GHANA ASSOCIATION OF BANKS

# INDUSTRY FRAUD REPORT

## SEPTEMBER - DECEMBER 2025

FOLLOW US

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

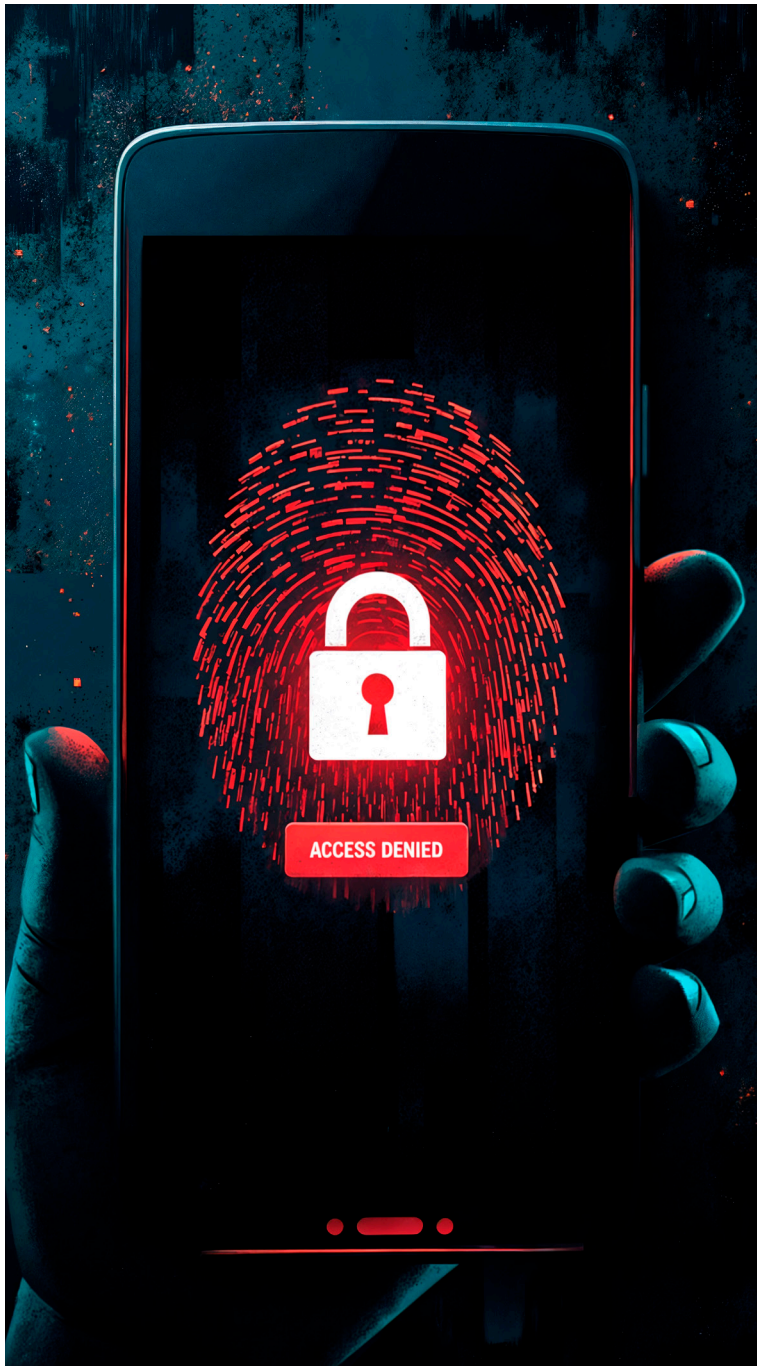
# EXECUTIVE SUMMARY

The Ghana Association of Banks (GAB) Fraud Report for the period September to December 2025 captures a sustained escalation in fraud activity and financial exposure across Ghana's banking sector, reflecting both the rapid digitisation of financial services and persistent weaknesses in behavioural, operational, and control environments. Over the four-month period, member banks recorded a total of 105 fraud incidents across multiple typologies, involving an attempted amount of approximately GHS 7.12 million. Of this amount, about GHS 2.52 million was recovered, resulting in a net industry loss of approximately GHS 4.60 million. These outcomes underscore a widening gap between fraud execution and recovery effectiveness, particularly within fast-settling digital channels.

Fraud incidents during the period were overwhelmingly concentrated in digitally mediated channels. Electronic Transfer–related fraud emerged as the most dominant typology, accounting for 53 cases or 50.5% of total incidents, highlighting the centrality of mobile banking, USSD, and bank-to-wallet channels in overall fraud volumes. Card and POS fraud followed with 18 cases (17.1%), while cash suppression accounted for 9 cases (8.6 percent), confirming that internal control and process-driven risks remain material. Cyber and email-related fraud, mobile money fraud, account takeover, identity theft and impersonation, and unauthorised transfers occurred less frequently, each contributing between 2 and 4 percent of total cases, but often with disproportionate financial impact.

In value terms, fraud exposure was highly concentrated in a small number of typologies. Electronic Transfer fraud accounted for the largest share of attempted amounts, with approximately GHS 4.31 million, representing 60.6% of total value at risk. This was followed by cash suppression, involving about GHS 1.04 million (14.7%), and unauthorised transfers amounting to GHS 668,191 (9.4%). Cyber and email-related fraud contributed GHS 401,884 (5.7%), while identity theft and impersonation resulted in GHS 239,451 (3.4%) loss. All other typologies individually accounted for less than 2 percent of total amounts involved, illustrating the asymmetric nature of fraud risk across channels.

Net losses during the period were similarly concentrated. Electronic Transfer fraud accounted for approximately GHS 2.29 million in net losses, representing 49.9% of total industry losses, reflecting low recovery rates once funds were transferred into mobile money wallets and third-party accounts. Cash suppression followed with net losses of about GHS 820,650 (17.9%, despite relatively higher recovery rates, underscoring persistent weaknesses in cash handling, reconciliation, and supervision. Unauthorised transfers resulted in net losses of GHS 546,891 (11.9%), while cyber and email-related fraud accounted for GHS 401,884 (8.7%). Losses from identity theft and impersonation, card and POS fraud, mobile money fraud, and account takeover were smaller in absolute terms but remain significant given their recurrence and behavioural drivers.



A defining theme across the September–December period was the central role of modus operandi rooted in human behaviour. A substantial proportion of cases involved customers being socially engineered into disclosing PINs, passwords, one-time passwords, and device approval codes. Common schemes included fake data bundle offers, fraudulent online shopping platforms, impersonation of telecom or bank staff, and deceptive investment or visa application narratives. Device-related vulnerabilities such as stolen phones, ignorantly giving registered SIM cards, delayed reporting, and compromised email accounts further enabled unauthorised access to banking platforms. In parallel, several high-impact cases reflected staff-related lapses, including failure to follow verification procedures, reliance on verbal instructions, and insider misconduct in cash handling and account processing.

Beyond direct financial losses, the fraud patterns observed during the period raise broader reputational, operational, and systemic concerns. Recurrent impersonation, forged documents, and misuse of fictitious bank statements in verification and onboarding processes pose risks to correspondent banking relationships, embassy verification systems, and international confidence in Ghana's banking controls. If left unaddressed, these trends may invite increased external scrutiny and impose indirect compliance and reputational costs on the sector.

In response to these developments, the report underscores the need for a multi-layered strategic response. At the institutional level, banks must strengthen authentication and transaction control frameworks, reduce reliance on SMS-based OTPs, enhance real-time monitoring of high-risk digital transactions, and reinforce operational discipline in cash handling and staff supervision. At the industry level, deeper collaboration among banks, telecom operators, regulators, law enforcement agencies, and the Cybersecurity Authority is essential to improve intelligence sharing, accelerate wallet blocking and fund recovery, and deliver coordinated public education.

In conclusion, the fraud trends observed between September and December 2025 depict a banking environment facing growing pressure from digitally enabled, fast-executing fraud schemes alongside unresolved internal control vulnerabilities. Without decisive and coordinated action, continued digital expansion will further magnify exposure. For boards and executive management, the priorities are clear: comprehensive fraud awareness campaign, strengtheningfraud-resistant controls, embed behavioural risk management into governance frameworks, and deepen industry-wide collaboration to protect public confidence and preserve the stability of Ghana's banking sector.

