GHANA ASSOCIATION OF BANKS

INDUSTRY FRAUD REPORT

JANUARY - MARCH 2026

FOLLOW US

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

EXECUTIVE SUMMARY

This report presents a consolidated analysis of fraud cases reported by member banks of the Ghana Association of Banks for the period January to March 2026. It reflects 73 confirmed cases, with a total attempted exposure of approximately GHS 14.05 million. This amount is made up of GHS12.05 million that emerged from the successful cases, with the remaining GHS1.997(about GHS 2 million) from a single wire transfer fraud attempted but prevented. Out of GHS12.05 million recoveries of about GHS 1.01 million were made resulting in a net loss of GHS 11.05 million.

In January, 20 out of the 23 universal banks submitted their reports, while in February and March the submissions dropped to 13 and 14 banks respectively. As a result, the reported figures do not represent full industry aggregates, since the non-reporting banks may have had material cases that could significantly affect the overall outcome, including potential outliers. Accordingly, this report should be interpreted as an indicative or operational guide based solely on the cases reported, rather than a comprehensive reflection of the entire banking industry.

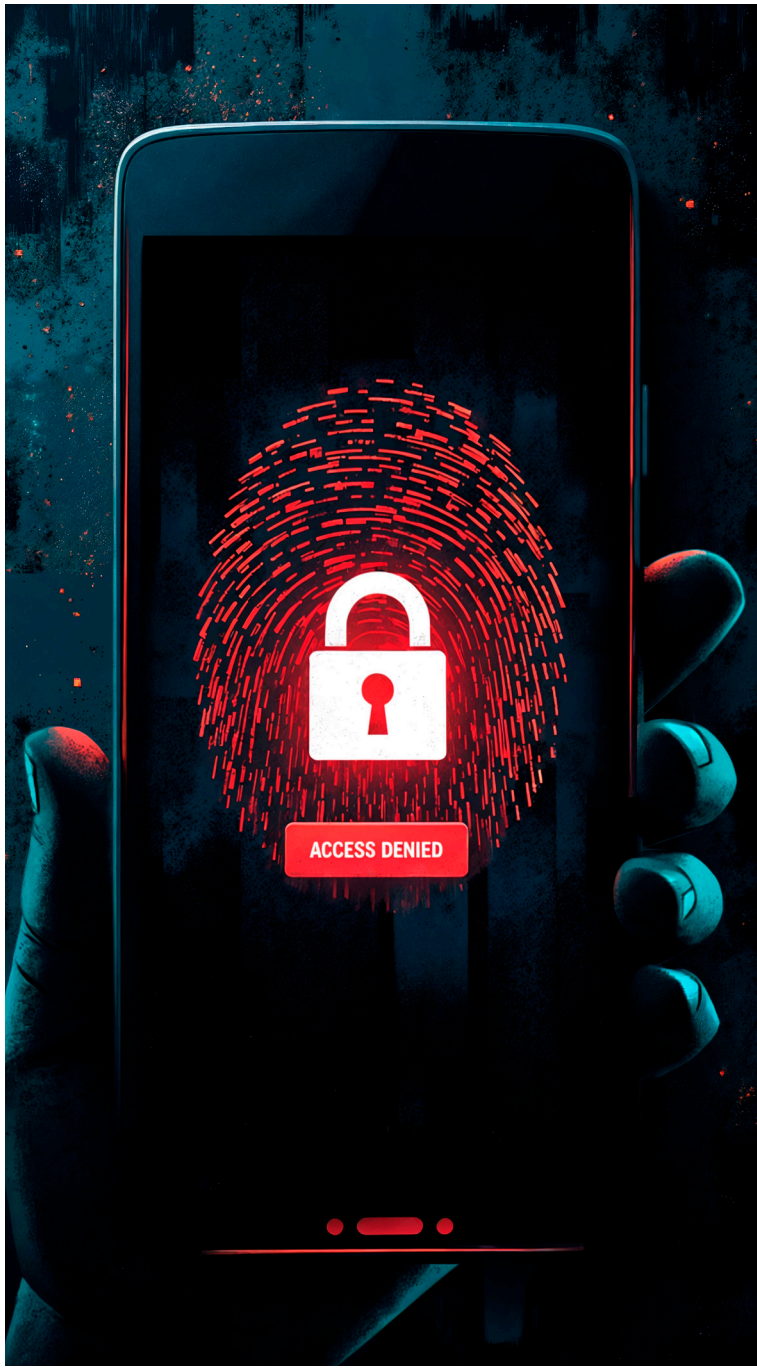
The analysis shows a fraud landscape that is increasingly multi-channel, digitally enabled, and operationally complex. Mobile Money and Card/POS fraud dominate in frequency, while Cash Suppression, Forgery, and E-Transfer fraud account for the most significant financial losses. A key structural concern remains the consistently low recovery rate, particularly in digitally executed frauds where funds are rapidly dispersed across multiple wallets and platforms, making recovery difficult.

Importantly, the report provides a clear and well-structured presentation of fraud modus operandi, offering practical insight into how fraud is executed across different typologies. This is intended to guide risk managers and fraud control teams across the industry in strengthening detection mechanisms, improving preventive controls, and enhancing response strategies.

The findings further confirm that while external fraud is widespread, internal control weaknesses and staff-related misconduct continue to drive some of the most severe financial losses, highlighting the need for stronger governance and supervisory frameworks.

This report forms part of the Ghana Association of Banks' ongoing commitment to strengthen industry-wide fraud mitigation, enhance operational resilience, and support coordinated risk management efforts across member institutions. It also seeks to help the banking industry keep pace with emerging fraud trends and evolving attack vectors.

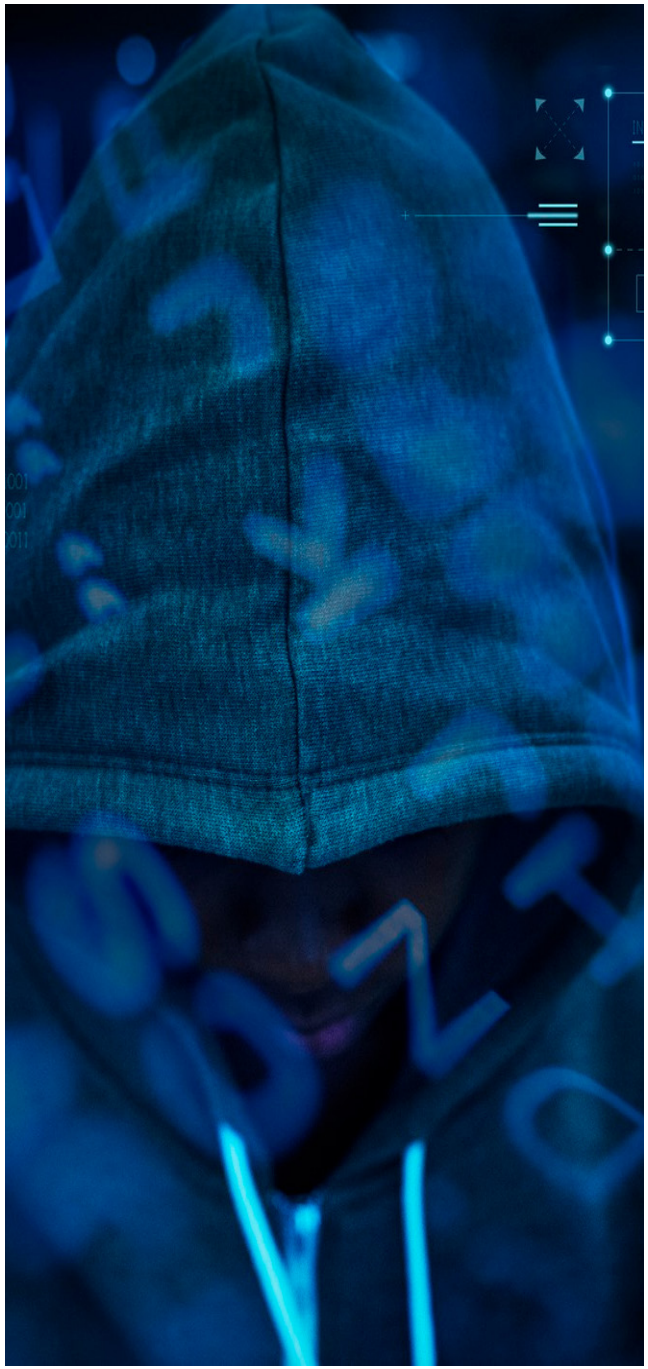
In addition, the Association is advancing preparations for a national-level fraud awareness campaign, aimed at improving both customer and staff vigilance. However, the effectiveness of such initiatives is strongly dependent on timely information sharing across banks and financial



ecosystem partners, which remains critical for maintaining operational alertness and preventing systemic fraud escalation.

Below is a summary of the typological counts and loss distribution of the reported fraud incidences between the period.

The Monthly level consolidation have been presented in the Appendix for further reference.



The typological distribution of fraud cases and losses Reported for Jan-March 2026

Fraud Typology	Cases	Attempted (GHS)	Recovered (GHS)	Net Loss (GHS)
Cash Suppression/Theft	9	5,299,832.03	297,404.80	5,002,427.23
Card/POS	18	3,666,848.71	422,765.48	3,244,083.23
Forgery (incl. Doc. Alteration)	4	2,130,401.54	207,200.00	1,923,201.54
Wire Transfer (Attempted)	1	1,997,200.00	0	0.00*
E-Transfer	7	297,091.84	0	297,091.84
Cheque Fraud	1	200,000.00	0	200,000.00
Mobile Money	23	143,108.00	1,070.00	142,038.00
Cyber/IS	1	105,000.00	0	105,000.00
Manipulation of Accounts	1	77,800.00	62,700.00	15,100.00
Advance Fee	2	65,181.00	0	65,181.00
Social Engineering	2	12,312.84	0	12,312.84
Account Takeover	2	25,885.00	15,000.00	10,885.00
Identity Theft / Impersonation	1	24,433.00	0	24,433.00
USSD Fraud	1	7,019.50	0	7,019.50
Total	**73**	**14,052,113.46**	**1,006,140.28**	**11,048,773.18**

INTRODUCTION

Fraud remains one of the most persistent and evolving risks facing the banking sector in Ghana. The rapid expansion of digital financial services, increased interoperability between banks, mobile money operators, and fintech platforms, and the growing sophistication of fraud techniques have collectively broadened the exposure of financial institutions to diverse and increasingly complex fraud typologies.

This report presents a consolidated review of fraud incidents reported by member banks of the Ghana Association of Banks for the first quarter of 2026. It is designed to provide a structured industry-wide perspective on fraud trends, financial impact, and operational vulnerabilities. The data presented is strictly based on reported cases submitted for January, February and March.

The objective of this report is threefold. First, to provide clarity on the distribution and financial impact of fraud typologies across the banking sector. Second, to highlight emerging patterns, vulnerabilities, and systemic weaknesses that require attention from both operational and strategic risk management perspectives. Third, to support the Ghana Association of Banks' broader mandate of strengthening fraud prevention and mitigation frameworks through coordinated industry action.

