GAB
GHANA ASSOCIATION OF BANKS

INDUSTRY FRAUD REPORT

APRIL - JUNE 2026

EXECUTIVE SUMMARY

This report presents a consolidated analysis of fraud incidents reported by member banks of the Ghana Association of Banks for the period April to June 2026. The analysis covers 287 reported cases, with total exposure amounting to GH¢18,972,660.15 during the quarter.

Overall, attempted fraud incidents recorded a success rate of over 98 percent. The findings also suggest that fraud is being executed with increasing speed, reducing the window available for banks to intercept transactions and recover funds.

Of the total exposure, only GH¢323,350.13 was recovered, representing approximately 1.7 percent. This resulted in an estimated net loss of GH¢18,622,419.19, equivalent to about 98.2 percent of total exposure

The figures do not necessarily represent a complete industry aggregate. They reflect only the incidents contained in the submissions received by GAB and may change as investigations progress and additional recoveries are made. The report should therefore be read as an indicative operational assessment of the reported fraud environment, rather than a full census of every fraud event in the banking industry.

The analysis reveals a clear dual-risk structure. Card/POS Fraud was the most frequent typology, recording 131 cases and representing 45.6% of all incidents. However, a single credit/application fraud produced the highest financial impact, a net loss of GHS 9,530,000.00. The distinction is important: high-volume digital fraud creates a substantial operational workload, while a small number of credit, account-takeover, cheque, forgery and internal incidents can produce disproportionately large losses.

Recovery performance remained weak. Recoveries were equivalent to only 1.7% of successful fraud amounts. In many digital cases, funds were rapidly transferred into mobile wallets, mule accounts, merchant platforms or cash-out points before intervention was possible. This confirms that prevention, early detection and coordinated transaction holds are more effective than relying on recovery after funds have been dispersed.

The modus operandi was increasingly multi-channel. Common methods included deceptive food-ordering and parcel-delivery links, credential harvesting, card-not-present purchases, stolen or compromised phones, bank-to-wallet transfers, impersonation, cloned cheques, forged mandates and supporting documents, manipulation of customer accounts, cash suppression and misuse of staff access. Fraudsters frequently combined human deception with legitimate payment infrastructure, allowing them to appear as authorised customers before moving the proceeds quickly across institutions.

The cases also demonstrate that external and internal fraud cannot be managed separately. Customer credential compromise and social engineering were the main entry points in many retail cases, but some of the most severe exposures arose from weak document validation, credit processes, privileged access, maker-checker failures and insufficient monitoring of dormant, deceased-customer or operational accounts. Governance and process discipline therefore remain as important as digital-security investment.

The structured typology and modus-operandi analysis is intended to provide practical guidance to fraud-control teams, risk managers and operational leaders. It supports stronger preventive controls, improved detection rules, faster response arrangements and more targeted customer and staff education. Effective industry action will depend on timely and consistent information sharing among banks, mobile network operators, payment service providers, merchants, regulators and law-enforcement agencies.

INTRODUCTION

Fraud remains one of the most persistent and evolving operational risks facing Ghana's banking industry. It creates direct financial losses, increases the cost of investigation and customer remediation, weakens confidence in payment channels and can expose financial institutions to legal, regulatory and reputational consequences. The risk extends beyond individual transactions because repeated incidents can affect customer trust in the wider financial system.