## Consolidated Fraud Summary (September–December 2025)

| Typology | Number of Cases | Attempted Amount (GHS) | Amount Recovered (GHS) | Net Loss (GHS) |
|---|---|---|---|---|
| E-Transfer | 53 | 4,311,056.88 | 2,016,150.00 | 2,294,906.88 |
| Card / POS | 18 | 110,863.08 | 9,929.91 | 100,933.17 |
| Cash Suppression | 9 | 1,044,810.00 | 224,160.00 | 820,650.00 |
| Cyber / Email | 4 | 401,884.17 | 0.00 | 401,884.17 |
| Mobile Money | 4 | 86,189.00 | 39,482.02 | 46,706.98 |
| Account Takeover | 3 | 48,050.00 | 0.00 | 48,050.00 |
| Forgery & Manipulation of Documents | 3 | 0.00 | 0.00 | 0.00 |
| Identity Theft & Impersonation | 3 | 239,450.70 | 12,000.00 | 227,450.70 |
| Unauthorized Transfer | 3 | 668,191.00 | 121,300.00 | 546,891.00 |
| ATM Fraud | 2 | 79,200.00 | 0.00 | 79,200.00 |
| Cheque Fraud | 2 | 96,000.00 | 96,000.00 | 0.00 |
| Advance Fee Fraud | 1 | 30,000.00 | 0.00 | 30,000.00 |
| **TOTAL** | **105** | **7,115,694.83** | **2,519,021.93** | **4,596,672.90** |

# INTRODUCTION

At the Ghana Association of Banks (GAB), safeguarding the integrity, stability, and resilience of Ghana's banking sector remains a core priority, given that a sound and trustworthy financial system is fundamental to macroeconomic stability, investor confidence, and public trust.

As digital financial services continue to expand rapidly in Ghana, driving convenience, efficiency, and financial inclusion, they have simultaneously increased exposure to fraud risks across banking and payment ecosystems. Both the Bank of Ghana (BoG) and GAB have consistently emphasized that financial crime is no longer static. It is evolving in form, speed, and sophistication, with material implications for operational resilience, customer confidence, and systemic stability.

Over the four-month period from September to December 2025, a total of 105 reported fraud incidents were recorded across multiple typologies, involving an attempted amount of approximately GHS 7.12 million. Recoveries during the period amounted to about GHS 2.52 million, resulting in a net industry loss of approximately GHS 4.60 million. These outcomes point to a sustained elevation in fraud risk compared to earlier periods, driven largely by digital channels, mobile money integration, and weaknesses in both customer and internal control environments.

The data confirms a decisive shift in fraud patterns within Ghana's banking sector. Traditional cheque manipulation and isolated cash theft cases are increasingly being overtaken by electronic transfers, mobile money–linked fraud, card-not-present transactions, impersonation, and cyber-enabled social engineering schemes. These typologies are characterized by rapid execution, cross-platform movement of funds, and limited recovery windows once transactions are completed. As funds move quickly from bank accounts into mobile wallets and third-party platforms, detection becomes more complex and loss mitigation more difficult.

The reporting period also reinforces the central role of human behaviour in fraud outcomes. A significant proportion of cases involved customers voluntarily disclosing credentials, PINs, and one-time passwords under social engineering pressure. Other cases reflected lapses in staff verification procedures, weak adherence to escalation protocols, or insider misconduct. These trends underscore that fraud risk is not solely a technology issue but also a governance, process, and culture challenge.

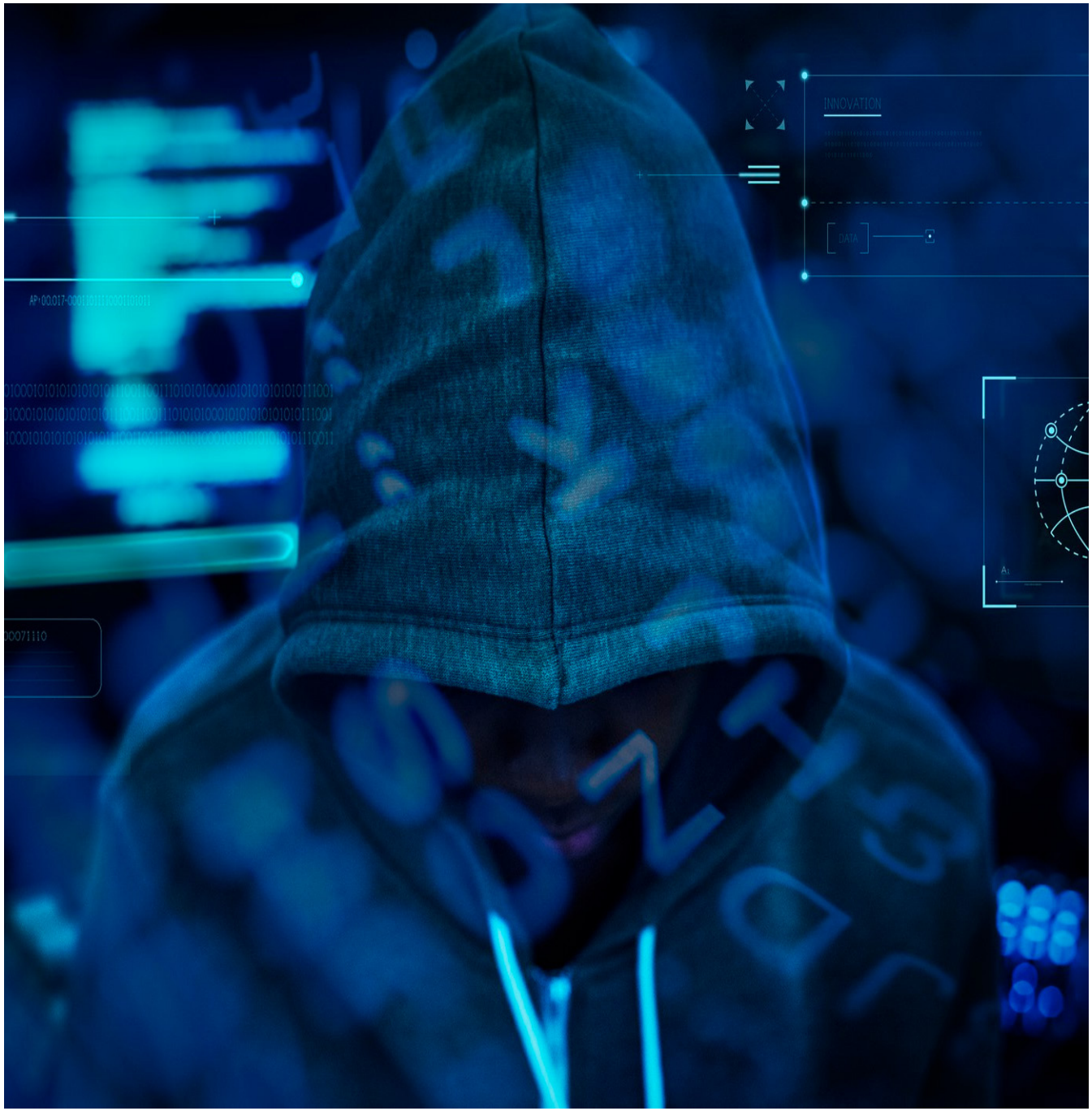
The objective of the GAB Fraud Reports is to complement the work of the Bank of Ghana by providing timely, structured, and forward-looking insights into emerging fraud typologies. The reports document prevailing modus operandi,

highlight control gaps, and quantify the financial and operational impact of fraud incidents across member banks. This approach supports industry-wide learning and informed decision-making.

Building on earlier quarterly editions, this report examines the growing volume, complexity, and digital intensity of fraud cases recorded between September and December 2025. Each case has been reviewed in detail, with narratives developed to illustrate evolving schemes, behavioural drivers, and control weaknesses. In line with established practice, all identifying information has been anonymized to preserve institutional confidentiality and protect customer privacy.

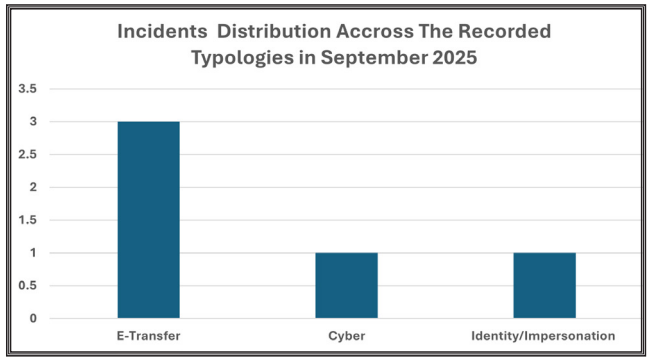
This initiative reflects GAB's broader commitment to strengthening interbank collaboration, enhancing situational awareness, and promoting a collective defence against fraud. By institutionalizing periodic fraud reporting, the Association seeks to support a shift from reactive response to a more intelligence-led and preventive approach to fraud risk management.