While individual banks continue to strengthen internal controls and customer protection systems, the findings underscore the increasing importance of industry-wide collaboration and real-time information sharing. Fraudsters are increasingly exploiting gaps between institutions, channels, and financial ecosystems, making isolated institutional responses less effective.

In response, the Ghana Association of Banks continues to play a central coordinating role in promoting collective resilience. This includes ongoing efforts to enhance fraud intelligence sharing and the development of a national-level fraud awareness campaign, aimed at improving public education and reinforcing preventive behaviour among both customers and staff. However, the success of such initiatives will depend significantly on timely, structured, and consistent information sharing across member banks and ecosystem partners.

Ultimately, this report is intended to contribute to a more coordinated, proactive, and intelligence-driven fraud risk management framework within the Ghanaian banking industry, ensuring that institutions remain responsive to evolving threats while strengthening overall financial system integrity.

JANUARY 2026 FRAUD NARRATIVE: MODUS OPERANDI AND STRATEGIC INSIGHTS

The fraud landscape in January 2026 was largely defined by a recurring pattern: attackers did not primarily break systems; instead, they worked through people, processes, and weak linkages between banking platforms and mobile money ecosystems. The incidents, when viewed together, tell a coherent story of how small lapses, whether by customers or institutions, were systematically exploited to produce financial losses.

A substantial portion of the cases began with what appeared to be routine digital interactions. Customers, in several instances, attempted ordinary activities such as purchasing goods online or responding to what seemed like legitimate service prompts. In the process, they unknowingly disclosed sensitive information, particularly mobile money PINs or banking credentials. Once these details were obtained, fraudsters moved swiftly. Funds were transferred from bank accounts into linked mobile wallets and, almost immediately, dispersed across multiple unknown wallets. This rapid layering made recovery extremely difficult. In many of these situations, the customer had no intention of authorizing any transfer; however, the combination of social engineering and seamless bank-to-wallet integration allowed fraud to be executed efficiently.

Closely related to this pattern were cases where account linkages to mobile money platforms played a central role. Some customers were not fully aware that their bank accounts had been connected to mobile wallets, often through prior registrations or system-driven integrations. Fraudsters exploited this gap in awareness. Once access was gained, either through PIN disclosure or compromised device transactions could be initiated without triggering immediate suspicion. The funds were then funneled through the mobile money ecosystem, where speed and fragmentation worked in favor of the perpetrators. These cases highlight how convenience-driven financial integration, if not properly controlled and communicated, can become a major vulnerability.

In parallel, a number of incidents reflected full or partial account takeover. Here, fraud did not rely solely on tricking the customer remotely but was facilitated by proximity and trust. In one instance, an individual who assisted a customer during account opening and mobile app setup later leveraged that familiarity to gain access to the account. In another, a stolen mobile phone combined with a weak transaction PIN and other details such as a date of birth, provided an easy entry point. Once inside the account, the fraudsters behaved like legitimate users, initiating transfers through approved channels. These cases demonstrate that the line between legitimate assistance and unauthorized access can easily blur when controls around credentials and device security are weak.

Card-related fraud presented a slightly different but equally instructive pattern. Several customers reported unauthorized transactions conducted on online merchant platforms, despite not actively using their cards at the time. This suggests that card details had been compromised earlier and stored for later exploitation, particularly in card-not-present environments. In one notable case, the issue was not external compromise but an internal system anomaly, where an automated reversal mechanism erroneously credited customers for transactions that had already been successfully processed. Some beneficiaries quickly utilized these excess funds. Although recovery efforts were largely successful, the incident exposed how internal system logic, if not rigorously tested, can create fraud-like outcomes even in the absence of external attackers.

Beyond digital channels, there were also incidents rooted in internal process failures and staff misconduct. In these cases, employees directly manipulated transactions or withheld funds entrusted to them by customers. Deposits collected were not credited, and in some instances, accounts were debited without authorization. These actions were often concealed within otherwise normal transaction flows, making detection less

immediate. Eventually, investigations uncovered the discrepancies, and in several cases, partial or full recovery was achieved. Nonetheless, these incidents reinforce the reality that internal actors, when combined with weak supervision and excessive access, can pose risks comparable to external fraudsters.

A particularly high-value case illustrated the growing sophistication of cyber-enabled fraud. The attack began with a fraudulent email prompting the customer to reset their banking credentials. Around the same time, the customer experienced a temporary disruption in mobile connectivity, suggesting a possible SIM-related compromise. With control over both the credentials and communication channel, the fraudsters were able to authenticate transactions and execute multiple withdrawals within a short window. By the time the activity was detected, the funds had already been moved and depleted. This sequence shows how modern fraud schemes increasingly combine phishing, identity compromise, and telecom manipulation to bypass traditional safeguards.

There were also instances where customers were drawn into advance payment schemes, believing they were engaging in legitimate commercial transactions. Payments were made to individuals posing as suppliers or intermediaries, often through informal online platforms. Once the funds were transferred, communication ceased entirely. Unlike other cases, these incidents did not involve unauthorized access but rather deliberate deception that induced voluntary payment, making recovery particularly challenging.

In all, the January cases reveal a consistent underlying theme: fraud is increasingly driven by the exploitation of trust, speed, and integration across financial channels. Whether through social engineering, weak credential practices, system loopholes, or insider access, perpetrators are leveraging the very features designed to enhance convenience and efficiency.

For banks, the implications are clear. The first and most immediate lesson is that customer-facing vulnerabilities are now the primary entry point for fraud. Education can no longer be treated as a secondary control; it must be continuous, targeted, and responsive to evolving tactics. At the same time, the speed at which funds are moved, especially into mobile wallets, means that detection and response must occur in real time, not after the fact.

Equally important is the need to reassess authentication frameworks. Reliance on single-factor or easily compromised credentials is no longer sufficient in an environment where attackers can intercept communications or manipulate users. Stronger, layered authentication mechanisms are essential.

Internally, the cases highlight that controls around staff access, transaction monitoring, and reconciliation must remain robust and dynamic. Even as banks invest in digital transformation, traditional risks such as staff misconduct have not disappeared; they have simply evolved in form.

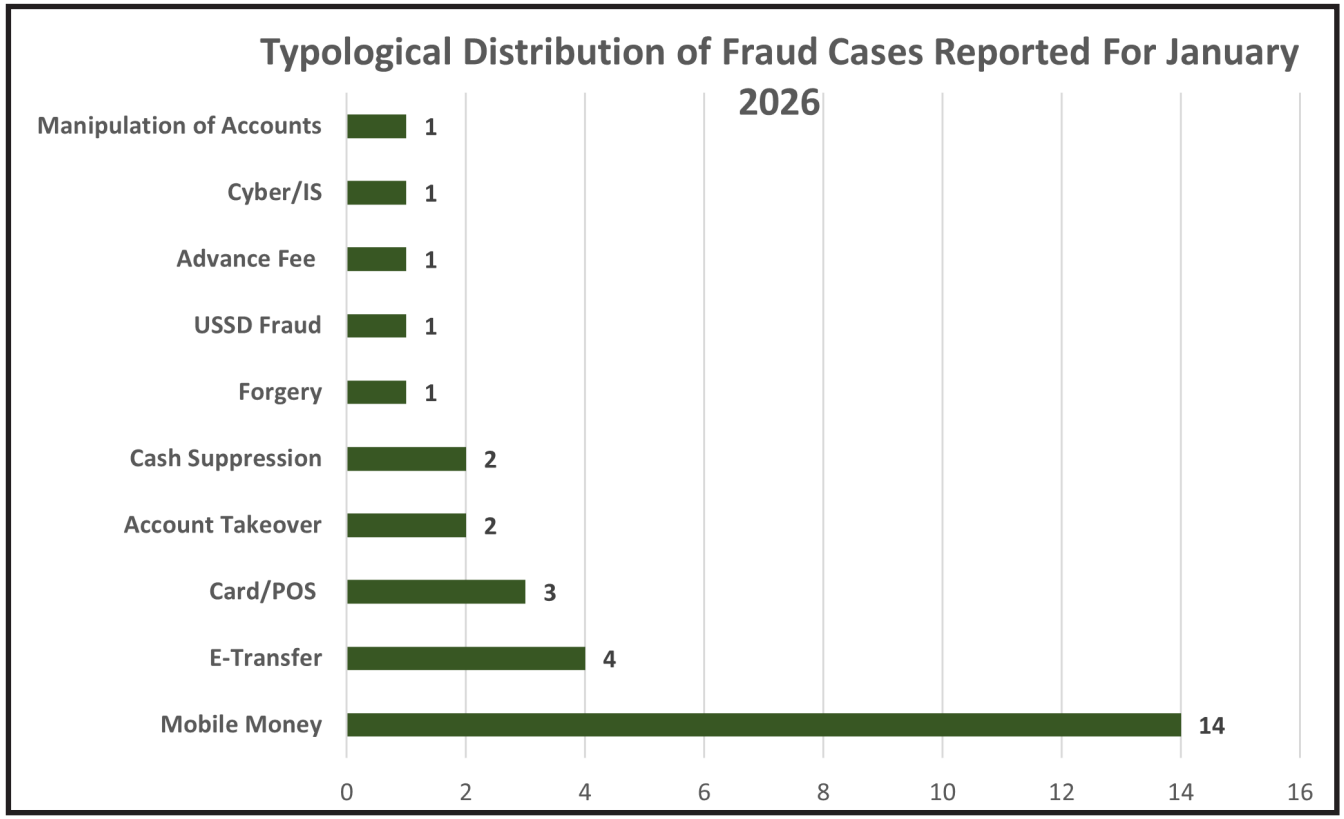
Finally, the increasing intersection between banking systems and external platforms, particularly mobile money and telecommunications networks, underscores the need for closer institutional collaboration. Fraud prevention can no longer be managed in isolation; it requires coordinated action across the broader financial ecosystem.

In essence, January's fraud incidents do not point to a single weakness but rather to an interconnected risk environment, where human behavior, technology, and process gaps converge. Addressing this requires an equally integrated response; one that combines technology, policy, and continuous vigilance.

TYPOLOGICAL DISTRIBUTION AND LOSS ANALYSIS FOR JANUARY 2026

The fraud landscape in January is heavily concentrated in a few dominant typologies, both in terms of frequency (number of cases) and financial impact (amounts involved and losses), revealing a clear divergence between high-volume retail fraud and low-frequency, high-impact fraud.

From a case distribution perspective, Mobile Money fraud overwhelmingly dominates, accounting for 14 out of 30 cases (47%). This confirms that mobile money remains the most frequently exploited channel, largely driven by social engineering and wallet-linkage vulnerabilities observed earlier. The next most frequent categories are E-Transfer (4 cases) and Card/POS fraud (3 cases) are significantly lower, while all other typologies occur as isolated or low-frequency events (1–2 cases each). This indicates a long tail of fraud types, where multiple niche typologies exist but are not as recurrent.