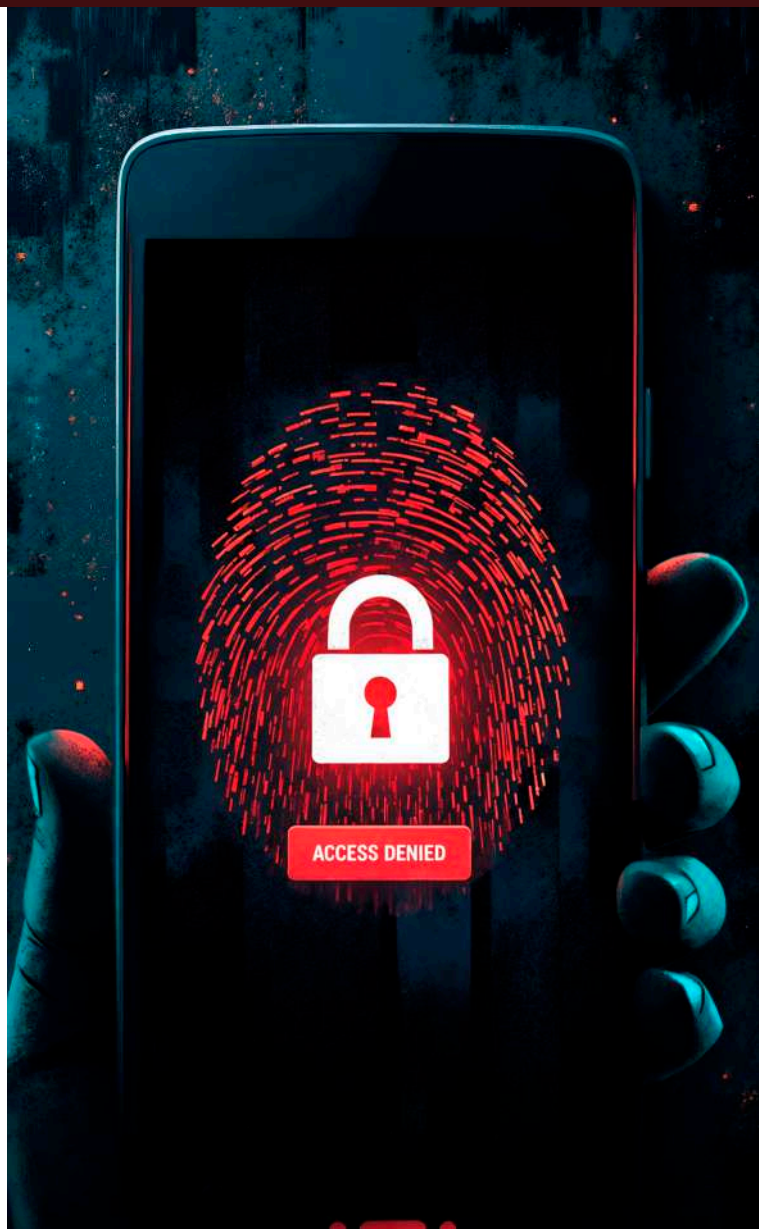
The rapid expansion of digital banking, mobile money, instant transfers, online commerce and interoperable payment services has significantly improved access, speed and convenience. At the same time, it has widened the number of channels through which fraud can be initiated and proceeds can be moved. Fraudsters increasingly exploit the connections among bank accounts, cards, mobile wallets, merchant platforms, telecommunications networks and third-party beneficiary accounts. A weakness at one point in this chain can therefore create exposure across several institutions and platforms.

The reported cases show that modern fraud does not depend only on direct attacks against banking systems. Many incidents begin with the manipulation of customers, staff or business processes. Deceptive links, impersonation, false merchant pages, compromised devices and credential harvesting are used to obtain information that allows the fraudster to appear as a legitimate customer. In other cases, forged documents, cloned cheques, weak verification procedures, excessive access rights or insider misconduct are used to bypass established controls.

This report provides a consolidated assessment of fraud incidents reported for April, May and June 2026. It examines the distribution of cases across fraud typologies, reported exposure, recoveries and estimated net losses, and distinguishes between high-frequency incidents and lower-frequency events with greater financial severity. It also analyses the principal modus operandi and the control weaknesses that enabled the reported incidents.

The objectives are threefold. First, the report provides an industry-level view of the reported fraud position during the quarter. Second, it identifies recurring tactics, transaction pathways and vulnerabilities that require operational and strategic attention. Third, it translates the evidence into practical implications for authentication, transaction monitoring, staff oversight, document validation, customer protection and cross-institutional response.

The analysis is based on the reported cases only. It should not be interpreted as a complete