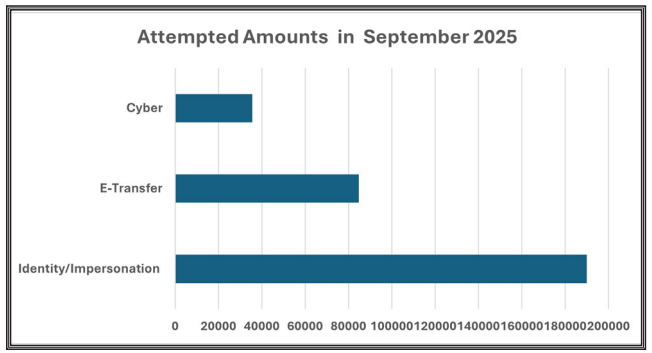
Member banks are encouraged to integrate these insights into operational controls, staff training, and strategic planning, while customers are urged to remain vigilant partners in fraud prevention. Through shared responsibility and proactive engagement, Ghana's banking sector can continue to strengthen its defences and preserve trust in an increasingly digital financial environment.

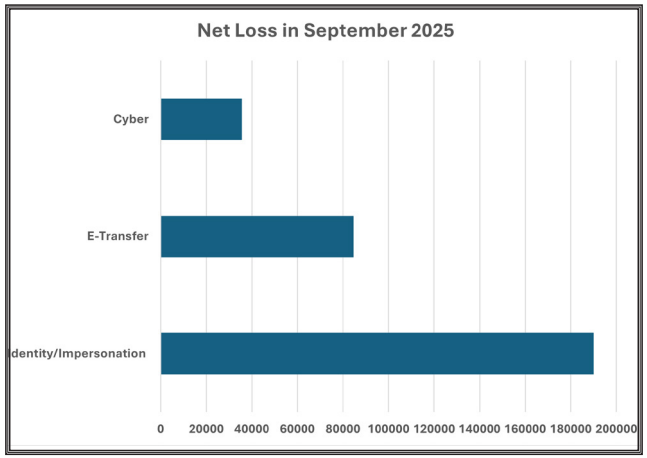


# THE NARATIVE IN SEPTEMBER 2025

The fraud incidents recorded in September 2025 reflects the continued shift in Ghana's banking sector toward digitally enabled and identity-driven fraud, where speed and deception consistently outpace detection and recovery. Although only five cases were reported during the month, the financial impact was significant, with a total attempted amount of GHS 310,300 and no recoveries, resulting in a 100% net loss.




Fraud activity was heavily concentrated in mobile and electronic transfer channels, particularly where bank platforms interface with mobile money wallets. Fraudsters relied extensively on social engineering, credential harvesting, and impersonation, using phone calls, deceptive links, and false authority to obtain login details, OTPs, and device approval codes. Once accounts were compromised, funds were rapidly transferred to mobile wallets and withdrawn before effective intervention could occur. Cases involving delayed reporting of stolen mobile devices further illustrated how customer behavior can neutralize existing controls.

From a typological perspective, E-Transfer fraud dominated by frequency, accounting for three of the five cases (60%), with GHS 84,700 involved, representing 27.3% of total losses. While these incidents were smaller in individual value, the absence of recoveries meant all losses were fully crystallized.

In contrast, Identity Theft and Impersonation, though limited to one case, was the most financially severe, involving GHS 190,000 that is over 61% of total losses for the month. This incident demonstrated how authority-based impersonation and internal trust exploitation can produce outsized losses when verification discipline is relaxed.

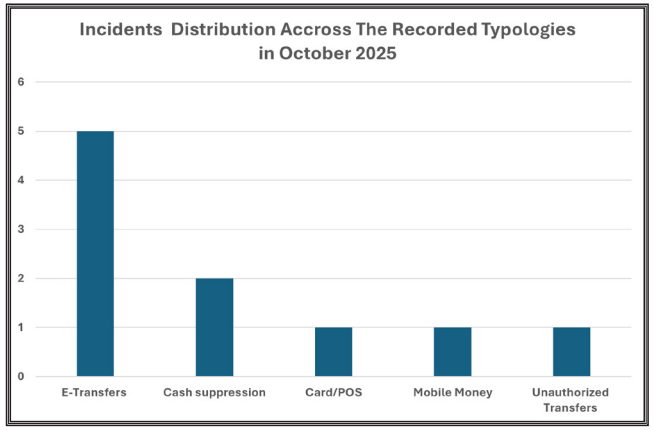
Cyber fraud accounted for one case involving GHS 35,600 (11.5%), arising from credential harvesting via deceptive online links. While smaller in value, it reinforced the role of cyber techniques as key enablers of broader digital fraud.

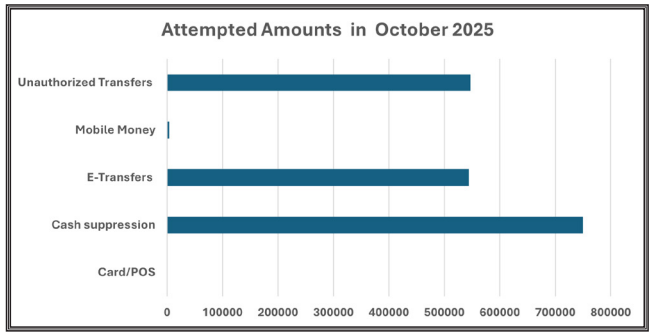
Overall, September 2025 revealed a low-volume but high-severity fraud environment, marked by a sharp imbalance between frequency and financial impact across typologies. The average loss per case of approximately GHS 62,060 underscores the intensity of risk even when incident counts are low. The complete absence of recoveries highlights the structural challenge of fund retrieval once fraud is executed through electronic channels.

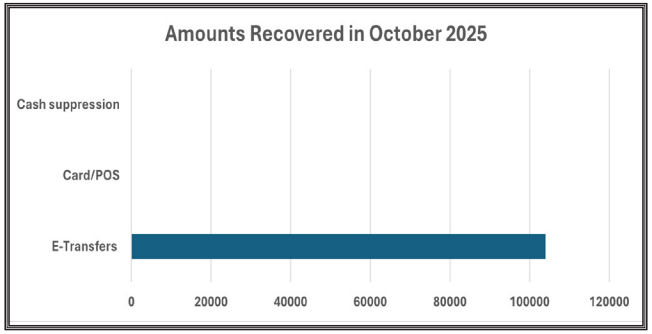
In sum, the month's trends reaffirm that fraud risk is increasingly digitally driven, identity-based, and time-sensitive. Frequent, lower-value E-Transfer fraud continues to erode funds incrementally, while infrequent impersonation incidents pose the greatest systemic threat. Strengthening real-time transaction controls, verification discipline, bank-telco coordination, and sustained customer and staff awareness remains critical to reducing exposure in this evolving threat landscape.

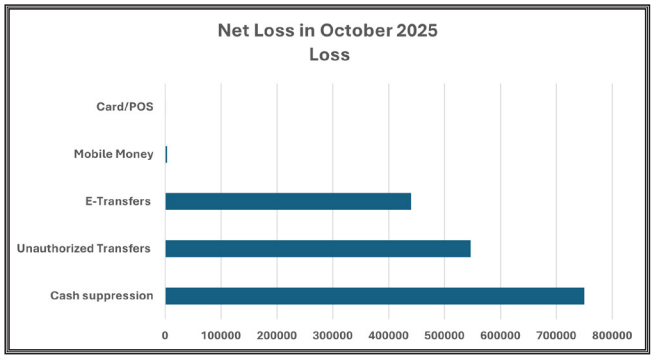
# THE NARATIVE IN OCTOBER 2025

The fraud incidents recorded in October 2025 revealed a sharp escalation in both scale and complexity of fraud within Ghana's banking sector, driven largely by electronic transfers, cash suppression, and unauthorized interbank transactions. During the month, member banks reported ten (10) fraud cases spanning five major typologies, with a total attempted amount of approximately GHS 1.85 million. Recoveries amounted to GHS 104,000, resulting in a net loss of about GHS 1.74 million, underscoring the growing financial severity of fraud risks.




A defining feature of October was the dominance of electronic transfer–related fraud, which accounted for five cases (50% of total incidents) and an attempted amount of GHS 544,220, representing nearly 30% of total exposure. These cases were largely enabled by credential compromise, delayed reporting of stolen devices, and weaknesses in customer data updates, particularly where phone number changes were not fully synchronized across digital channels. Although GHS 104,000 was recovered from one large social-engineering-driven transfer scheme, the remaining electronic transfer incidents resulted in net losses of GHS 440,220, highlighting the persistent difficulty of recovering funds once they exit the banking system into mobile money ecosystems.

Cash suppression emerged as the single largest loss driver by value, with two cases totaling GHS 750,000, accounting for over 40% of the total attempted amount for the month. These incidents involved internal actors and outsourced cash collection personnel, who exploited trust and weak reconciliation processes to withhold customer deposits. Despite arrests, internal investigations, and provisional refunds to customers, the full amounts remained unrecovered at reporting date, reinforcing the enduring risk posed by insider and quasi-insider fraud in cash-handling operations.

October also recorded a high-value unauthorized transfer case, involving GHS 546,891, where forged customer signatures and inadequate reconciliation enabled staff to move funds through the ACH platform to other banks. This single case accounted for almost 30% of total losses, demonstrating how internal control failures and document manipulation can rival digital fraud in financial impact.

