.

Yet the most damaging incidents in August came from within. Internal fraud, particularly cash suppression, reached alarming levels. The largest case involved a staff member responsible for collecting deposits who failed to deliver them, leading to the suppression of very large sums over time. Other cases of teller miscounts and collusion with external actors were also reported, showing that weaknesses in basic cash-handling processes remain a recurring vulnerability. While some recoveries were made, these incidents demonstrated that insider threats, when left unchecked, can dwarf external fraud losses. Similarly, there were attempts at ledger manipulation and ATM key misuse by staff, though some of these were detected and prevented before any actual loss occurred.

A similar pattern appeared in August, where forged bank statements were once again presented for visa applications. Fraudsters attempted to pass off these documents as genuine to secure travel permits. Fortunately, verification checks exposed the deception before any harm was done. These cases demonstrated that not all fraud is purely financial; some schemes aim to misuse the credibility of banking institutions to achieve non-financial gains. However, the risks are still significant because repeated circulation of forged documents can damage the industry’s credibility. This underscored the importance of secure statement issuance, the use of tamper-proof features, and greater collaboration with consulates and other authorities that rely on bank documents.

Overall, the August cases painted a picture of fraud that is growing more complex and multi-layered. On one hand, external actors are adopting advanced techniques that exploit digital ecosystems, including mobile devices, emails, and USSD platforms. On the other hand, internal weaknesses, particularly around cash custody and privileged access, are generating some of the largest single exposures. The convergence of these risks demands a twofold response: investment in advanced digital controls to outpace external fraudsters, and a renewed commitment to internal discipline, surveillance, and accountability. August therefore served as a strong reminder that while technology evolves, the most enduring risk remains human behavior—whether it is the customer persuaded by a convincing call, or the staff member who chooses to betray the trust of their institution.

Summary of the fraud cases reported in August 2025

Typology	Number of Cases	Amount Involved (GHS)	Amount Recovered (GHS)	Net Loss (GHS)
Cash Suppression / Theft	5	1,488,600	93,000	1,395,600
E-Money / Electronic Banking Fraud	3	439,717.95	0	439,717.95
Social Engineering Fraud	1	39,900	10,000	29,900
Account Takeover Fraud	2	18,130	0	18,130
Internal Fraud / Account Manipulation	3	413,283.18	377,796	35,487.18
Card / POS / ATM / Robbery	2	17,365.83	0	17,365.83
Document / Visa Fraud	2	n/a	n/a	n/a
Impersonation	1	26,672.00	26,672.00	0
Total	17	2,443,669.96	507,468.00	1,936,201.96



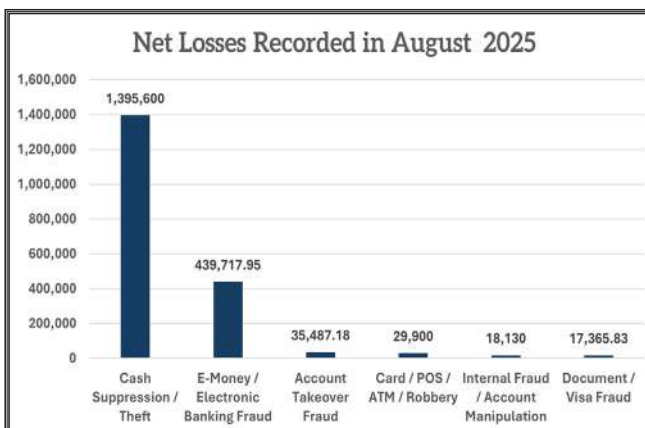
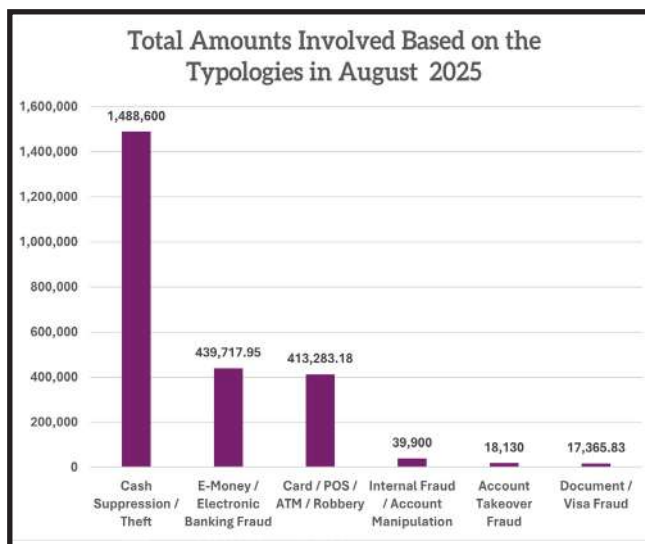
# TYPOLGY-WISE INSIGHTS IN AUGUST 2025