However, when the focus shifts from frequency to financial exposure, the structure changes dramatically. Card/POS fraud emerges as the single most significant risk driver, accounting for GHS 2.44 million out of the total GHS 2.86 million attempted (≈85%). Despite representing only 3 cases, it drives the overwhelming majority of losses, with no recoveries recorded, resulting in a full net loss of GHS 2.44 million. This clearly categorizes Card/POS fraud as a low-frequency, high-severity risk, requiring disproportionate attention relative to its occurrence.

In contrast, Mobile Money fraud, while the most frequent, involved GHS 41,133 attempted, with minimal recovery (GHS 1,070) and a net loss of GHS 40,063. This reinforces its classification as a high-frequency, low-to-moderate value fraud, which cumulatively contributes to losses but is not individually catastrophic. The operational implication is that Mobile Money fraud is more of a volume-driven risk, requiring scalable controls rather than case-by-case intervention.

E-Transfer fraud also shows a notable impact, with GHS 35,690.34 in attempted amounts and no recoveries, translating directly into losses. This suggests weak recovery mechanisms once funds are transferred, aligning with the earlier observation of rapid fund movement across wallets and accounts.

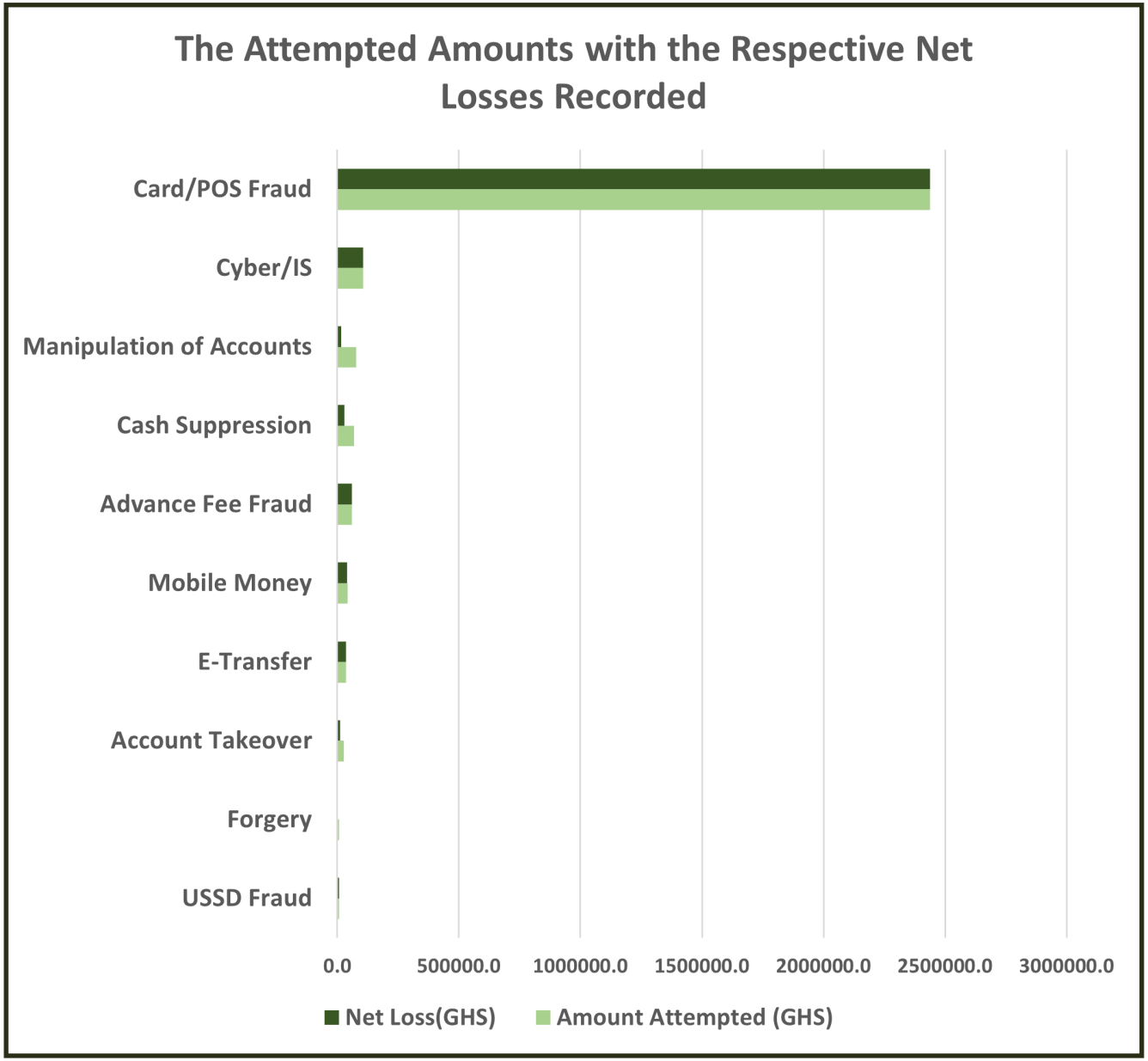
Mid-tier risk categories include Cyber/IS fraud (GHS 105,000 loss) and Advance Fee fraud (GHS

59,112 loss), both of which are single-case but high-impact incidents. These typologies highlight the growing importance of cyber-enabled deception and online transaction risks, where even isolated cases can materially affect total losses.

A particularly important insight emerges from Account Takeover and Manipulation of Accounts. Although these involve relatively moderate attempted amounts (GHS 25,885 and GHS 77,800 respectively), they show partial recoveries (GHS 15,000 and GHS 62,700). This suggests that fraud involving identifiable beneficiaries or internal linkages has a higher probability of recovery, unlike more anonymous channels such as card fraud or mobile money dispersals.

Similarly, Cash Suppression recorded GHS 68,300 attempted with GHS 39,000 recovered, indicating that internally driven fraud cases are more recoverable, likely due to traceability and institutional control over staff.

At the lower end, Forgery stands out as the only typology with full recovery (GHS 7,200) and zero loss, suggesting that fraud involving physical interaction and identifiable perpetrators is easier to resolve compared to digital and cross-platform fraud.



FEBRUARY 2026 FRAUD NARRATIVE : MODUS OPERANDI AND STRATEGIC INSIGHTS

The fraud incidents recorded in February 2026 present a more complex and layered picture than the previous month. While digital fraud remained prevalent, there was a noticeable shift toward high-value internal fraud, structured deception, and control failures within operational processes. The cases, when read together, reveal how fraudsters , both external and internal, systematically exploited trust, procedural gaps, and weaknesses in oversight to execute and, in some cases, sustain fraudulent activity over time.

The month began with an incident that clearly illustrates how well-established operational relationships can be manipulated for prolonged fraud. A teller, operating within an agency environment, exploited familiarity with a customer to repeatedly siphon funds during deposit transactions. By subtly removing portions of cash before processing deposits and discouraging the customer from verifying amounts, the suspect was able to sustain the scheme over several months. The fraud was not a one-off event but a deliberate, repetitive pattern built on trust and routine, only uncovered through CCTV review and subsequent investigation. The immediate recovery of a portion of the funds, alongside the suspect's admission of a much larger cumulative theft, underscores how such schemes can remain undetected until a trigger event prompts scrutiny.

In contrast, another case demonstrated how fraud can be prevented when controls are properly applied. An attempt was made to induce the bank into reversing a non-existent mobile money transaction under the pretext of an erroneous transfer. The request followed a known fraud pattern, but verification procedures revealed that no such transaction had occurred. By declining the request and escalating awareness internally, the bank effectively neutralized the attempt. This incident highlights the importance of pattern recognition and adherence to verification protocols, particularly in environments where fraudsters rely on urgency and deception rather than system compromise.

Card-related fraud featured prominently during the month, with multiple cases involving unauthorized transactions across online merchant platforms. Customers reported receiving debit alerts for transactions they did not initiate, often from international or unfamiliar merchants. In some instances, customers had received one-time passwords but denied using them, suggesting either credential compromise or manipulation during authentication processes. These transactions were typically executed rapidly across multiple platforms, indicating that once card details were exposed, fraudsters acted quickly to maximize gains before detection. The bank's response of blocking cards and restricting accounts, helped contain further losses, but the incidents point to ongoing vulnerabilities in card-not-present environments and customer interaction with authentication prompts.

A particularly instructive set of cases involved staff-driven fraud and internal manipulation of funds. In one instance, staff handling corporate funds altered deposit documentation and diverted significant amounts before handing over reduced values for processing. In another case, a teller directly withdrew funds from customer accounts by forging authorization through thumbprints, deliberately structuring transactions below supervisory thresholds to avoid detection. These cases demonstrate a calculated understanding of internal controls and how they can be bypassed. The fraudsters did not act randomly; they operated within system limits, exploiting approval thresholds and documentation processes to conceal their actions.

Beyond direct cash manipulation, the month also revealed a deeper level of institutional risk through a case involving fraudulent collateral documentation. A credit facility had been granted based on property presented as collateral, supported by valuation reports and legal documentation. However, subsequent investigation revealed that the property did not belong to the borrower, and the supporting documents including certificates from official sources were falsified. The fraud was not limited to a single document but involved a chain of failures across valuation, legal verification, and credit approval processes. By the time the issue was uncovered, the exposure had reached a significant level. This case highlights how fraud can be embedded within core banking activities such

as lending, where reliance on documentation and third-party verification creates opportunities for manipulation.

Digital fraud continued to manifest through social engineering and mobile money channels, though often with smaller transaction values compared to internal fraud cases. Customers were contacted by fraudsters posing as bank staff or service providers and were persuaded to disclose sensitive information or follow malicious links. In other instances, customers knowingly used mobile money services but later disputed transactions they did not authorize, suggesting that access to their wallets had been compromised. Funds were typically transferred out of accounts and quickly moved across wallets, reinforcing the recurring challenge of speed and traceability in mobile money ecosystems.

There were also cases that fell into the category of advance fee fraud, where customers engaged with individuals on online platforms for the purchase of goods. Payments were made in good faith, but once funds were transferred, the supposed sellers became unreachable. These incidents did not involve unauthorized system access but rather deception that induced voluntary transactions, making prevention largely dependent on customer awareness rather than system controls.

Another notable incident involved what initially appeared to be fraud but was later understood as an operational error with financial consequences. A teller, after identifying a cash discrepancy during a transaction, mistakenly compensated the customer instead of reconciling the difference properly, resulting in a loss. While not fraudulent in intent, the case highlights how human error within transactional processes can produce outcomes similar to fraud, particularly in high-pressure environments.

Across all cases, a clear narrative emerges. Fraud in February was not confined to a single channel or technique; instead, it spanned external deception, internal manipulation, documentation fraud, and operational lapses. The common thread is the exploitation of trust, weak verification processes, and gaps in oversight.

For banks, several important insights arise from these patterns. First, internal controls and staff oversight require continuous strengthening, particularly in areas involving cash handling, account access, and transaction authorization. Fraudsters operating from within the system often possess detailed knowledge of control weaknesses and can exploit them systematically over time.

Second, verification processes, whether for transactions, customer requests, or collateral documentation must be rigorous and consistently applied. The effectiveness of controls is not only in their design but in their execution. Where verification was strictly followed, fraud attempts were successfully prevented; where it was weak or bypassed, losses occurred.