In contrast, mobile money fraud was limited to one case involving GHS 3,989, driven by classic social engineering where a customer disclosed multiple credentials to a fraudster impersonating a telecom official. Although smaller in value, the incident mirrored broader trends of identity exploitation and credential surrender.

# THE NARATIVE IN OCTOBER 2025 (CONT....)

Card/POS fraud remained relatively contained, with one low-value case of GHS 831.93, which was fully refunded, illustrating that card-based controls and chargeback mechanisms continue to be more effective than those governing electronic transfers and cash operations.

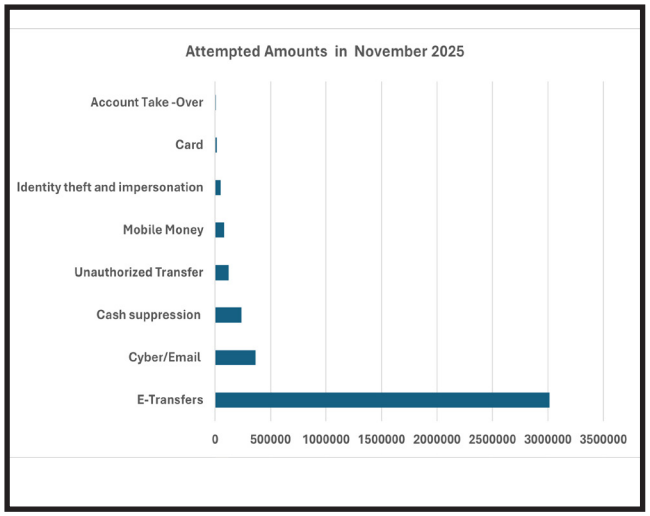
Across all typologies, a recurring pattern was the central role of human behavior, on the side of both customers and staff in enabling fraud. Customers shared PINs, OTPs, and credentials under pressure or deception, while internal lapses in reconciliation, verification, and staff oversight amplified losses. Fraudsters consistently exploited speed and trust, moving funds rapidly before detection and capitalizing on gaps between digital convenience and control robustness.

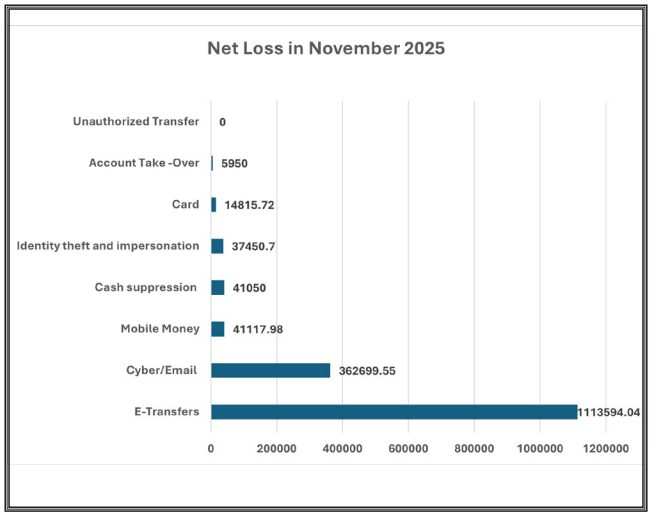
In summary, October 2025 marked a turning point in fraud severity, characterized by higher-value incidents, increased insider involvement, and sustained dominance of electronic transfer channels. While isolated recoveries and refunds provided limited relief, the month's outcomes underscore the urgent need for stronger real-time transaction monitoring, tighter cash-handling oversight, disciplined execution of customer data updates, and continuous staff and customer education. Without decisive improvements in these areas, the convergence of digital and insider fraud risks will continue to magnify losses across the sector.

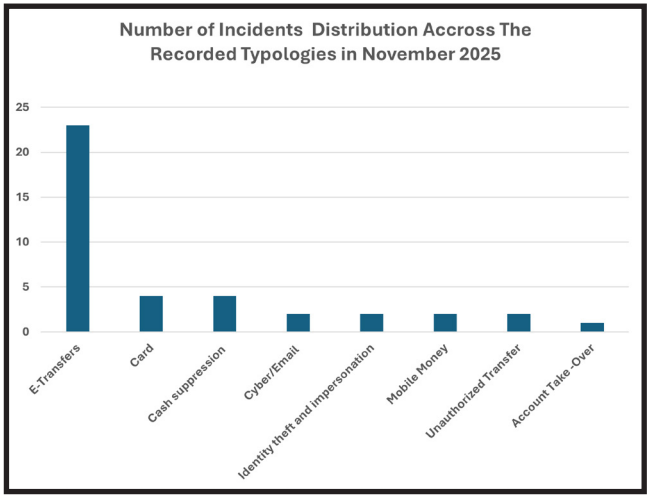
# THE NARATIVE IN NOVEMBER 2025

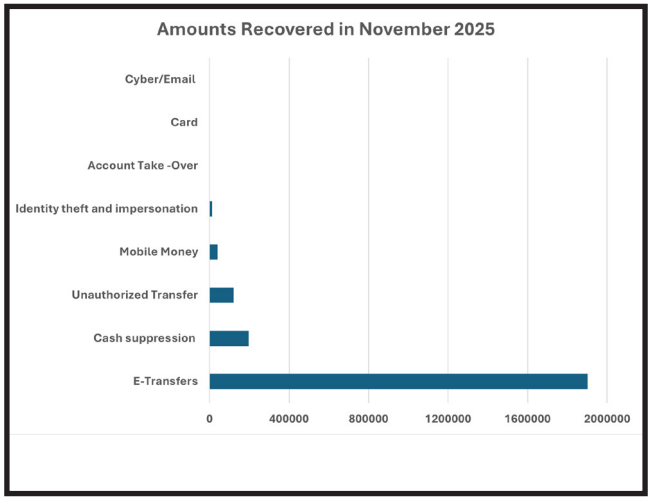
The fraud incidents recorded in November 2025 marked one of the most active and financially significant months within the reporting period, reflecting both the scale and persistence of fraud risks confronting Ghana's banking sector. During the month, member banks reported 40+ fraud incidents spanning eight major typologies, with a total attempted amount exceeding GHS 4.1 million.

Although recoveries were substantial at approximately GHS 2.28 million, the sector still recorded a net loss of about GHS 1.82 million, underscoring the dual challenge of high fraud frequency and uneven recovery outcomes.




A defining feature of November was the overwhelming dominance of electronic transfer–related fraud. E-Transfers accounted for 23 cases, representing over 50% of all incidents reported. These cases involved an attempted amount of GHS 3.02 million, which alone constituted more than 70% of total fraud exposure for the month. While recoveries of GHS 1.90 million mitigated some of the impact, the typology still resulted in a net loss of GHS 1.11 million, making it the single largest driver of net losses. Most of these incidents stemmed from mobile phone theft, social engineering, MoMo linkage abuse, and credential compromise, where fraudsters rapidly moved funds from bank accounts into mobile wallets and onward to multiple networks before detection.

Cash suppression emerged as the second most significant risk area, both in terms of frequency and operational concern. Four cases were recorded, involving GHS 237,510, with recoveries of GHS 196,460, leaving a net loss of GHS 41,050. These incidents largely involved relationship officers, tellers, and direct sales agents, who exploited trust and weak reconciliation to withhold or misuse customer deposits. Although recoveries were relatively strong due to internal investigations and disciplinary action, the recurrence of such cases highlights persistent insider risk and control weaknesses in cash-handling processes.

Cyber and email-enabled fraud also featured prominently, with two cases totaling GHS 362,699.55, all of which resulted in net loss due to zero recovery. These cases involved email impersonation of senior company officials and smishing , where fraudulent instructions bypassed verification protocols and harvested card details for unauthorized online transactions. The complete loss rate in this category reinforces the difficulty of recovering funds once cyber-enabled fraud is executed.

Unauthorized transfers, though limited to two cases, involved GHS 121,300, but notably recorded full recovery, resulting in zero net loss. These cases were largely linked to internal misconduct, including unauthorized postings and transfers by staff, which were detected early through internal controls and reversed. This contrast demonstrates that timely detection significantly improves recovery outcomes, particularly for internally originated fraud.

Mobile money fraud accounted for two cases with a combined attempted amount of GHS 80,600. Recoveries of GHS 39,482.02 reduced the net loss to GHS 41,117.98. These incidents were driven by impersonation of bank staff and social engineering of branch personnel, illustrating that mobile money fraud increasingly targets not only customers but also operational staff through authority-based deception.