In August 2025, the Ghana Association of Banks (GAB) received fraud reports from its member banks highlighting 17 cases spanning multiple typologies. The incidents reflect both operational and digital vulnerabilities, as well as internal collusion, emphasizing the sector-wide nature of financial crime.

Cash Suppression and Theft dominated the month, with five cases totaling GHS 1,488,600. Partial recovery was achieved in two cases (GHS 93,000), resulting in substantial net losses. These incidents underscore ongoing weaknesses in cash handling, internal controls, and operational monitoring across banks.

Electronic and E-Money Fraud continued to be significant, with three successful cases totaling GHS 439,717.95, none of which were recovered. Fraudsters exploited mobile and electronic banking platforms, highlighting the critical need for enhanced cybersecurity measures, real-time monitoring, and customer awareness initiatives.

Social Engineering Fraud was reported in one case totaling GHS 39,900, with partial recovery of GHS 10,000. This reflects the persistent sector-wide risk posed by human-targeted scams and emphasizes the importance of continuous staff and customer education.



Account Takeover Fraud was reported in two cases totaling GHS 18,130, with no recovery. These incidents demonstrate vulnerabilities in account authentication and monitoring systems across multiple banks.

Internal Fraud and Manipulation of Accounts contributed significantly, with three cases totaling GHS 413,283.18, of which GHS 377,796 was recovered, highlighting that while internal controls can enable partial recovery, insider threats remain a significant challenge.

Card / Plastic Fraud and ATM Related Fraud accounted for smaller, yet notable, losses totaling GHS 17,365.83, indicating ongoing exposure to electronic and physical payment fraud.

Document and Visa-Related Fraud were reported in two cases, though amounts were not disclosed. These cases reinforce the need for rigorous verification processes for high-value transactions, including visa and document-related approvals.