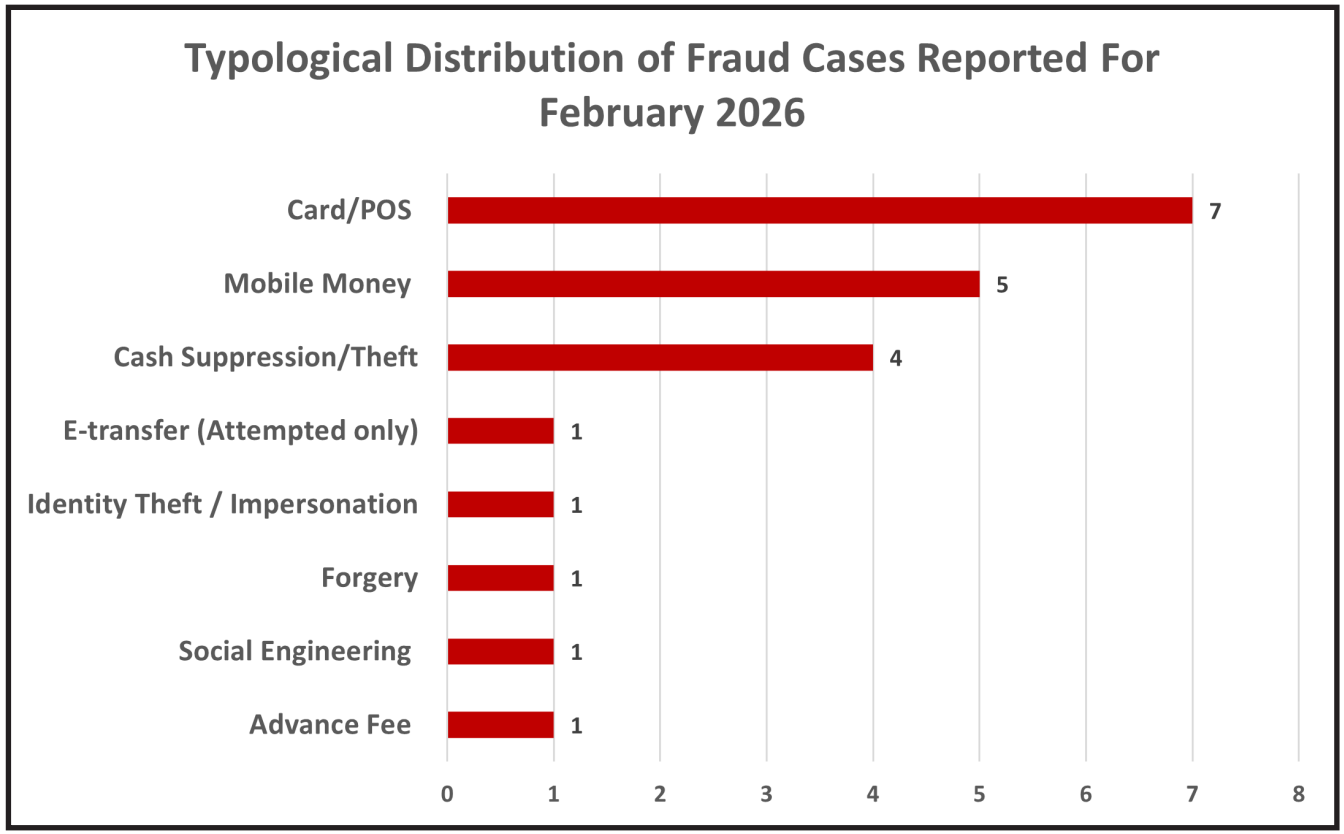
Third, the persistence of cards and mobile money fraud underscores the need for enhanced monitoring and customer engagement. Customers remain a critical line of defense, but they are also a point of vulnerability. Strengthening awareness, alongside deploying real-time detection tools, is essential to reducing exposure.

Finally, the cases highlight the importance of integrating fraud risk management across all banking functions, including credit, operations, and digital channels. Fraud is no longer isolated to specific activities; it is embedded across the entire banking value chain.

In summary, February's incidents demonstrate that while technology continues to shape the methods of fraud, the underlying drivers remain rooted in human behavior, process weaknesses, and control gaps. Addressing these effectively requires not only technological solutions but also strong governance, vigilant oversight, and a culture of accountability across the institution.

TYPOLOGICAL DISTRIBUTION AND LOSS ANALYSIS FOR FEBRUARY 2026

The February fraud data presents a marked escalation in both scale and concentration of losses, with total attempted fraud rising to GHS 5.83 million, more than double January's level. Unlike January, where losses were heavily skewed toward digital channels, February is characterized by significant internal and process-driven fraud, alongside continued exposure to card-related risks. From a case distribution standpoint, Card/POS fraud is the most frequent typology, accounting for 7 out of 21 cases (≈33%), followed by Cash Suppression/Theft (4 cases) and Mobile Money (5 cases). The remaining categories; Advance Fee, Social Engineering, Forgery, Identity Theft/ Impersonation, and E-transfer, each appear as single incidents. This indicates that while fraud remains diversified, operational and card-related fraud dominate day-to-day activity.



However, the financial impact tells a very different story. Cash Suppression/Theft emerges as the most significant contributor to losses, with GHS 2.49 million attempted and GHS 2.29 million in net losses, accounting for approximately 46% of total losses. Despite some recovery (GHS 201,575), the scale of loss highlights the severity of internal fraud risk, particularly where schemes are sustained over time or involve large-value transactions. This reinforces the earlier narrative that insider-related fraud can be both high-value and difficult to detect early.

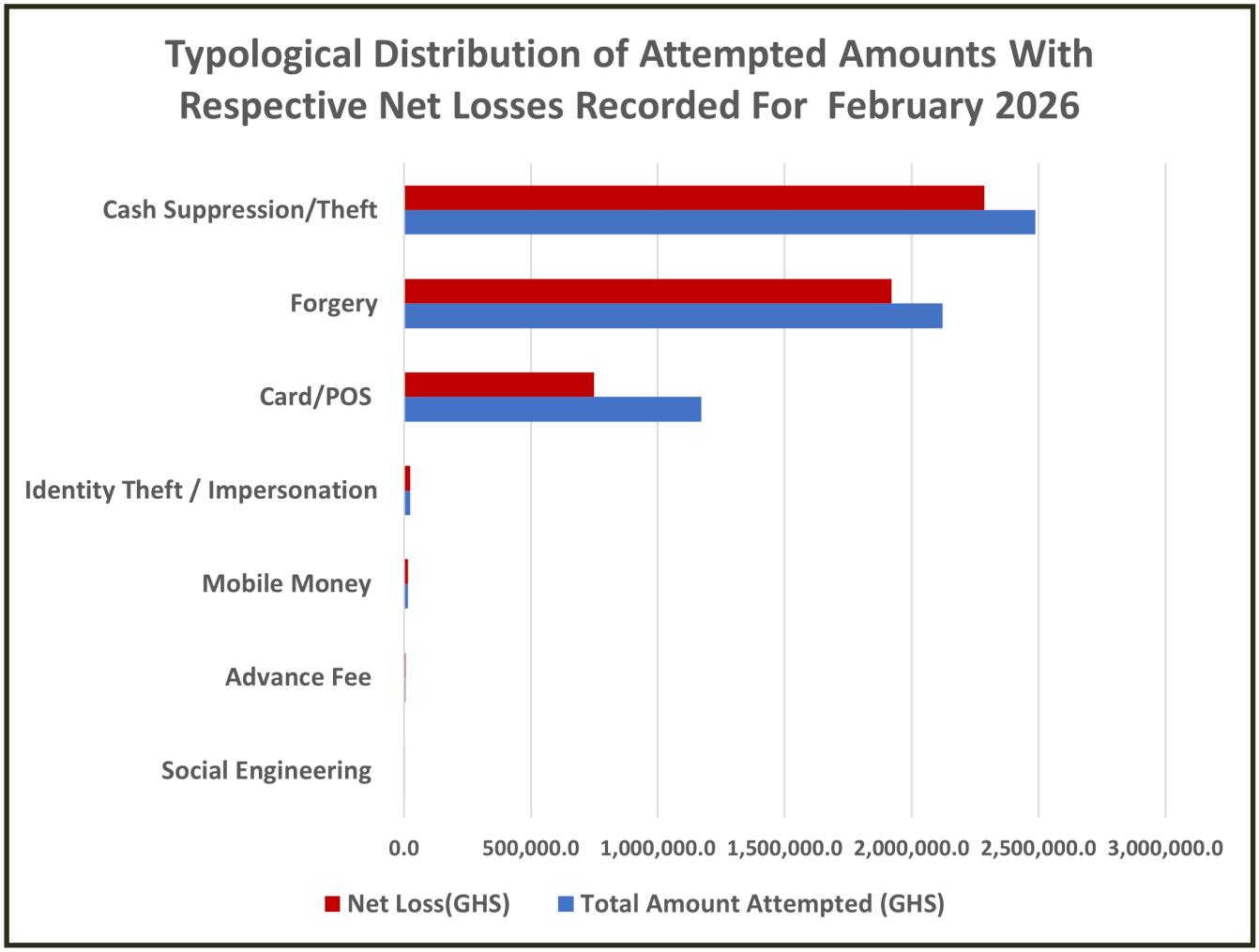
Closely following is Forgery, which, despite being a single case, resulted in GHS 2.12 million attempted and GHS 1.92 million in losses. This is particularly significant because it shows how weaknesses in documentation, collateral verification, and due diligence processes can create systemic financial exposure. Together, Cash Suppression/Theft and Forgery alone account for over 80% of total losses, clearly indicating that February's risk profile is dominated by internal control failures and process vulnerabilities rather than retail fraud.

Card/POS fraud, while the most frequent category, also contributed substantially to losses, with GHS 1.17 million attempted and GHS 748,519.88 in net losses. However, unlike January, there was significant recovery (GHS 422,765.48), suggesting improved response mechanisms such as chargebacks or transaction blocking. Even so, Card/POS fraud remains a major financial risk, combining both

frequency and relatively high loss severity.

At the lower end of the spectrum, Mobile Money fraud accounted for 5 cases but only GHS16,225 [LS2.1]in losses, reinforcing its position as a high-frequency but low-value risk category. Similarly, Social Engineering (GHS 4,536) and Advance Fee fraud (GHS 6,069) contributed marginally to total losses, though they remain important from a customer protection and reputational risk perspective.

A notable inclusion is Identity Theft/Impersonation, which resulted in GHS 24,433 in losses from a single case. While not large in value relative to other categories, it highlights the continued vulnerability of identity verification processes, particularly in account closures and withdrawals.
Interestingly, E-transfer fraud recorded no financial loss, indicating that either the attempted fraud was unsuccessful or effectively mitigated. This suggests that controls around this channel may have improved, or that detection mechanisms were effective in preventing execution.