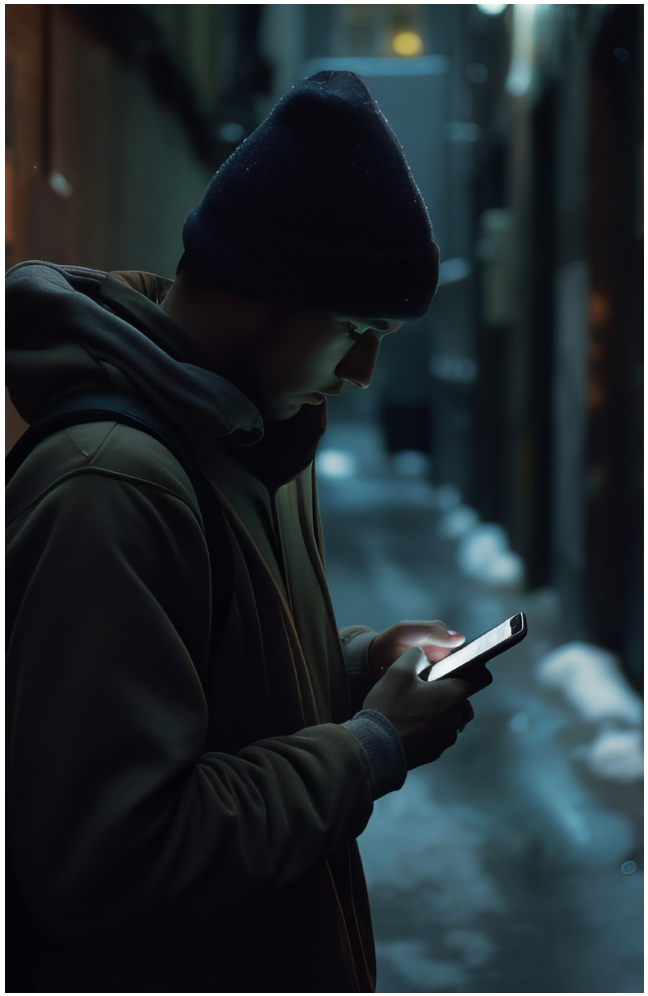
Identity theft and impersonation recorded two cases, involving GHS 49,450.70, with recoveries of GHS 12,000, leaving a net loss of GHS 37,450.70. These cases cut across both customer impersonation and misuse of internal processes, reaffirming that identity-based fraud remains a potent risk vector when verification controls are weak or inconsistently applied.

Card fraud, while relatively contained, involved four cases totaling GHS 14,815.72, all of which resulted in net loss. These incidents were largely card-not-present transactions on international merchant sites, again reflecting global fraud trends manifesting locally.

Finally, account take-over fraud, though limited to one case, resulted in a net loss of GHS 5,950, following device theft and delayed credential updates. This case reinforced the ongoing risk posed by poor device security and delayed customer response.

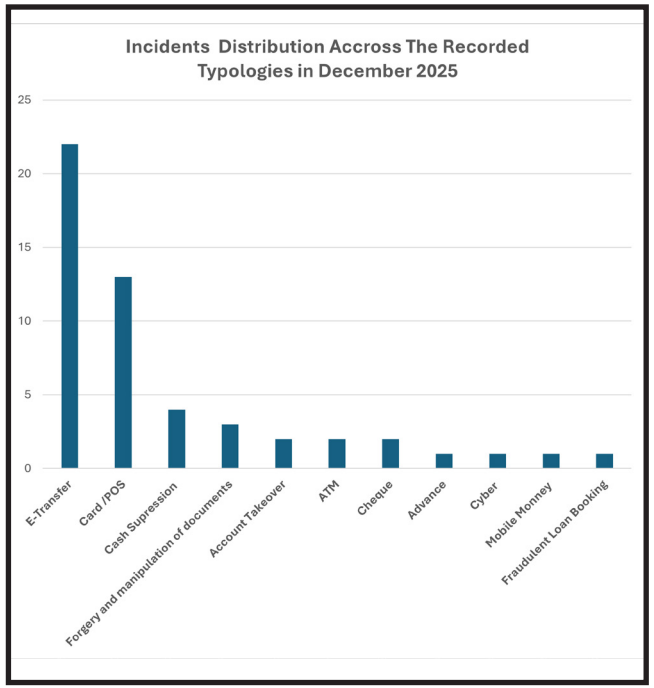
November 2025 therefore depicts a high-volume, high-value fraud environment, where electronic transfers dominate exposure, insider-related fraud persists despite controls, and cyber-enabled schemes continue to produce near-total losses. While recoveries were materially higher than in prior months, they were unevenly distributed, with successful recoveries largely limited to cases detected early or involving internal reconciliation.

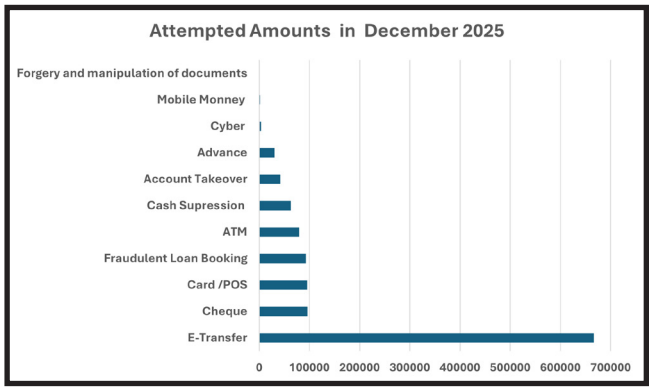
In summary, the month reinforces the urgency of strengthening real-time transaction monitoring, tightening verification discipline (especially for electronic and email instructions), enhancing cash-handling oversight, and deepening staff and customer awareness. Without sustained improvements in these areas, the scale and velocity of fraud observed in November will continue to pose significant financial and reputational risks to the banking sector.

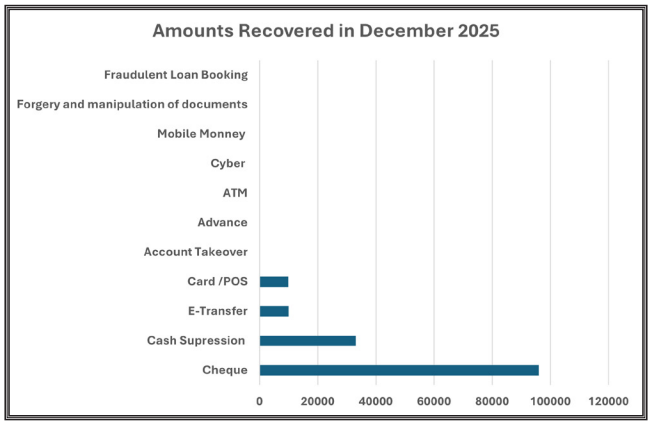


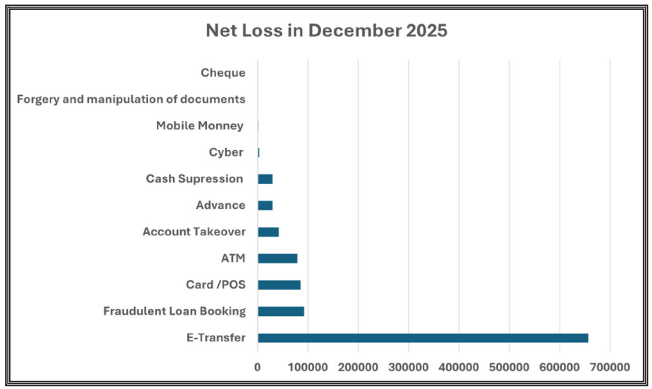
# THE NARATIVE IN DECEMBER 2025

The fraud incidents recorded in December 2025 reflect a high-activity, multi-typology threat environment, combining persistent digital-channel abuse with recurring operational and identity-based weaknesses. Across the month, member banks reported 52 fraud incidents spanning 11 typologies, with a total attempted amount of GHS 1,169,469.89. Recoveries amounted to GHS 149,006.91 (about 12.7% of the amount at risk), leaving a net loss of GHS 1,020,462.98 (about 87.3% of exposure).This profile confirms that losses remained heavily concentrated in fast-moving digital channels and high-impact internal/identity compromises.




E-Transfer-related fraud dominated in December with 22 cases (42.3% of all incidents) and an attempted amount of GHS 666,392.84 representing about 57.0% of total exposure. Although GHS 10,000 was recovered within this category, the typology still recorded a net loss of GHS 656,392.84, representing roughly 64.3% of the month's total losses. These cases were largely driven by credential compromise, mobile-to-wallet fund movements, USSD exploitation, and rapid cash-outs, including scenarios where customers disclosed PINs/OTPs to fraudsters through impersonation and fake merchant links ; and in most instances where suspicious activity occurred without timely containment.

Alongside E-Transfers, Card/POS fraud remained materially active, with 13 cases (25.0% of all incidents) involving GHS 95,215.43 (about 8.1% of total exposure). Only GHS 9,929.91 was recovered, leaving a net loss of GHS 85,285.52 (about 8.4% of total losses). The pattern was consistent with card-not-present abuse and phishing-led compromise, including fraudulent merchant platforms and impersonation sites, reinforcing the continued spillover of global card fraud dynamics into local banking exposure.