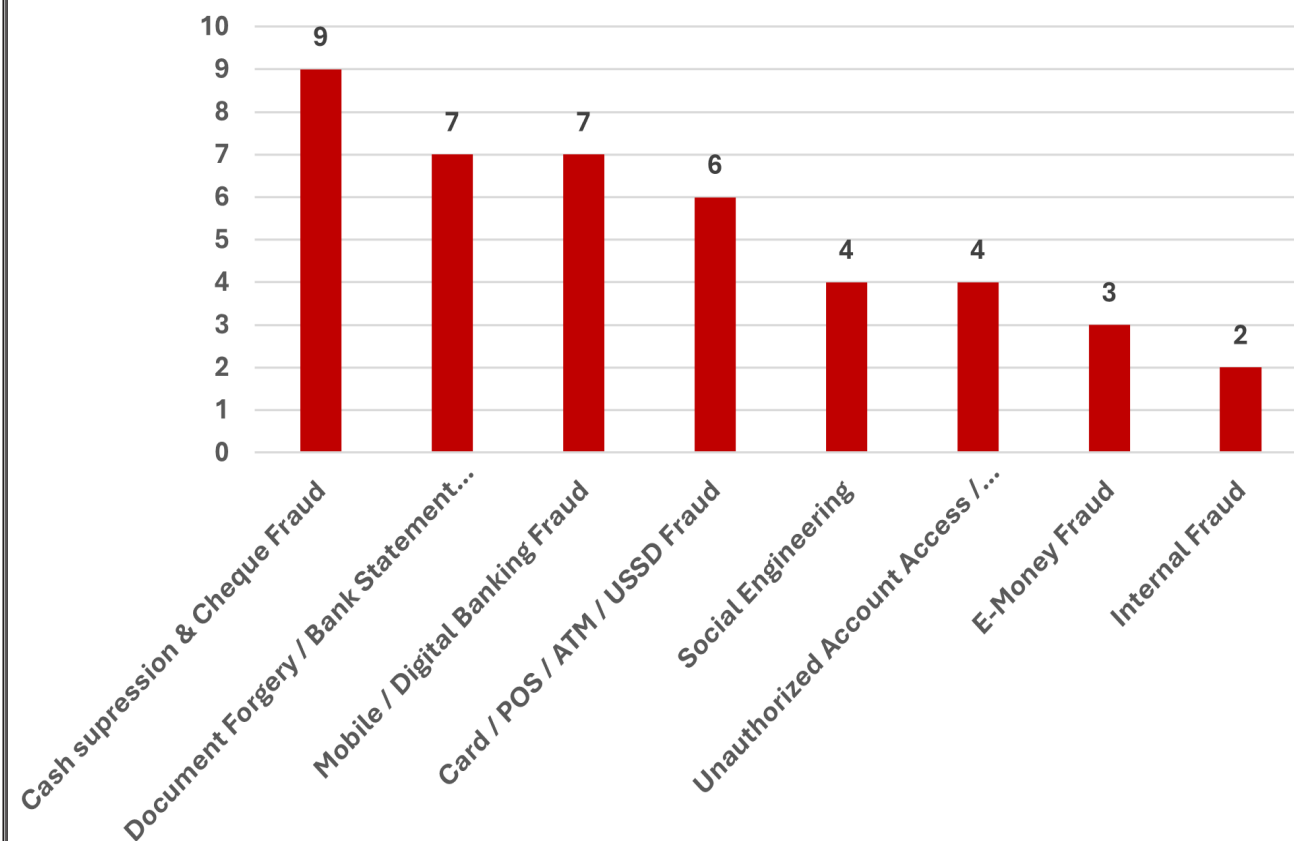
Finally, Impersonation (GHS 26,240) was attempted but unsuccessful, reflecting the continued vigilance of member banks in detecting and preventing fraud attempts.

# SUMMARY OF THE NARATIVES JUNE -AUGUST 2025

Between June and August, we have observed based on the reported forty-four (44) cases that the fraud landscape in banking sector demonstrated a persistent and evolving threat environment, characterized by a combination of external attacks targeting digital channels and internal collusion exploiting procedural weaknesses. Across the three months, a recurring theme was the sophisticated use of social engineering, device compromise, and insider manipulation to execute financial crimes.

External fraud relied heavily on exploiting customer trust and the integration of banks with digital and telecom systems. Impostors posing as bank officials employed carefully scripted calls to create urgency, prompting customers to share sensitive information such as one-time passwords or login credentials. These details were then used to authorize transfers to mobile wallets, which were quickly layered across multiple accounts and withdrawn at agent points. Device theft and SIM reassignments further amplified this risk, as fraudsters gained immediate access to accounts through saved credentials or by resetting banking information using reissued phone numbers. Email compromise also emerged as a common tool, allowing attackers to intercept notifications and authorize undetected transactions. Across June, July, and August, these methods revealed that the weakest link often remained the human element, with customers inadvertently facilitating their own exploitation.

## Number of Cases Reported Across The Typologies From June To August 2025



Card and account-based fraud remained prevalent, with incidents of card-not-present transactions, cloning, phishing, and unauthorized international transfers. Fraudsters frequently executed small, repeated debits to evade detection, while phishing and stolen credentials allowed access to USSD and wallet platforms, particularly in August. In several cases, chargebacks and refunds mitigated losses, but the persistence of these activities highlighted the ongoing global risk and the need for stronger authentication protocols, such as 3-D Secure, and enhanced monitoring of unusual transactions.

A notable pattern across all three months involved the submission of falsified bank statements, particularly for visa applications. Fraudsters either altered genuine statements or produced fully fabricated documents, aiming to misuse the credibility of banks for non-financial gains. While most attempts were intercepted during verification, these incidents underscored the reputational and regulatory risks associated with fraudulent documentation.