MARCH 2026 FRAUD NARRATIVE : MODUS OPERANDI AND STRATEGIC INSIGHTS

The fraud incidents recorded in March 2026 reflect an environment where both sophistication and scale increased, with fraudsters combining technical manipulation, insider access, and social engineering to execute high-impact schemes. Compared to previous months, March stands out not just for the diversity of cases, but for the magnitude of exposure and the deliberate exploitation of systemic control weaknesses.

The month opened with a classic but increasingly common tactic, attempted business email compromise. A fraudulent instruction, disguised as a legitimate request from a corporate client, was sent to initiate a high-value transfer. On the surface, the request appeared routine; however, closer scrutiny revealed that the email address had been spoofed. A simple but critical verification step, i.e. calling the client directly, exposed the deception and prevented what would have been a significant loss. This case reinforces a key reality: fraudsters are investing in impersonation techniques that rely on operational complacency rather than system breaches, and strong verification culture remains one of the most effective defenses.

Shortly after, a series of incidents highlighted the continued exploitation of customer accounts through unauthorized digital access. In one case, a customer noticed multiple debits after performing a routine withdrawal, indicating that access to the account had already been compromised prior to the transaction. In another, a much larger incident unfolded where an attacker gained control of a customer's email account, intercepted authentication credentials, and used this access to reset internet banking details. With full control established, the fraudster executed multiple transfers across mobile wallets and other channels. The sequence was methodical in terms of compromise, credential reset, access, and rapid fund movement, demonstrating a clear understanding of digital banking workflows and authentication dependencies.

Mobile money fraud continued to feature prominently, but with a notable shift in approach. In one striking case, a fraudster impersonated a bank staff member and contacted a branch directly, instructing a teller to process an urgent transfer. The request, delivered through what appeared to be an official communication channel, was executed without sufficient verification. Only after the transaction was completed did it become clear that the instruction was fraudulent. This incident illustrates how fraud is no longer limited to customers; bank staff themselves are increasingly being targeted through social engineering, exploiting authority, urgency, and internal communication channels.

Other mobile money cases followed more familiar patterns. Customers reported unauthorized transfers from accounts linked to their wallets, often after being deceived into disclosing PINs or interacting with fraudulent online platforms. In each instance, funds were quickly routed through mobile wallets, reinforcing the persistent challenge of speed and dispersion in mobile money ecosystems, which continues to hinder recovery efforts.

Internal and operational fraud also featured significantly during the month, particularly in cases involving cash handling and custodial responsibilities. In one incident, funds collected from a customer were partially lost in transit, raising questions around custody and control during physical cash movements. In another, a far more serious breach occurred where a staff member responsible for collateral administration allegedly diverted funds running into millions that were meant for perfecting collateral for credit facilities. This was not an opportunistic act but a systematic abuse of role and access, carried out over time and only uncovered through internal audit processes. The scale of the exposure highlights how critical functions within the credit lifecycle can become high-risk points if oversight is insufficient.

Forgery-related incidents also emerged, though on a smaller scale. Individuals manipulated receipts or inflated payment values in institutional settings such as hospitals, taking advantage of trust placed in intermediaries handling payments. While the amounts involved were relatively modest, the cases demonstrate how basic document manipulation

remains a viable fraud method in less controlled environments.

Card-related fraud remained consistent with previous trends but appeared more widespread in March. Multiple cases involved unauthorized transactions across international merchants, often in card-not-present scenarios. Customers denied authorizing these transactions, suggesting that card details had been compromised and later used for online purchases. In each case, the response involved blocking cards and initiating chargebacks, but the pattern underscores the continued vulnerability of card systems in digital commerce environments, particularly where authentication can be bypassed or manipulated.

A particularly significant case during the month involved unauthorized transfers on a very large scale, driven by insider access and weak system controls. The perpetrator, entrusted with access to a corporate payment platform, exploited shared credentials and the absence of robust authentication mechanisms to insert fraudulent transactions alongside legitimate ones. By embedding unauthorized transfers within normal transaction flows and manipulating supporting records, the fraud went undetected for a prolonged period. Funds were diverted into various personal and affiliated accounts and used for personal investments and expenditures. This case is especially critical because it highlights how privileged access, when combined with weak segregation of duties and inadequate monitoring, can lead to catastrophic financial exposure.

Further reinforcing the role of deception, a case of cheque fraud involved the use of a cloned cheque to withdraw a substantial amount from a customer's account. The duplication of cheque details and redirection of funds to a different bank indicate a deliberate attempt to exploit gaps in cheque verification processes.

Across the month, social engineering continued to underpin many of the fraud cases. Customers were lured into clicking links, responding to calls from individuals posing as bank or telecom staff, or disclosing sensitive credentials under false pretenses. Once again, the fraudsters did not need to breach systems directly; instead, they leveraged human trust and behavior as the primary entry point.

When these incidents are viewed collectively, several key insights emerge for banks. First, the growing prevalence of impersonation, whether targeting customers, staff, or corporate clients, demands a stronger culture of verification at all levels. No instruction, regardless of its apparent authenticity, should bypass established validation procedures.

Second, the cases highlight the urgent need to strengthen controls around digital identity and authentication. Email compromise, credential sharing, and weak PIN practices continue to provide easy entry points for fraudsters. Multi-layered authentication and tighter control over credential usage are essential.

Third, the scale of internal fraud observed in March underscores the importance of robust governance over staff access and critical processes, particularly in areas such as credit administration and corporate banking platforms. Monitoring systems must be capable of detecting anomalies even when transactions appear legitimate on the surface.

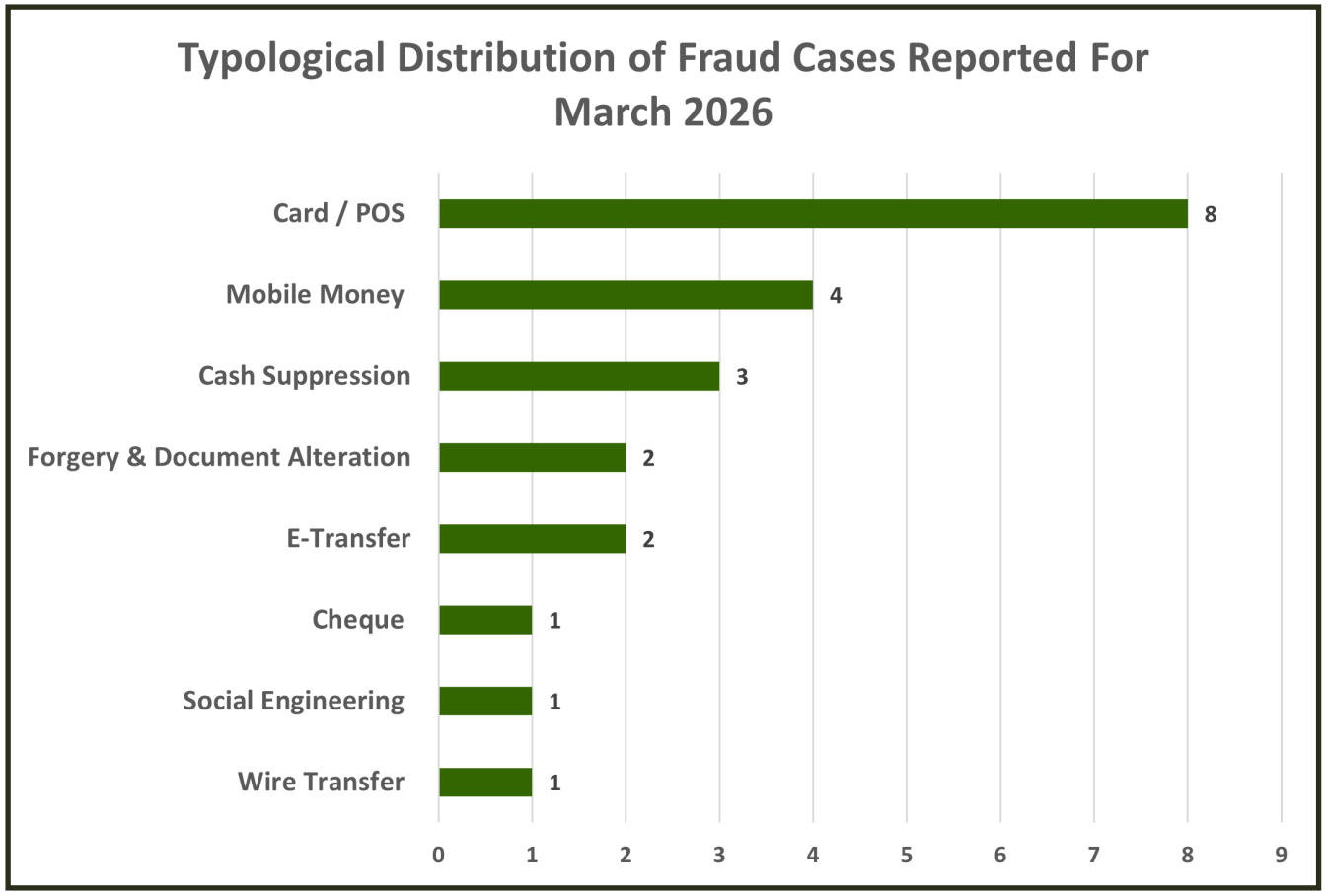
Fourth, the persistence of mobile money and card fraud reinforces the need for real-time monitoring and rapid response mechanisms, given how quickly funds can be moved and dissipated once access is gained.

Ultimately, March 2026 illustrates a fraud environment where the boundaries between external and internal threats are increasingly blurred, and where attackers combine technical knowledge, psychological manipulation, and process exploitation to achieve their objectives. For banks, responding effectively will require not only technological investment but also a deep integration of controls, awareness, and accountability across the entire operational framework.

TYPOLOGICAL DISTRIBUTION AND LOSS ANALYSIS FOR MARCH 2026

The March fraud data reflects a highly concentrated risk structure, where a few typologies drive the majority of financial exposure, despite a relatively moderate number of cases (22 cases). The total attempted fraud stands at GHS 5.35 million, with recoveries of only GHS 56,829.80, resulting in a net loss of GHS 3.30 million. This indicates a very low recovery rate (1.6%), the weakest across the three months, underscoring the increasing difficulty in reversing fraud once executed.

From a case distribution perspective, Card / POS fraud is the most frequent typology, accounting for 8 out of 22 cases (36%), followed by Mobile Money fraud (4 cases) and Cash Suppression (3 cases). The remaining categories including E-Transfer, Forgery & Document Alteration, Social Engineering, Cheque Fraud, and Wire Transfer Fraud which occur as isolated / low-frequency incidents. This again reflects a broad spread of typologies, but with concentration in a few dominant channels.



However, as seen in previous months, frequency does not translate to financial impact. The most significant driver of losses in March is Cash Suppression, with GHS 2.74 million attempted and GHS 2.69 million in net losses, accounting for approximately 81% of total losses. Despite minimal recovery (GHS 56,829.80), the magnitude of loss confirms that internal fraud remains the most financially destructive risk category, particularly when it involves prolonged activity or abuse of custodial responsibilities.