December also revealed persistent weaknesses in operational handling and internal control discipline. Cash suppression, recorded in 4 cases (7.7%), involved GHS 62,677 (about 5.4% of exposure). With GHS 33,077 recovered, the typology closed at a net loss of GHS 29,600(2.9% of total losses), an indicative

# THE NARATIVE IN DECEMBER 2025 (CONT.....)

of recurring internal/agent vulnerabilities in cash collection and reconciliation. Similarly, ATM-related fraud though limited to 2 cases (3.8%) also resulted in a net loss of GHS 79,200, driven by preventable weaknesses such as default PIN non-change and opportunistic cash collection after customer error, demonstrating how basic hygiene failures continue to generate outsized losses.

Fraud anchored in identity compromise and account access also remained evident. Account takeover accounted for 2 cases (3.8%) involving GHS 42,100, with no recovery, resulting in a full net loss of GHS 42,100. These incidents were largely linked to email compromise, password reset manipulation, beneficiary creation, and OTP harvesting, reflecting the growing exposure created when authentication and notification controls are bypassed or weakened.

Beyond account takeover, December recorded a Fraudulent Loan Booking incident of 1 case (1.9%),where GHS 92,700 was fraudulently booked in a customer's name, resulting in a full net loss of GHS 92,700. Although low in frequency, this typology is high-risk because it combines identity misuse, documentation gaps, and downstream reputational and legal exposure.

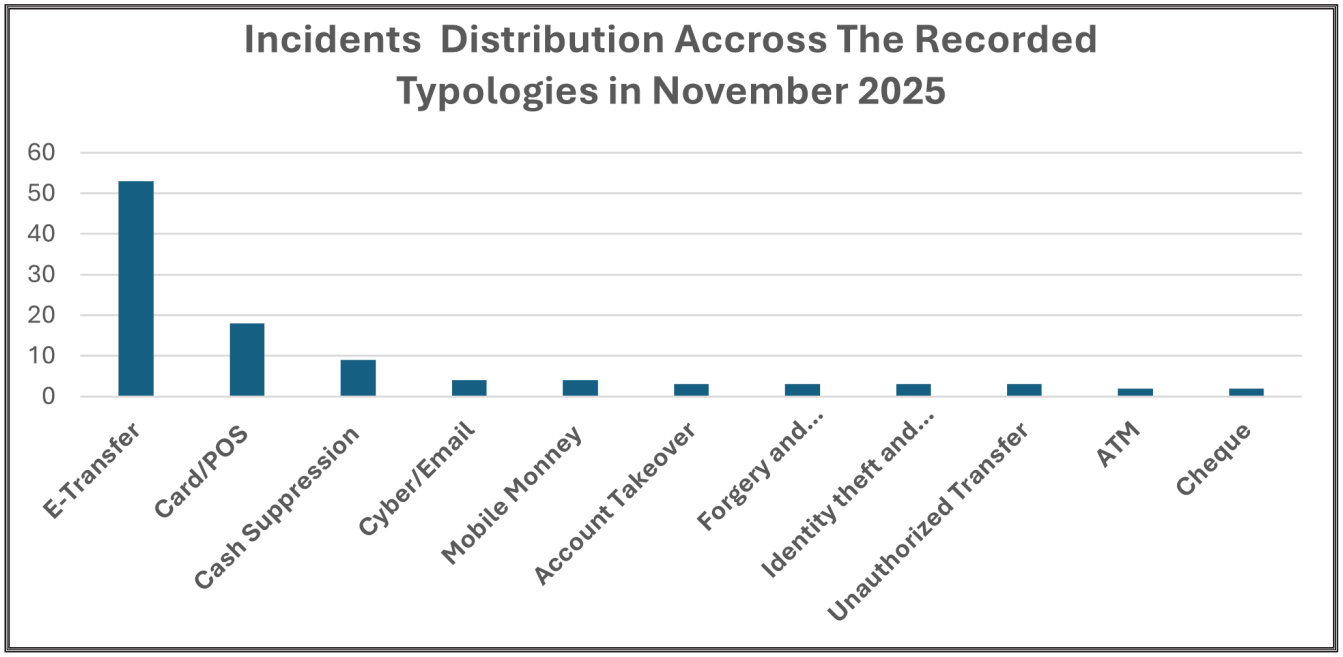
Encouragingly, Cheque-related cases showed the strongest recovery outcome. Cheque fraud recorded 2 cases (3.8%) involving GHS 96,000, with GHS 96,000 recovered, resulting in zero net loss , an evidence that traditional controls such as cheque validation and early interdiction can still be effective when properly applied. Similarly, Forgery and manipulation of documents involving 3 cases (5.8%) recorded no financial loss, as attempted forged statements and related document schemes were detected and contained, though they continue to pose reputational and compliance risks.

In summary, December 2025 was characterized by a strong concentration of losses in E-Transfers and digitally mediated fraud, with recoveries largely limited to cheque interdictions, selective card recovery, and partial internal cash suppression containment. The month's trends reinforce three priorities: tighter real-time control over bank-to-wallet and USSD activity, stronger identity and account-access safeguards (especially email/OTP pathways), and sustained discipline in operational controls such as cash handling and customer authentication.

# THE PREVAILING MODUS OPERANDI ACROSS SEPTEMBER–DECEMBER 2025

Between September and December 2025, fraud incidents across the banking sector converged around a relatively narrow but highly effective set of modus operandi, reflecting a shift away from technically complex attacks toward behaviour-driven exploitation of digital channels, internal processes, and trust relationships. Across the period, fraudsters demonstrated a clear understanding of how banking systems, customer behaviour, and operational workflows interact, and consistently targeted the weakest points within this ecosystem.

A dominant modus operandi throughout the four months was credential harvesting through social engineering, which served as the primary entry point for most digital fraud incidents. Fraudsters repeatedly contacted customers via phone calls, WhatsApp messages, SMS links, and fake online platforms, presenting themselves as mobile network operators, bank officials, online vendors, loan facilitators, or service providers offering discounted data bundles or urgent account assistance. Through these engagements, customers were induced to disclose sensitive information such as mobile money PINs, USSD codes, mobile banking passwords, one-time passwords (OTPs), and device approval codes. Once these credentials were obtained, fraudsters either re-registered mobile banking applications on new devices or executed direct transactions through USSD and mobile apps, effectively turning the customer into the unwitting authorizer of the fraud. This approach proved particularly potent because it bypassed traditional technical controls; authentication was compromised at the human level rather than the system level.




Closely linked to credential compromise was the exploitation of lost or stolen mobile devices combined with delayed reporting. Numerous cases across the period showed that when customers failed to promptly notify their banks after losing a phone, fraudsters were able to self-register USSD services, onboard mobile applications, or reactivate dormant digital channels. This window of opportunity allowed unauthorized bank-to-wallet transfers to be executed and cashed out rapidly. The recurring nature of this modus operandi underscores how transaction security can be rendered ineffective when customer response times lag behind fraud execution speeds. In these cases, the fraud itself was often technically simple, but the absence of immediate account blocking enabled full loss realization.

Another highly consequential modus operandi involved impersonation aimed at bank staff, rather than customers. Fraudsters posed as senior branch officials or internal colleagues and leveraged perceived authority, urgency, and familiarity to manipulate frontline staff into processing transactions outside standard verification protocols.

By referencing internal processes, naming real branches or officers, and conveying instructions verbally, fraudsters were able to override control discipline and induce compliance. These incidents revealed that hierarchical pressure and informal communication channels can undermine even well-designed controls when staff do not insist on formal validation through approved workflows. Although less frequent than customer-facing scams, this modus operandi carried disproportionately high financial impact.

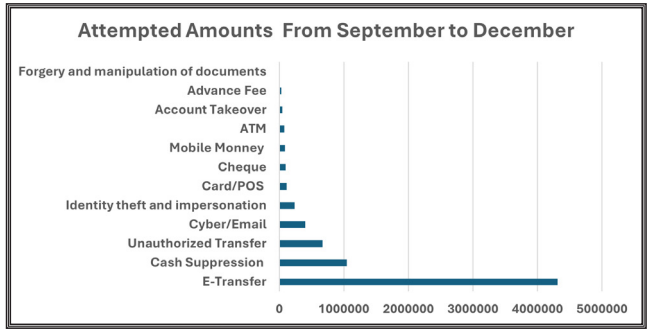
Across nearly all digital fraud cases, the monetization phase followed a consistent and aggressive pattern, centered on mobile money ecosystems. Once funds were transferred out of bank accounts, they were quickly routed into mobile wallets, often spread across multiple beneficiary wallets, and withdrawn or utilized within minutes. The speed of these movements significantly constrained recovery efforts, even when banks acted swiftly to escalate recipient wallets to telecommunications providers. This rapid cash-out strategy reflects deliberate planning by fraudsters, who ensured that wallets, agents, and withdrawal channels were ready in advance. As a result, recoveries were largely dependent on immediate intervention, and delays of even a few hours often translated into total loss.