Internal fraud contributed significantly to the overall threat environment. Cash suppression, deliberate teller miscounts were consistently observed. Some staff exploited positions of trust to withhold deposits or manipulate ledger entries, while large-scale incidents in August illustrated that insider breaches could surpass external losses. Recoveries were occasionally possible during reconciliations, yet the recurring nature of these cases emphasized

systemic weaknesses in cash-handling oversight. Countermeasures such as dual verification, surprise audits, continuous CCTV monitoring, and stricter access controls emerged as critical strategies to curb insider abuse.

The modus operandi across these months highlighted speed, deception, and exploitation of both technology and human behavior. External fraudsters prioritized rapid movement of funds before detection, leveraging social engineering, device compromises, and digital vulnerabilities. Insider fraud relied on deliberate procedural lapses, trust violations, and sometimes collusion with external parties. Meanwhile, document-related fraud targeted institutional credibility rather than direct financial gain.

Overall, the period from June to August painted a picture of a multi-layered fraud environment. Effective mitigation requires a dual approach: strengthening digital defenses, including collaboration with telecom operators, advanced authentication, and monitoring of mobile and online platforms; and enhancing internal oversight, with rigorous cash-handling controls, staff accountability, and continuous verification processes. These months reinforced that while technology can both enable and prevent fraud, human behavior, whether as a victim, insider, or perpetrator, remains the central factor shaping the risk landscape.





# DIVING INTO THE NUMBER: FRAUD ANALYSIS

## Summary of the fraud cases as reported from June to August 2025

Between June and August 2025, fraud reporting from member banks of the Ghana Association of Banks (GAB) reveals a diverse and evolving landscape of financial crime. A total of 44 cases were recorded across nine major typologies, reflecting the persistent vulnerabilities faced across the banking sector, including human factors, internal collusion, and weaknesses in digital and traditional banking channels. The data underscores the adaptive nature of fraudsters, who exploit both operational and systemic gaps across multiple institutions.

During this three-month period, the total amount involved in fraud cases reached GHS 4.7 million. These figures highlight the growing sophistication and diversification of fraudulent activities across both local and foreign currency transactions. Recoveries amounted to GHS 0.9, demonstrating that banks have been able to mitigate some of the financial impact through improved monitoring and responsive fraud management systems. However, the low and insignificant recoveries were not enough to offset the overall exposure.

Consequently, the sector still recorded a net loss of GHS 3.8 million, underscoring the urgency of adopting stronger preventive and corrective measures.

Typology	Number of Cases	Total Amount Involved	Amount Recovered	Net Loss
Social Engineering	4	GHS 371,900	GHS 10,000	GHS 361,900
Unauthorized Account Access / Transfers	4	GHS 73,900	GHS 0	GHS 73,900
Cash Suppression and Cheque Fraud	9	GHS 2,191,828.50	GHS 177,639.50	GHS 2,014,189
Document Forgery / Bank Statement	7	GHS 287,868.00	GHS 279,868.00	GHS 8,000
Mobile / Digital Banking Fraud	7	GHS 768,787.95	GHS 0	GHS 768,787.95
Card / POS / ATM / USSD Fraud	6	GHS 298,857.76	GHS 150,250.53	GHS 148,607.23
E-Money Fraud	3	GHS 370,572	GHS 0	GHS 370,572
Internal Fraud	2	GHS 306,687.18	GHS 271,200	GHS 35,487.18
Account Takeover Fraud	2	GHS 18,130	GHS 18,130	
Total	44	GHS 4,687,530.39	GHS 888,958.03	GHS 3,798,572.36

# THE PREVAILING FRAUD TYPOLOGIES

## Social Engineering Fraud

Social engineering continued to dominate the fraud profile, with scams, digital manipulation, and impersonation recorded across 4 cases. Member banks reported total amounts involved of GHS 371,900, with recoveries of only GHS 10,000, leaving net losses of GHS 361,900. These incidents demonstrate the sector-wide challenge of human-targeted fraud, where both staff and customers are manipulated into authorizing payments. Continuous staff training, enhanced verification procedures, and customer awareness campaigns remain critical defenses against this typology.