In contrast, Card / POS fraud, while the most frequent, contributed only GHS 58,031.28 in losses, a sharp decline in financial impact compared to February. This suggests that although card fraud remains operationally significant, its severity has reduced, possibly due to improved controls, lower transaction values, or quicker detection.

E-Transfer fraud recorded GHS 261,401.50 in losses across just 2 cases, making it the second-largest contributor to total losses. This highlights the continued vulnerability of digital transfer channels, particularly where account access is compromised

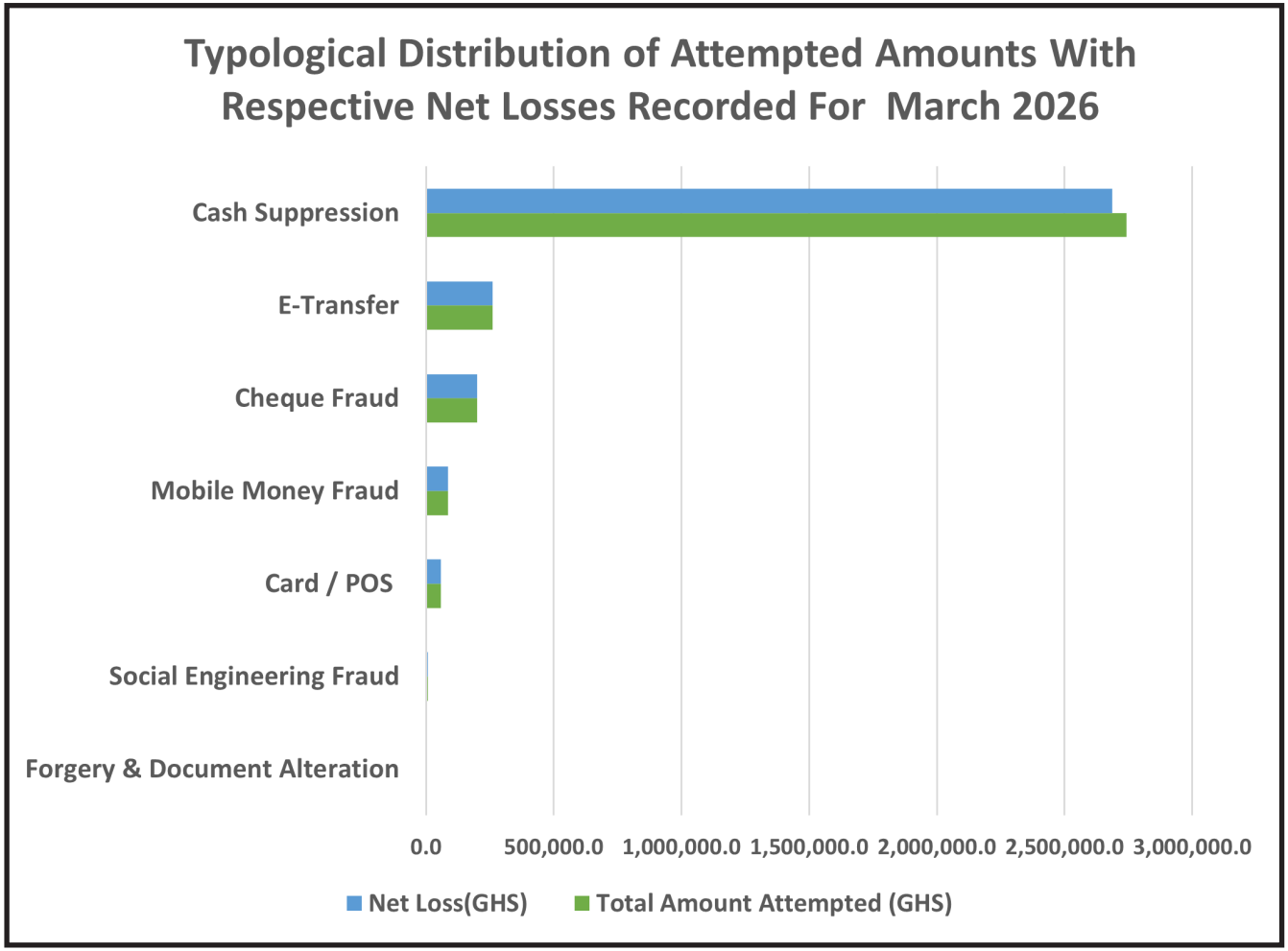
and funds can be moved rapidly with little chance of recovery.

Similarly, one single cheque Fraud, resulted in a substantial GHS 200,000 loss, reinforcing that traditional instruments remain relevant risk channels, especially where verification processes are weak or can be bypassed.

Mobile Money fraud, with 4 cases and GHS 85,750 in losses, continues to follow the familiar pattern of moderate frequency and moderate value, driven largely by social engineering and unauthorized wallet transactions. While not as severe as internal fraud, its persistence highlights ongoing exposure within the retail segment.

At the lower end, Social Engineering Fraud (GHS 7,776.84) and Forgery & Document Alteration (GHS 1,265) contributed minimally to total losses, though they remain important indicators of underlying behavioral and process vulnerabilities.

A notable category is Wire Transfer Fraud (Attempted), involving a GHS 1.99 million attempted transaction that was successfully prevented, resulting in zero loss. This is a critical positive signal, demonstrating that effective verification controls, particularly call-back procedures, can completely eliminate high-value fraud risk when properly applied.



CONSOLIDATED KEY INSIGHTS: JANUARY TO MARCH

Throughout the three months, the fraud cases collectively reveal a clear structural shift in how fraud is executed within the banking ecosystem. The patterns are not isolated; they reinforce each other and point to systemic vulnerabilities that require coordinated responses. The insights below synthesize the core lessons emerging from all incidents.

The most dominant insight is that fraud is now primarily human-driven rather than system-driven. In the vast majority of cases, fraudsters did not hack banking systems; instead, they manipulated customers, staff, or trusted relationships. Whether through phishing emails, deceptive phone calls, fake online platforms, or impersonation of bank officials, the entry point was consistently human trust and behavioral gaps. This means that even the most advanced systems can be undermined if users, both customers and employees, are not adequately protected or informed.

Closely linked to this is the increasing role of social engineering as the central fraud technique. Across all months, fraudsters relied heavily on persuasion, urgency, and deception to obtain sensitive credentials such as PINs, passwords, and OTPs. In several cases, customers willingly disclosed information under false pretenses, enabling fraudsters to execute transactions seamlessly. This indicates that fraud prevention must move beyond technical controls to include continuous behavioral and awareness interventions.

Another critical insight is the risk introduced by bank–mobile money integration. Many fraud cases were successfully executed because bank accounts were linked to mobile wallets, sometimes without the customer's full awareness. Once access was gained, funds were quickly transferred into mobile wallets and dispersed across multiple accounts. The speed and fragmentation of these transactions significantly reduced recovery chances. This highlights that financial integration, while improving convenience, has also expanded the attack surface and accelerated fraud execution cycles.

The data also reveals a growing trend of impersonation targeting not just customers, but bank staff and corporate clients. Fraudsters posed as bank officials, internal staff, or legitimate business clients to initiate transactions. In some cases, even frontline bank employees were deceived into processing fraudulent transfers. This demonstrates that fraud is increasingly penetrating internal communication channels, making it imperative for banks to enforce strict verification protocols regardless of the perceived source of a request.

A particularly concerning pattern is the rise in insider-related fraud and abuse of privileged access. Several high-value cases involved staff manipulating transactions, diverting funds, or exploiting their roles within the system. In more sophisticated instances, insiders embedded fraudulent transactions within legitimate workflows to avoid detection. This confirms that internal threats remain as significant as external ones, especially when combined with weak supervision, poor segregation of duties, and inadequate monitoring systems.

In addition, the cases expose weaknesses in authentication and credential management systems. Fraudsters were able to exploit weak PINs, shared credentials, intercepted OTPs, and compromised email accounts to gain unauthorized access. In some instances, the absence of robust secondary authentication or control mechanisms enabled large-scale fraud to occur undetected. This underscores the need for strong, multi-layered authentication frameworks that go beyond basic credential checks.

The persistence of card fraud, particularly in card-not-present environments, highlights ongoing vulnerabilities in digital payment systems. Compromised card details were used across multiple online platforms, often internationally, before detection occurred. Even where authentication measures like OTPs existed, they were sometimes bypassed or manipulated. This suggests that card security must evolve alongside the growth of e-commerce and digital payments.

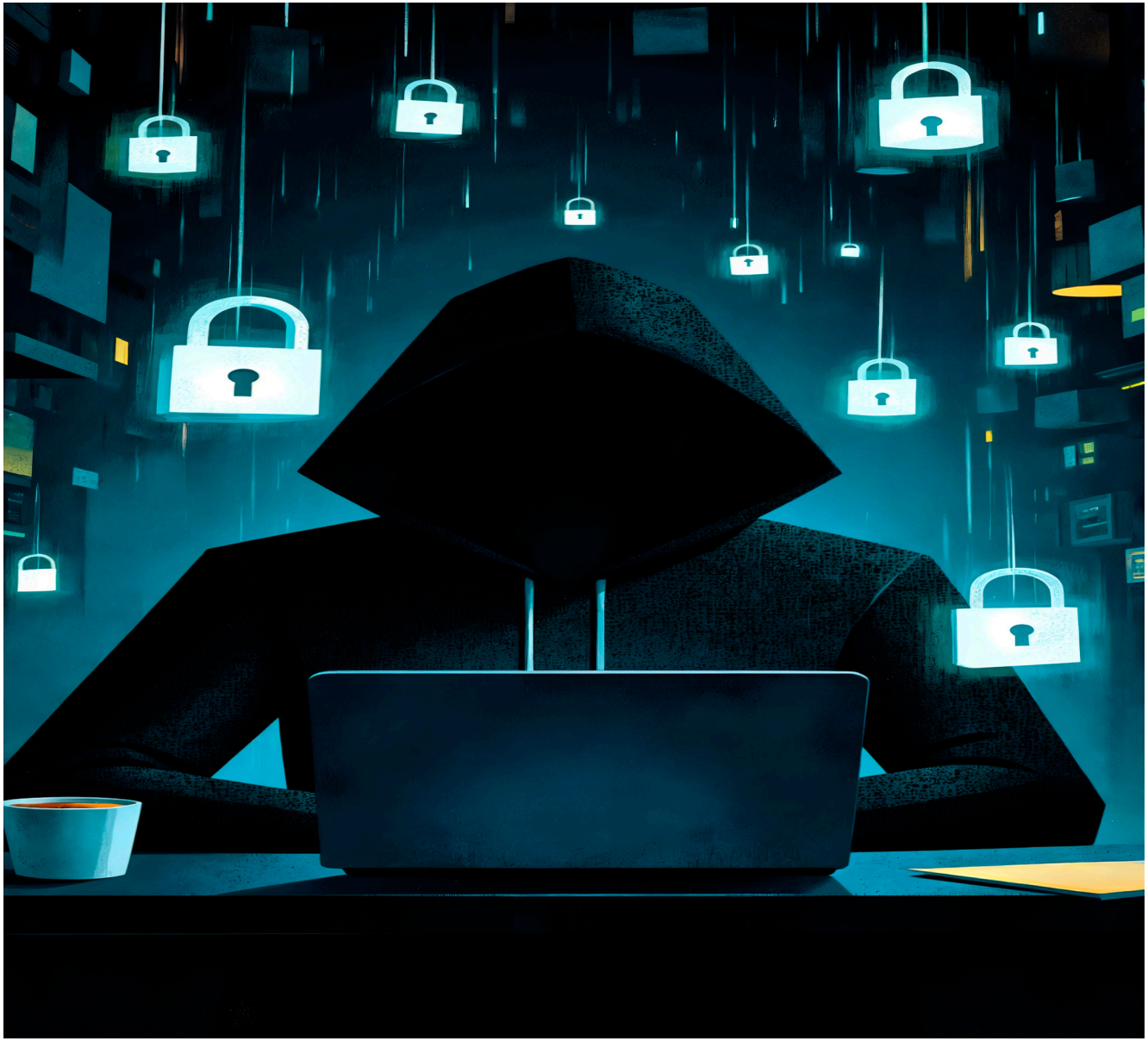
Another key insight is the speed of fraud execution versus the lag in detection and response. In many cases, once access was gained, fraudsters executed multiple transactions within minutes or hours, rapidly moving funds across accounts and

CONSOLIDATED KEY INSIGHTS: JANUARY TO MARCH (CONT...)

platforms. By the time the fraud was identified, the funds had already been dissipated. This indicates that traditional, reactive approaches to fraud management are no longer sufficient; real-time monitoring and intervention are now essential.