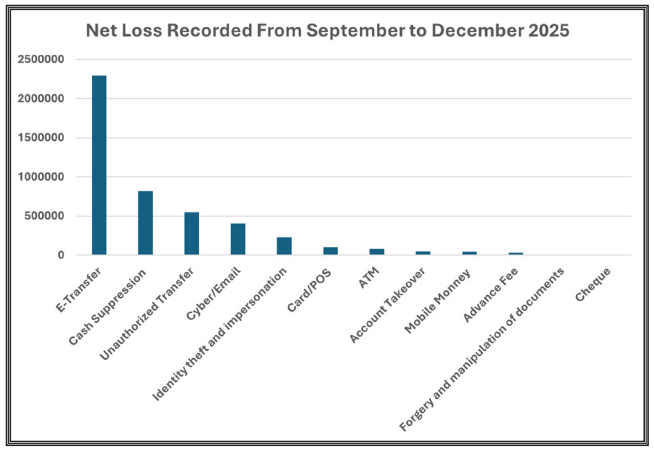
Email compromise and notification manipulation also emerged as a recurring enabling modus operandi. In several cases, fraudsters gained access to customers' or corporate users' email accounts, allowing them to intercept password reset notifications, OTPs, and transaction alerts. In some instances, alerts were deleted or diverted, while in others, customers reported receiving no notifications at all for high-risk transactions. This created a detection gap in which unauthorized activities proceeded unnoticed until balances had already been depleted. The reliance on email and SMS as secondary control layers thus became a vulnerability when those channels were compromised or unreliable.

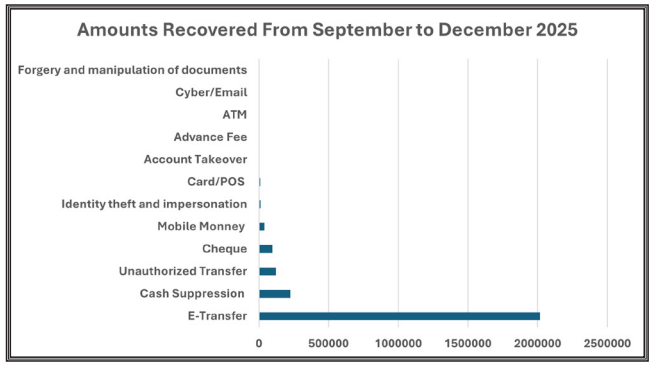
While digital fraud dominated the reporting period, cash suppression and insider-related abuses remained a significant modus operandi, particularly in October and November. These cases involved cash collectors, tellers, or relationship officers receiving customer funds but failing to credit accounts, suppressing deposits until reconciliation or cheque presentation revealed the shortfall. Unlike digital fraud, which relied on speed, cash suppression exploited trust, physical access, and procedural gaps. Detection was often delayed, and although some recoveries were achieved, the incidents highlighted the persistent risk posed by insider misconduct within cash-handling and agency-based models.

Overall, the prevailing modus operandi from September to December 2025 demonstrates that fraud risk is increasingly human-centric and process-driven, rather than purely technological. Fraudsters consistently exploited trust, urgency, authority, and delayed response, using digital channels primarily as execution tools rather than points of intrusion. The convergence of social engineering, mobile channel abuse, impersonation, and rapid monetization reflects a mature fraud environment in which attackers understand not only banking systems, but also human behaviour and organizational dynamics. This pattern underscores the need for controls that combine robust technical safeguards with strong behavioural discipline, real-time monitoring, and sustained education for both customers and staff

# PREVAILING TYPOLOGIES : WHAT DOMINATED AND WHY




### 1) E-Transfer Fraud (Dominant in both frequency and value)

E-Transfer fraud was the most dominant typology, accounting for 53 cases (50.48%), representing half of all incidents. It also carried the largest exposure with an attempted amount of GHS 4,311,056.88 (60.59%), meaning roughly three-fifths of total fraud value flowed through e-transfer channels. Recoveries in this category were GHS 2,016,150 (80.04% of all recoveries), yet it still produced the single largest net loss of GHS 2,294,906.88 (49.93% of total losses).

This confirms that e-transfer fraud is where the sector is most exposed because it combines: (i) customer credential compromise, (ii) instant settlement, and (iii) easy monetization through wallet ecosystems.

### 2) Cash Suppression (Lower frequency, high impact)

Cash suppression recorded 9 cases (8.57%) with attempted amounts of GHS 1,044,810 (14.68%). Recoveries were GHS 224,160 (8.90%), leaving GHS 820,650 (17.85%) in net losses.

Although far fewer than e-transfer cases, cash suppression remained highly damaging because incidents tend to be high-value and are often detected only after reconciliation, complaints, or cheque presentation failures. The recurring presence of cash suppression across October–December also signals persistent vulnerabilities in cash collection models and deposit credit workflows.

### 3) Unauthorized Transfers (High-severity event risk)

Unauthorized transfers accounted for 3 cases (2.86%), but exposure was significant at GHS 668,191 (9.39%). Recoveries reached GHS 121,300 (4.82%), leaving a net loss of GHS 546,891 (11.90%).

The typology reflects high-severity operational failures, including forged signatures and ACH platform abuse. Even with low frequency, the net loss share indicates that these cases are disproportionately damaging.

### 4) Card/POS Fraud (High volume, lower value, customer impact)

Card/POS fraud accounted for 18 cases (17.14%), but attempted value was relatively low at GHS 110,863.08 (1.56%). Recoveries were GHS 9,929.91 (0.39%), resulting in net losses of GHS 100,933.17 (2.20%).

This profile is consistent with persistent card-not-present exposure, phishing-enabled card compromise, and global merchant-based risks. While not the largest financial driver, it remains a reputational and customer trust issue given recurring unauthorized debits and chargeback dependency.

# PREVAILING TYPOLOGIES : WHAT DOMINATED AND WHY (CONT.....)

### 5) Cyber/Email Fraud (Low frequency, 100% loss)

Cyber/email fraud recorded 4 cases (3.81%), with GHS 401,884.17 (5.65%) attempted and zero recovery, resulting in a full net loss of GHS 401,884.17 (8.74%).

This typology continues to function as a gateway risk—through email compromise, smishing, and fraudulent instructions—often enabling broader e-transfer and account takeover fraud.

### 6) Identity Theft & Impersonation (Low frequency, high leverage)

Identity theft and impersonation appeared in 3 cases (2.86%) with GHS 239,450.70 (3.37%) attempted. Only GHS 12,000 (0.48%) was recovered, leaving a net loss of GHS 227,450.70 (4.95%).

These cases demonstrate the enduring power of authority-based manipulation—impersonating branch managers, telco staff, or trusted contacts—to bypass verification discipline and accelerate losses.

### 7) Other channels (ATM, Account Takeover, Mobile Money, Cheque, Advance fee)

Account takeover (3 cases; 2.86%) resulted in GHS 48,050 (0.68%) attempted and GHS 48,050 (1.05%) in losses, reflecting persistent device/email compromise risks.

Mobile money (4 cases; 3.81%) had modest exposure (GHS 86,189) with GHS 39,482.02 recovered, leaving a net loss of GHS 46,706.98.

Cheque fraud (2 cases; 1.90%) was fully contained GHS 96,000 as it recorded zero net loss, reinforcing that traditional controls are still effective when verification is strong.

Advance fee fraud (1 case; 0.95%) produced a full net loss of GHS 30,000, reflecting high victim susceptibility and low recovery probability in such schemes.

## Key Insights and Takeaways (September–December 2025)

• Digital channels are the epicenter of both volume and value. With E-Transfers alone contributing 50.5% of cases and 60.6% of attempted value, the banking sector's primary exposure sits in credential-driven, mobile-enabled transfer ecosystems.

• Recovery success is concentrated, not widespread. While total recoveries reached GHS 2.52 million, the majority (80%) came from E-Transfers, and several typologies; especially Cyber/Email that recorded zero recoveries, confirming that recovery is highly dependent on speed of intervention and reversibility of the payment rail.

• Internal and operational weaknesses remain material and costly. Cash suppression, though only 8.6% of cases, contributed 17.9% of total losses, showing that insider misconduct and cash-handling weaknesses still generate major losses even in a digital fraud era.

• Fraud severity is increasingly shaped by impersonation and process override. Cases involving impersonation of officials, forged instructions, and authority pressure demonstrate that the "human layer" of control remains exploitable ,both on the customer side (social engineering) and within branch operations (staff manipulation).

• Legacy fraud is being contained better than digital fraud. The zero net loss on cheque fraud contrasts sharply with digital channels, reinforcing that structured verification and slower settlement still provide defensive advantages when consistently enforced.