## Unauthorized Account Access and Transfers

Unauthorized account access and fraudulent transfers were reported in 4 successful cases, involving GHS 73,900 with no recovery. These cases highlight the sector-wide vulnerabilities in account authentication and transaction monitoring across multiple banks. Strengthening multi-factor authentication, deploying real-time alerts, and implementing anomaly detection systems are essential measures to mitigate these risks.

## Cash Suppression and Cheque Fraud

Cash and cheque fraud accounted for the largest monetary impact, with 9 cases totaling GHS 2,191,828.50, of which GHS 177,639.50 was recovered, leaving net losses of GHS 2,014,189.

Reported incidents included cash suppression, cash theft, and cheque fraud, illustrating weaknesses in cash-handling procedures, cheque processing, and internal controls. The high losses emphasize the need for rigorous reconciliation, segregation of duties, and surprise audits across member banks.

## Document Forgery and Bank/Visa Statement Falsification

This typology included 7 cases, covering bank and visa statement falsification, document forgery, and attempted impersonation GHS 26,672.00. The total amounts involved were GHS 287,868.00 with recoveries of GHS 279,868.00, resulting in net losses of GHS 8,000. These data suggest that verification protocols in some banks were effective in mitigating losses, although persistent attempts at forgery indicate the need for continual vigilance, particularly for high-value or visa-related transactions.

## Mobile and Digital Banking Fraud

Digital channels, including mobile money, internet banking, and electronic banking, were heavily targeted. Seven successful cases totaling GHS 768,787.95 were reported with no recoveries. This reflects a sector-wide trend where digital banking platforms are increasingly attractive to fraudsters, necessitating enhanced cybersecurity, transaction monitoring, multi-factor authentication, and customer education.

## Card, POS, ATM, and USSD Fraud

Six cases were reported across member banks, including card cloning, POS manipulation, ATM withdrawals, USSD fraud, and robbery-assisted withdrawals. The total amounts involved were GHS 298,857.76, with partial recoveries of GHS 150,250.53, leaving a net loss of GHS 148,607.23. These incidents demonstrate ongoing sector-wide vulnerabilities in electronic payment systems and highlight the need for robust real-time monitoring and alert mechanisms.