The cases also highlight vulnerabilities within core banking processes such as credit administration and collateral management. Fraudulent documentation, fake collateral, and inadequate verification processes led to significant financial exposures. These were not technical breaches but failures in due diligence, validation, and cross-functional coordination. This demonstrates that fraud risk extends beyond transactions into strategic banking functions like lending and asset management.

Finally, there is a recurring theme of weak verification culture across both customers and staff. In several instances, fraud could have been prevented through simple checks—confirming a transaction request, verifying a source, or questioning unusual instructions. Where such verification was performed, fraud attempts failed; where it was bypassed, losses occurred. This reinforces that a strong culture of skepticism and verification is one of the most effective defenses against fraud.



CONSOLIDATED TYPOLOGICAL DISTRIBUTION AND LOSS ANALYSIS: JANUARY TO MARCH 2026

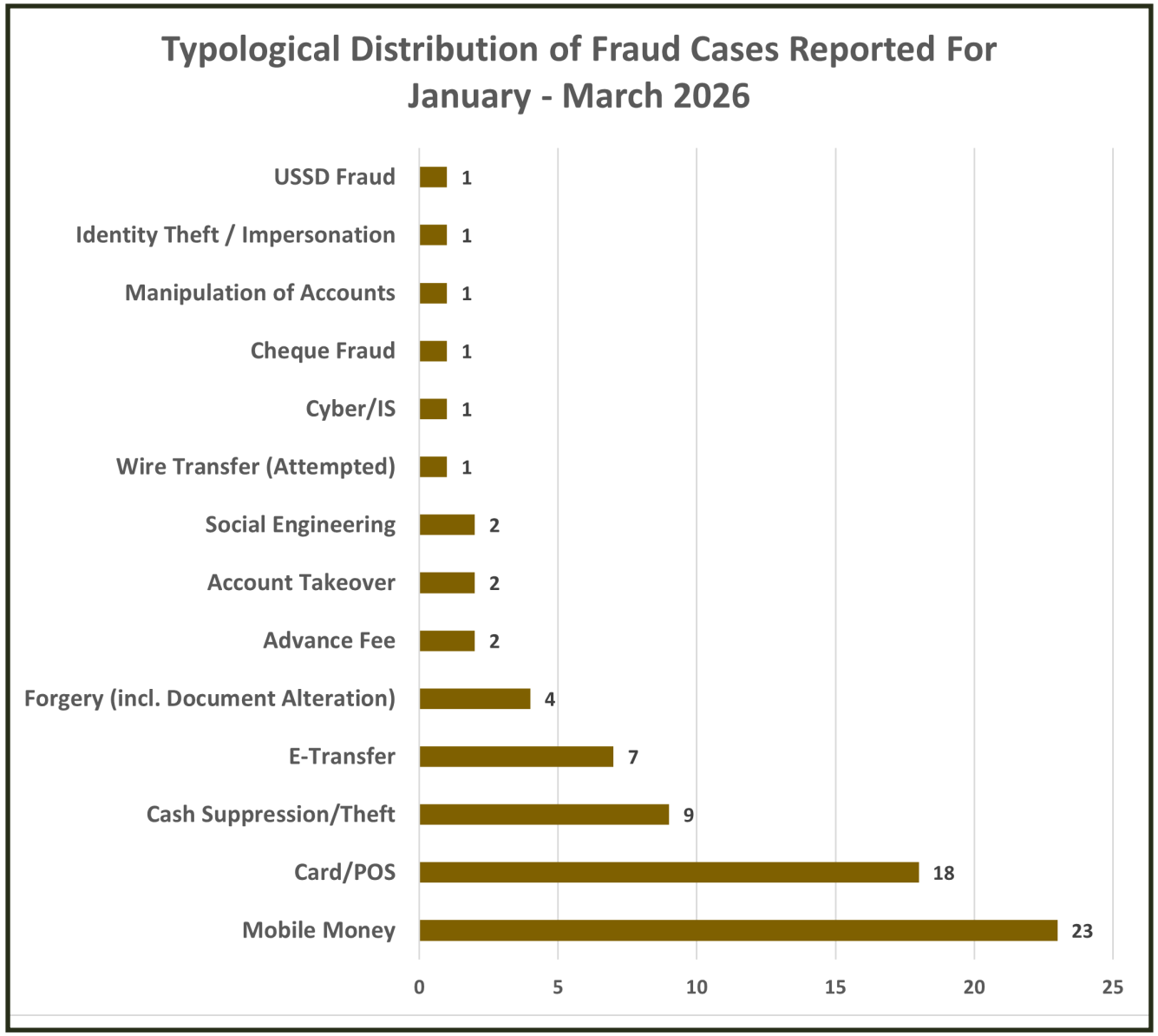
The consolidated data for January to March 2026 provides a clear and structured view of fraud risk across the institution, covering 73 cases, GHS 14.05 million in attempted fraud, GHS 1.01 million recovered, and a net loss of GHS 11.05 million. This translates into an overall recovery rate of just about 7.2%, reinforcing a consistent theme across the months: once fraud is executed, recovery is generally limited.

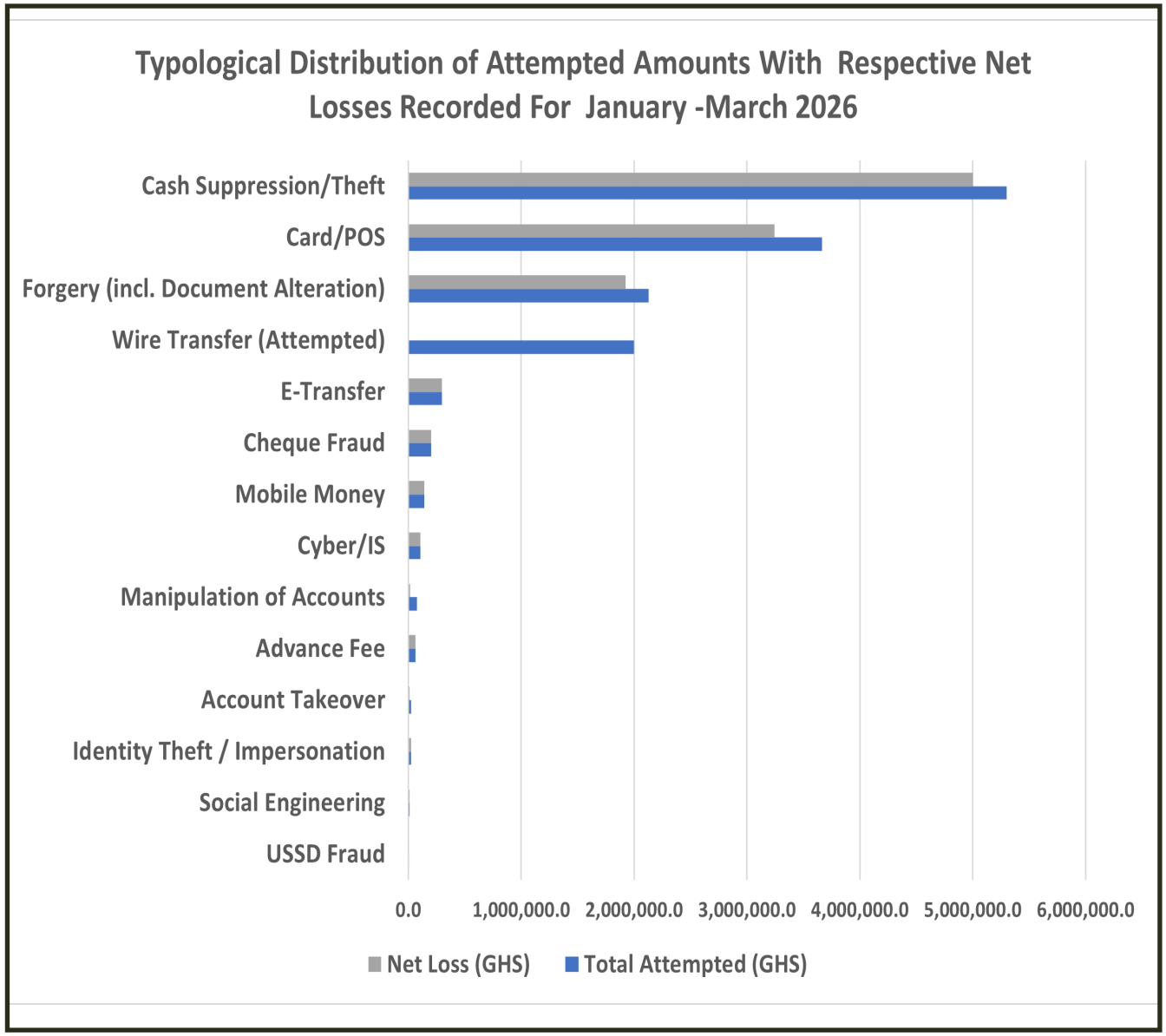
At a high level, the data reveals a three-tier fraud structure that is defined by volume, value, and severity, which is critical for policy and resource allocation.

The first layer is high-frequency, low-to-moderate value fraud, dominated by Mobile Money and Card/POS fraud.

Mobile Money fraud accounts for the highest number of cases (23 cases, 31.5%), making it the most operationally significant category. However, its financial impact is relatively low, with GHS 143,108 attempted and GHS 142,038 in net losses. This confirms that Mobile Money fraud is largely volume-driven, arising from social engineering, wallet compromises, and linkage vulnerabilities. While individual cases are small, the cumulative effect and the operational burden which is also substantial.