# IMPLICATIONS FOR THE BANKING INDUSTRY

The fraud patterns observed between September and December 2025 carry significant implications for the banking industry, particularly in relation to digital banking growth, operational risk, customer trust, and regulatory exposure.

## Increased Systemic Risk from Digital Channels

The dominance of electronic transfers, USSD, and mobile app transactions confirms that fraud risk has shifted decisively toward digital channels. These platforms allow rapid movement of funds with limited recovery windows. As digital usage continues to expand, fraud losses are likely to rise unless banks redesign controls to match transaction speed. This creates systemic exposure across the industry rather than isolated institutional risk.

## Limited Effectiveness of Post-Transaction Controls

The period under review shows that recovery rates remain low once funds exit customer accounts into mobile money wallets or third-party banks. This reinforces the reality that recovery mechanisms are largely ineffective for digital fraud. Banks that continue to rely on post-incident recalls face growing financial losses and customer disputes. Fraud management must therefore move upstream to prevention and interruption.

## Heightened Operational and Compliance Risk

Impersonation cases, insider involvement, and weak verification processes expose banks to operational failures and control breaches. Where staff acted on verbal instructions or bypassed procedures, the bank assumed liability. These failures increase regulatory scrutiny and raise questions around internal governance, training adequacy, and compliance culture.

## Rising Customer Liability Disputes

A large share of cases involved customers voluntarily sharing PINs, OTPs, and credentials. While customers were often complicit, banks still faced reputational pressure and refund demands. This increases dispute volumes, lengthens resolution timelines, and strains customer relationships. Without clearer customer accountability frameworks, banks will continue to absorb reputational and financial costs.

## Dependency on External Stakeholders

The reliance on telecom operators for wallet blocking and fund recovery highlights a structural dependency outside direct bank control. Delays in telco responses directly reduced recovery outcomes. This dependency increases operational uncertainty and exposes banks to risks they cannot independently mitigate, underscoring the need for stronger inter-industry coordination.

# IMPLICATIONS FOR THE BANKING INDUSTRY (CONT.....)

## Internal Fraud Remains a Persistent Threat

Cash suppression, unauthorized transfers, and fraudulent loan bookings demonstrate that internal fraud remains a material risk. These cases undermine confidence in internal controls and increase losses that are often fully borne by the bank. Weak supervision and delayed detection amplify the impact of such incidents.

## Reputational Impact and Trust Erosion

Repeated fraud narratives involving mobile banking, impersonation, and digital scams risk eroding customer confidence in electronic banking platforms. If customers perceive digital channels as unsafe, adoption may slow, directly affecting banks' digital transformation strategies and cost efficiency objectives.

## Pressure on Regulatory Expectations

The scale and repetition of similar fraud typologies suggest that regulators may demand stronger controls, clearer customer disclosures, and improved fraud reporting standards. Banks that fail to demonstrate effective mitigation may face supervisory action, higher capital buffers for operational risk, or stricter compliance requirements.

## Cost Implications for Banks

Fraud losses, refunds, investigations, litigation exposure, and system upgrades collectively increase operating costs. These costs are likely to rise as fraud volumes grow, placing pressure on profitability, especially in retail and SME banking segments.

## Overall Industry Implication

The September–December 2025 fraud trends indicate that fraud risk is no longer peripheral but central to banking operations. Digital growth without equally strong controls increases losses, operational strain, and reputational damage. The industry must therefore treat fraud risk management as a core strategic function rather than a reactive support activity.

# STRATEGIC RECOMMENDATIONS FOR THE BANKING INDUSTRY

## Strengthen Pre-Transaction Controls on Digital Channels

Banks must shift from reactive fraud handling to prevention. Real-time risk scoring should be embedded in USSD, mobile app, and internet banking transactions, especially for bank-to-wallet transfers. High-risk transactions should trigger step-up authentication, delays, or manual review before execution.

## Move Beyond SMS-Based Authentication

The continued compromise of OTPs delivered via SMS demonstrates that this control is no longer sufficient. Banks should accelerate the adoption of stronger authentication methods such as app-based approval, device binding, behavioural analytics, and transaction confirmation limits for new devices or beneficiaries.

## Tighten Device Management and SIM Change

Unauthorized access following phone theft and SIM reissuance remains a key driver of losses. Banks should enforce cooling-off periods for new device registrations, SIM-linked changes, and wallet linkages. Alerts for device changes must be mandatory and should block transactions until customer confirmation is obtained.

## Enhance Controls Around Bank-to-Wallet Transfers

Given the speed at which funds exit into mobile money ecosystems, banks should impose transaction caps, velocity limits, and delayed settlement for first-time wallet transfers. Industry-wide standards for wallet verification before fund release should be developed in collaboration with telcos.

## Strengthen Staff Verification and Escalation Protocols

Impersonation and social engineering cases involving staff indicate gaps in procedural discipline. Banks should enforce mandatory call-back and dual verification rules for all sensitive instructions, regardless of perceived urgency or seniority. Exceptions should not be permitted.

## Reinforce Internal Fraud Detection and Supervision

Cash suppression and unauthorized internal transfers show weaknesses in supervision. Banks should expand surprise audits, teller rotation, transaction pattern monitoring, and lifestyle red-flag analysis for staff in cash-handling and operations roles. Accountability for supervisory lapses must be enforced.

## Improve Inter-Industry Collaboration

Recovery outcomes depend heavily on telecom responsiveness. Banks, telcos, regulators, and law enforcement should establish formal protocols for rapid wallet freezing, information sharing, and fund tracing. A central fraud intelligence and blacklisting platform should be pursued at industry level.

## Clarify Customer Liability and Responsibility Frameworks

A significant portion of losses arose from customers voluntarily sharing credentials. Banks should clearly communicate liability boundaries and reinforce customer responsibility through revised account terms, onboarding disclosures, and continuous education. This will reduce disputes and manage expectations.

# STRATEGIC RECOMMENDATIONS FOR THE BANKING INDUSTRY (CONT.....)

## Intensify Targeted Customer Education

General fraud awareness messaging is no longer adequate. Education campaigns should focus on specific fraud scenarios observed during the period, including fake investment offers, visa scams, data bundle fraud, impersonation calls, and fraudulent links. Messaging should be continuous and channel-specific.

## Invest in Advanced Fraud Analytics

Banks should prioritise behavioural monitoring, anomaly detection, and cross-channel analytics to identify early warning signals. Fraud systems must correlate customer behaviour, device usage, transaction timing, and beneficiary patterns rather than relying on rule-based thresholds alone.

## Elevate Fraud Risk to Strategic Oversight

Fraud risk should be treated as a core enterprise risk. Boards and senior management must receive regular, data-driven fraud intelligence reports and ensure that fraud mitigation investments are aligned with digital growth strategies.

# CONCLUSION

The fraud patterns observed between September and December 2025 confirm that Ghana's banking sector is operating in an increasingly complex and high-risk environment shaped by rapid digitization, evolving criminal tactics, and persistent human and process vulnerabilities. While digital financial services have expanded access and efficiency, they have also enabled fraud schemes to execute at speed, scale, and with limited recovery once funds move through interconnected bank, mobile money, and card channels.

The period under review shows that fraud risk is now structurally concentrated in electronic transfer and mobile-enabled channels, which together accounted for the majority of cases, attempted values, and net losses. At the same time, cash suppression and other internal control failures remain a material source of financial loss, underscoring that traditional operational risks have not diminished but are instead coexisting with more sophisticated digital threats. This dual exposure highlights the need for banks to manage fraud as an enterprise-wide risk rather than a narrow technology or compliance issue.

A recurring and critical theme across the cases is the central role of human behaviour. Social engineering, impersonation, delayed reporting of device theft, weak adherence to verification protocols, and insider misconduct consistently shaped fraud outcomes. These patterns demonstrate that even robust systems can be undermined where behavioural controls, staff discipline, and customer awareness are weak. Fraud risk in this context is therefore as much a governance, culture, and conduct challenge as it is a technological one.

Recovery outcomes during the period further emphasize the urgency of preventive controls. Once funds are transferred into mobile wallets or layered across accounts, recovery opportunities narrow sharply. This reality reinforces the importance of real-time detection, early intervention, and strong coordination between banks, telecom operators, regulators, and law enforcement agencies to contain losses before cash-out occurs.

In conclusion, the September–December 2025 findings present a clear call to action for boards, management, and industry stakeholders. Strengthening fraud-resistant authentication, enforcing disciplined operational controls, investing in staff and customer education, and deepening interbank and cross-sector collaboration are no longer optional but essential to safeguarding trust in the banking system. Through sustained collective effort and a shift toward proactive, intelligence-led fraud risk management, Ghana's banking sector can better protect customers, preserve financial stability, and reinforce confidence in an increasingly digital financial ecosystem.

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