## E-Money Fraud

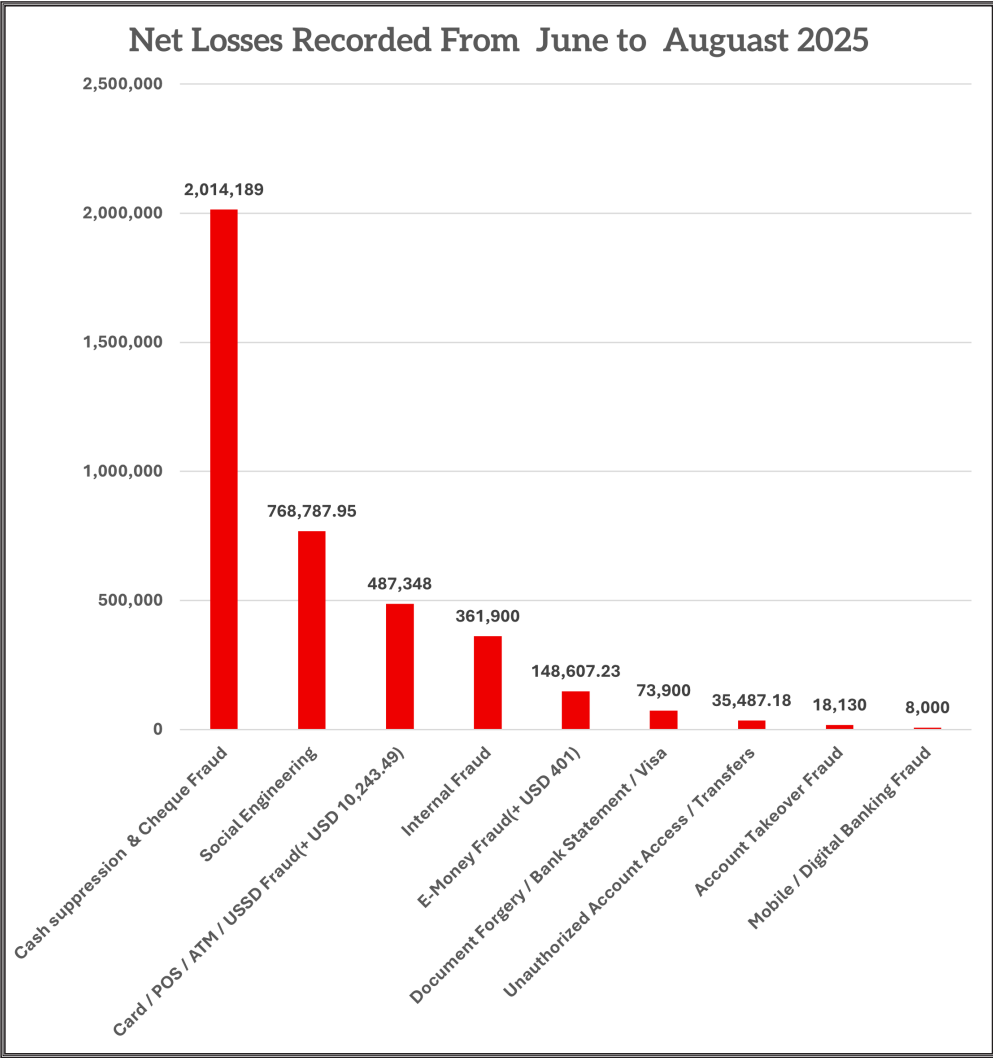
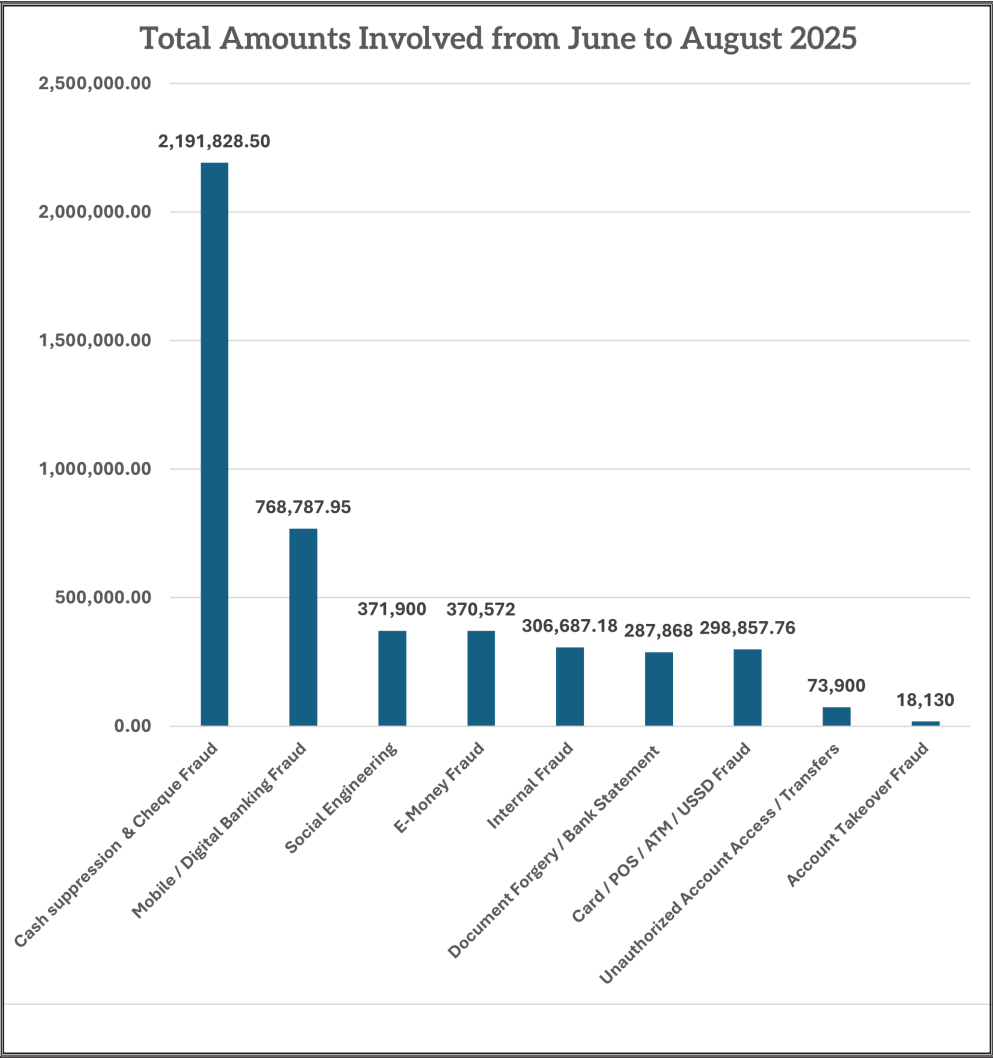
Three cases of e-money fraud were reported, totaling GHS 370,572 with no recovery. Fraudsters continued to exploit vulnerabilities in electronic wallet platforms across multiple banks, reinforcing the importance of real-time transaction monitoring and preventive measures for high-risk transactions.