Card/POS fraud, on the other hand, represents a hybrid risk. It is has high frequency (18 cases, 24.7%) and extremely high in value, with GHS 3.67 million





attempted and GHS 3.24 million in net losses. Despite some recovery (GHS 422,765.48), it remains one of the most financially damaging categories. This positions Card/POS fraud as a critical risk area, particularly in card-not-present environments and digital commerce, where fraudsters can scale transactions quickly.

The second layer is low-frequency but high-impact fraud, which is the primary driver of financial losses. Cash Suppression/Theft stands out as the single largest contributor to losses, with GHS 5.30 million attempted and GHS 5.00 million in net losses, despite representing only 9 cases (12.3%). This clearly establishes internal fraud as the most severe financial risk, driven by staff misconduct, weak supervision, and process lapses in cash handling and custodial roles.

Closely following is Forgery (including document alteration), with GHS 2.13 million attempted and GHS 1.92 million in losses from just 4 cases. This highlights deep vulnerabilities in documentation, collateral verification, and due diligence processes, particularly within credit and transactional validation systems.

E-Transfer fraud, while moderate in frequency (7 cases, 9.6%), resulted in GHS 297,091.84 in total losses with zero recovery, indicating that once funds are transferred through digital channels, recovery is almost impossible. This reinforces the need for stronger front-end controls.

Similarly, Cheque Fraud (GHS 200,000 loss) and Cyber/IS fraud (GHS 105,000 loss), though isolated cases, demonstrate that traditional instruments and cyber-enabled attacks remain relevant and potentially high-impact.

The third layer consists of emerging and niche fraud typologies, which individually contribute less but collectively highlight evolving risks.

Categories such as Advance Fee (GHS 65,181 loss), Social Engineering (GHS 12,312.84 loss), Identity Theft/Impersonation (GHS 24,433 loss), and USSD Fraud (GHS 7,019.50 loss) are relatively small in financial terms but are critical precursors and enablers of larger fraud schemes. They often represent the entry points through which fraudsters gain access to accounts or systems.

Notably, Account Takeover and Manipulation of Accounts show partial recoveries (GHS 15,000 and GHS 62,700 respectively), suggesting that fraud involving identifiable actors or internal linkages offers better recovery prospects compared to anonymous digital fraud.

A particularly important highlight is Wire Transfer Fraud (Attempted), involving GHS 1.99 million, which resulted in zero loss. This is a strong positive indicator that effective controls, especially transaction verification protocols, can completely eliminate high-value fraud risk when properly enforced.

KEY IMPLICATIONS FOR THE BANKING INDUSTRY

The Q1 2026 fraud data highlights a dual-risk structure in the banking environment: high-frequency retail fraud (Mobile Money and Card/POS) and high-impact institutional fraud (Cash Suppression, Forgery, E-Transfers, and Cyber incidents). While digital channels account for most cases, internal fraud and process weaknesses generate the largest financial losses, underscoring that governance and operational discipline remain as important as technological controls.

A second key implication is the very low recovery rate across most fraud types, especially those involving fast digital transfers and wallet ecosystems. Once funds are dispersed across multiple channels, recovery becomes difficult, reinforcing that prevention is significantly more effective than post-fraud remediation.

In addition, the data reveals a growing interconnected fraud ecosystem across banks, telecoms, and fintech platforms, where delays in detection and response amplify losses. This makes coordination and timely intelligence sharing critical to limiting systemic exposure.

STRATEGIC RECOMMENDATIONS FOR THE BANKING INDUSTRY

1. Strengthen internal controls and staff oversight:

Reinforce segregation of duties, supervisory checks, and audit trails, particularly in cash handling, collateral management, and transaction approvals.

2. Enhance digital security and authentication protocols

Implement stronger multi-factor authentication, transaction verification steps, and real-time alerts for high-risk channels such as E-Transfer, USSD, and Card-not-present transactions.

3. Tighten Mobile Money integration controls

Ensure explicit customer consent for wallet linkage, introduce periodic re-confirmation of linked accounts, and apply stricter transaction limits on bank-wallet transfers.

4. Improve real-time fraud detection systems

Deploy advanced analytics and anomaly detection tools to identify unusual transaction patterns early, especially in digital and cross-channel transfers.

5. Strengthen inter-bank and industry-wide information sharing

Establish faster and more structured communication channels among banks, Telcos, and regulators to enable early warning alerts, rapid account flagging, and coordinated response to emerging fraud patterns.

6. Intensify internal and customer education programs

Scale continuous training for staff on emerging fraud typologies while also educating customers on social engineering, phishing, and credential protection risks.

7. Adopt a risk-based fraud management approach

Prioritise resources based on both financial exposure and recovery likelihood, with greater focus on high-loss areas such as internal fraud, E-Transfers, and Card/POS fraud.

CONCLUSION

The analysis of fraud cases reported by member banks of the Ghana Association of Banks for the period January to March 2026 highlights an evolving and increasingly complex fraud landscape within the banking industry. The data shows that fraud is no longer concentrated within a single channel or typology but is now spread across digital platforms, internal processes, and hybrid ecosystems involving banks, mobile money operators, and fintech services. While Mobile Money and Card/POS fraud dominate in terms of frequency and operational exposure, the most significant financial losses continue to arise from Cash Suppression, Forgery, E-Transfers, and other process-driven vulnerabilities, particularly those linked to internal control weaknesses. A recurring concern is the low recovery rate across most typologies, especially where funds are rapidly transferred across multiple digital channels, reinforcing the need for stronger preventive controls rather than reliance on post-incident recovery.

A key insight from the review is that effective fraud detection and response depend not only on individual institutional controls but also on the speed and quality of information sharing across the industry. Many fraud patterns observed are cross-cutting in nature, indicating that delays in communication between institutions and ecosystem partners significantly increase overall exposure.

The structured presentation of fraud modus operandi in this report is intended to provide practical guidance to risk managers and fraud control teams across the banking sector. It is expected to support improved detection capabilities, strengthen preventive frameworks, and enhance coordinated responses to emerging threats.

In line with its mandate, the Ghana Association of Banks will continue to strengthen its efforts to safeguard the integrity and stability of the banking industry. This will be achieved through enhanced industry-wide information sharing, continuous stakeholder education, and deeper collaboration among banks and relevant financial ecosystem partners.

These efforts will also be complemented by ongoing preparations for a national fraud awareness campaign, aimed at improving both customer and staff awareness of evolving fraud risks. Ultimately, sustained collaboration and timely intelligence exchange remain central to building a more resilient, secure, and trusted banking environment in Ghana.

APPENDIX

JANUARY 2026

Banking Industry Fraud Returns | Values in Ghana Cedis (GHS)

Total Cases	Total Attempted	Total Recovered	Net Loss
30	GHS 2,864,671.91	GHS 124,970.00	GHS 2,739,701.91

Fraud Typology	No. of Cases	Amount Attempted (GHS)	Amount Recovered (GHS)	Net Loss (GHS)
Mobile Money	14	41,133.00	1,070.00	40,063.00
E-Transfer	4	35,690.34	0.00	35,690.34
Card/POS	3	2,437,532.07	0.00	2,437,532.07
Account Takeover	2	25,885.00	15,000.00	10,885.00
Cash Suppression	2	68,300.00	39,000.00	29,300.00
Forgery	1	7,200.00	7,200.00	0.00
USSD Fraud	1	7,019.50	0.00	7,019.50
Advance Fee	1	59,112.00	0.00	59,112.00
Cyber/IS	1	105,000.00	0.00	105,000.00
Manipulation of Accounts	1	77,800.00	62,700.00	15,100.00
Total	30	2,864,671.91	124,970.00	2,739,701.91

FEBRUARY 2026

Banking Industry Fraud Returns | Values in Ghana Cedis (GHS)

Total Cases	Total Attempted	Total Recovered	Net Loss
21	GHS 5,833,010.90	GHS 824,340.48	GHS 5,008,670.42

Fraud Typology	No. of Cases	Amount Attempted (GHS)	Amount Recovered (GHS)	Net Loss (GHS)
Cash Suppression/Theft	4	2,488,526.00	201,575.00	2,286,951.00
Card/POS	7	1,171,285.36	422,765.48	748,519.88
Advance Fee	1	6,069.00	0.00	6,069.00
Social Engineering	1	4,536.00	0.00	4,536.00
Forgery	1	2,121,936.54	200,000.00	1,921,936.54
Identity Theft / Impersonation	1	24,433.00	0.00	24,433.00
Mobile Money	5	16,225.00	0.00	16,225.00
E-transfer	1	0.00	0.00	0.00
Total	21	5,833,010.90	824,340.48	5,008,670.42

MARCH 2026

Banking Industry Fraud Returns | Values in Ghana Cedis (GHS)

Total Cases	Total Attempted	Total Recovered	Net Loss
22	GHS 5,354,430.65	GHS 56,829.80	GHS 3,300,400.85

Fraud Typology	No. of Cases	Amount Attempted (GHS)	Amount Recovered (GHS)	Net Loss (GHS)
Wire Transfer Fraud (Attempted)	1	1,997,200.00	0.00	0.00
E-Transfer	2	261,401.50	0.00	261,401.50
Mobile Money Fraud	4	85,750.00	0.00	85,750.00
Cash Suppression	3	2,743,006.03	56,829.80	2,686,176.23
Card / POS	8	58,031.28	0.00	58,031.28
Forgery & Document Alteration	2	1,265.00	0.00	1,265.00
Social Engineering Fraud	1	7,776.84	0.00	7,776.84
Cheque Fraud	1	200,000.00	0.00	200,000.00
Total	22	5,354,430.65	56,829.80	3,300,400.85

CONSOLIDATED: JANUARY – MARCH 2026

Banking Industry Fraud Returns | Values in Ghana Cedis (GHS)

Total Cases	Total Attempted	Total Recovered	Net Loss
73	GHS 14,052,113.46	GHS 1,006,140.28	GHS 11,048,773.18

Fraud Typology	No. of Cases	Amount Attempted (GHS)	Amount Recovered (GHS)	Net Loss (GHS)
Mobile Money	23	143,108.00	1,070.00	142,038.00
Card/POS	18	3,666,848.71	422,765.48	3,244,083.23
Cash Suppression/Theft	9	5,299,832.03	297,404.80	5,002,427.23
E-Transfer	7	297,091.84	0.00	297,091.84
Forgery (incl. Document Alteration)	4	2,130,401.54	207,200.00	1,923,201.54
Advance Fee	2	65,181.00	0.00	65,181.00
Account Takeover	2	25,885.00	15,000.00	10,885.00
Social Engineering	2	12,312.84	0.00	12,312.84
Wire Transfer (Attempted)	1	1,997,200.00	0.00	0.00*
Cyber/IS	1	105,000.00	0.00	105,000.00
Cheque Fraud	1	200,000.00	0.00	200,000.00
Manipulation of Accounts	1	77,800.00	62,700.00	15,100.00
Identity Theft / Impersonation	1	24,433.00	0.00	24,433.00
USSD Fraud	1	7,019.50	0.00	7,019.50
Total	**73**	**14,052,113.46**	**1,006,140.28**	**11,048,773.18**

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