## Internal Fraud

Internal fraud, involving collusion and manipulation of accounts, accounted for 2 cases, totaling GHS 306,687.18, with recoveries of GHS 271,200, leaving net losses of GHS 35,487.18. The data highlight that, although internal controls and monitoring enabled partial recovery, insider threats remain a significant risk across the sector.

# Account Takeover Fraud

Account takeover incidents were reported in 2 successful cases, totaling GHS 18,130 with no recovery. These cases demonstrate that account compromise remains a persistent threat across member banks, emphasizing the importance of robust authentication and proactive monitoring systems.





# IMPLICATIONS FOR THE BANKING INDUSTRY

## 1. Operational Risks

The report demonstrates that fraud incidents continue to expose critical weaknesses in banks' operational systems. Cash suppression, teller malpractices, and insider collusion emerged as persistent issues, particularly in August, when internal fraud accounted for significant losses. These lapses highlight the vulnerability of manual cash-handling processes, weak segregation of duties, and insufficient reconciliation mechanisms.

Digital channels also revealed operational blind spots. Fraudsters exploited SIM reissuance, stolen devices, and USSD channels to gain unauthorized account access and intercept OTPs. The reliance on SMS-based authentication created a systemic risk across the industry; as once compromised, customers' entire financial identity could be exploited within minutes. The speed of fund movement — often through mobile wallets and agent points — further exposed the limitations of banks' transaction monitoring systems, where real-time detection and blocking remain underdeveloped.

Collectively, these operational risks point to an urgent need for tighter internal controls, robust real-time surveillance, and cross-channel fraud detection capabilities.

## 2. Financial and Reputational Costs

The industry suffered a net loss of GHS 3.8 million in just three months, with cash and cheque fraud contributing GHS 2.01 million alone. Digital fraud and e-money losses added over GHS 1.1 million in exposure, most of which was unrecovered. The uneven recovery profile is a major concern: document and visa forgeries were often detected early and fully blocked, while social engineering and mobile fraud resulted in near-total losses.

Financial losses, however, are only one dimension of the cost. The reputational damage associated with repeated forgery of bank statements and fraudulent visa applications threatens to undermine international confidence in Ghanaian banks. Embassies and external institutions that receive falsified documents may begin to question the reliability of financial attestations, imposing indirect costs in the form of stricter verification requirements or reputational penalties.

The cost of inaction is compounded by customer dissatisfaction. Clients who lose funds to social engineering or account takeovers — often without timely recovery — are likely to lose confidence in their banks' ability to protect them, increasing the risk of attrition.

## 3. Sector-wide Trust and Confidence Issues

Trust is the foundation of the financial system, and fraud incidents erode this foundation. The report highlights how fraudsters rely heavily on manipulating trust — impersonating bank officials, creating urgency, and exploiting customers' unfamiliarity with fraud red flags. As these cases gain visibility, they create a perception that banks are unsafe custodians of funds.

The rising fraud in mobile and e-money platforms also raises systemic concerns. These channels are central to Ghana's financial inclusion agenda, but their vulnerability risks deterring customers from adopting digital solutions, slowing the momentum of cashless transformation. Furthermore, the persistence of insider fraud undermines not only institutional credibility but also collective sector-wide integrity.

If unaddressed, these issues could erode the gains made in digitization, widen the trust gap between banks and customers, and create reputational spillovers for the entire financial ecosystem.

# STRATEGIC RECOMMENDATIONS

## A. Institutional-Level Measures (Banks)

- Enhance transaction monitoring: Implement real-time surveillance systems with velocity checks, anomaly detection, and hybrid AI/rule-based models to spot irregular patterns across mobile, card, and USSD channels.
- Tighten cash-handling protocols: Enforce dual verification, teller rotation, and surprise cash audits to reduce opportunities for suppression and collusion.
- Insider risk management: Conduct periodic background checks, mandatory leave policies, and privileged-access monitoring. Establish safe whistleblower channels to detect collusion early.
- Secure document issuance: Introduce digitally verifiable statements (with QR codes or blockchain-backed signatures) to prevent fraudulent reproduction.

## B. Industry-Level Measures

- Telco collaboration: Develop Memoranda of Understanding (MOUs) with telecom operators to enable real-time SIM-swap alerts, mobile account freezes, and coordinated investigations.
- Joint fraud monitoring platforms: Build shared detection infrastructure across banks, PSPs, and telcos for monitoring suspicious e-money flows

and high-velocity transfers.

- Capacity building: Organize sector-wide training programs for fraud risk officers and IT teams to stay ahead of emerging attack techniques. The Ghana Association of Banks in collaboration with relevant stakeholder like the Chartered Institute of Bankers Ghana, Association of Certified Fraud Examiners in Ghana can help develop strategic capacity building seminars in that regards.

## C. Regulatory and Policy Interventions

- Standardized reporting protocols: Establish compulsory timelines and formats for fraud reporting to a central registry, enabling faster sector-wide response.
- Faster adjudication mechanisms: Work with the judiciary to fast-track fraud-related cases, reducing the prolonged litigation periods that currently discourage banks from pursuing recoveries.
- Cross-sector taskforce: Create a permanent anti-fraud taskforce involving BoG, GAB, telcos, EOCO, and the Cybersecurity Authority to strengthen intelligence sharing and enforcement

## D. Customer Awareness and Education

- Fraud awareness campaigns: Launch targeted multimedia campaigns (radio, TV, SMS, social media) to sensitize customers about common fraud schemes, especially social engineering.
- Vulnerable groups: Prioritize education for the elderly, rural populations, and first-time digital users, who are disproportionately targeted.
- Customer engagement: Push real-time alerts and reminders during high-risk transactions, reinforcing the “no-OTP-sharing” message.
- Feedback loops: Collect customer reports on fraud attempts to enrich monitoring systems and adapt educational content.

# CONCLUSION

Between June and August 2025, Ghana's banking sector recorded 44 fraud cases across nine typologies, with total losses exceeding GHS 3,704,919.27, despite recoveries of over GHS870,743.41. These figures highlight the persistence and complexity of fraud, as well as the urgent need for proactive, coordinated responses across the ecosystem. Three critical insights emerge from this quarter's data:

1. Digital vulnerabilities are escalating – fraudsters continue to exploit mobile, e-money, and online platforms, where recovery rates remain alarmingly close to zero.
2. Cash and cheque-related fraud remain highly costly, exposing operational gaps in physical transaction management.
3. Human factors such as social engineering and insider collusion are central drivers of losses, proving that fraud is not just a technological

issue, but also a behavioral, cultural, and governance challenge.

Addressing these threats requires a multi-stakeholder response. Banks must strengthen internal controls, invest in real-time monitoring, and enhance staff training. Telcos must reinforce SIM registration and e-money security frameworks. Customers must adopt safer digital practices and remain vigilant against manipulation. Regulators must enforce stricter compliance, foster sector-wide collaboration, and ensure timely intelligence sharing.

The Ghana Association of Banks (GAB) remains committed to supporting this coordinated effort. By presenting quarterly insights alongside the Bank of Ghana's annual fraud reports, we aim to provide near real-time intelligence that strengthens institutional defenses and customer protection. Together-banks, telcos, regulators, and customers we can reduce fraud exposure, preserve trust, and safeguard the integrity of Ghana's financial system.








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