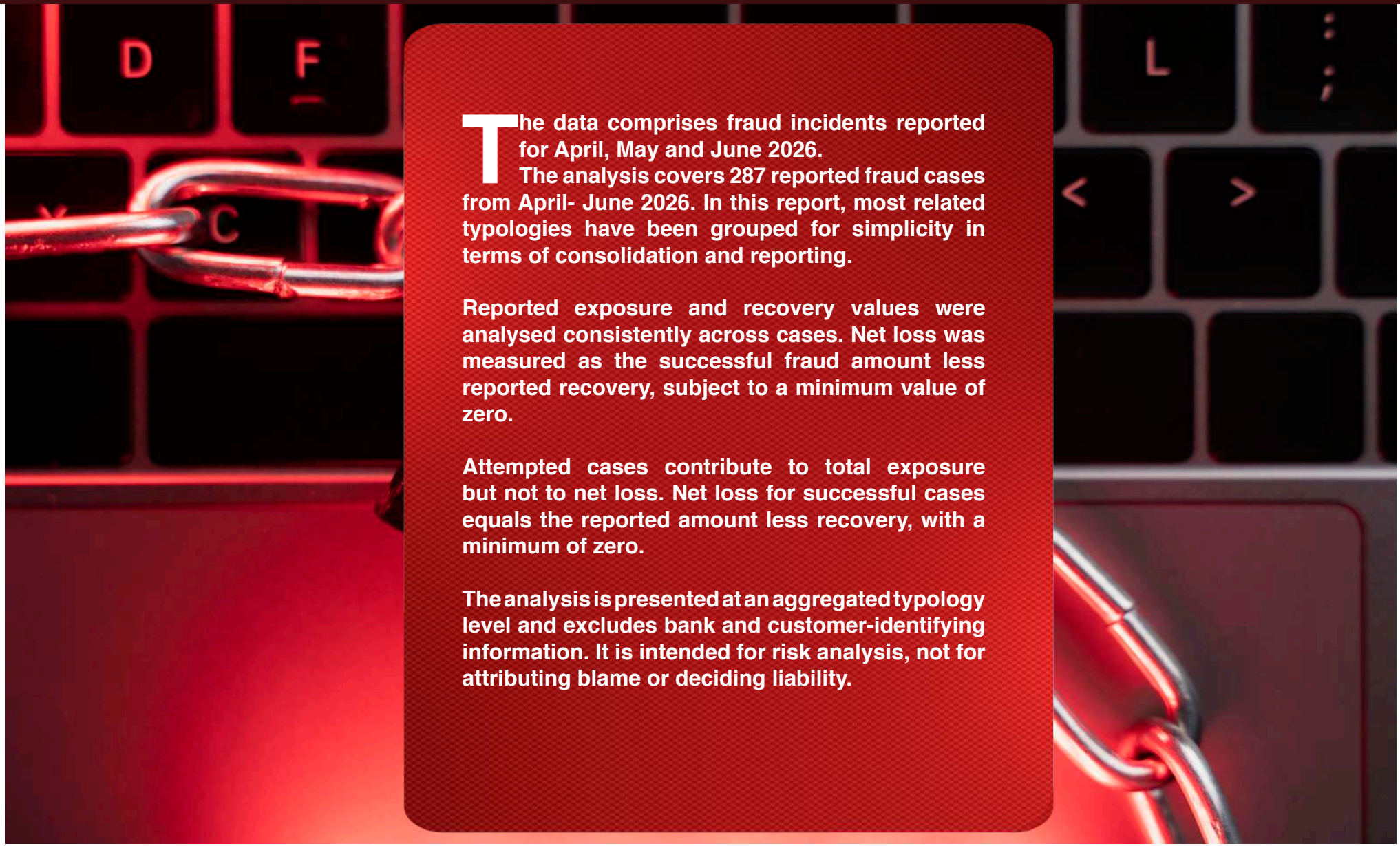
census of every fraud incident within the banking sector. Reporting coverage, classification practices, the stage of investigation and subsequent recoveries may differ across institutions and reporting periods. The findings therefore provide an indicative assessment of the reported fraud environment .

Although individual banks continue to invest in fraud-prevention systems, the cases demonstrate that institution-specific controls are not sufficient on their own. Fraud proceeds may move from an originating bank to another bank, a mobile wallet, an online merchant or a cash-out point within a short period. Effective detection and recovery therefore depend on timely information sharing, rapid beneficiary-account action and coordinated response arrangements among banks, mobile network operators, payment service providers, merchants, regulators and law-enforcement agencies.

The Ghana Association of Banks has therefore made this initiative one of it important coordinating roles in strengthening collective resilience. This includes promoting consistent fraud reporting, supporting industry intelligence exchange, encouraging common response standards and advancing customer and staff education on emerging fraud methods. These efforts complement the controls maintained by individual institutions and help reduce gaps that fraudsters may exploit across the wider financial ecosystem.

Ultimately, the report is intended to support a more proactive, risk-based and intelligence-shared approach to fraud management. By presenting both the financial impact and the operational methods behind the reported cases, it provides a basis for refining detection rules, strengthening preventive controls, targeting education and directing management attention toward the areas of greatest vulnerability.

SCOPE, METHOD AND DATA TREATMENT



The data comprises fraud incidents reported for April, May and June 2026.

The analysis covers 287 reported fraud cases from April- June 2026. In this report, most related typologies have been grouped for simplicity in terms of consolidation and reporting.

Reported exposure and recovery values were analysed consistently across cases. Net loss was measured as the successful fraud amount less reported recovery, subject to a minimum value of zero.

Attempted cases contribute to total exposure but not to net loss. Net loss for successful cases equals the reported amount less recovery, with a minimum of zero.

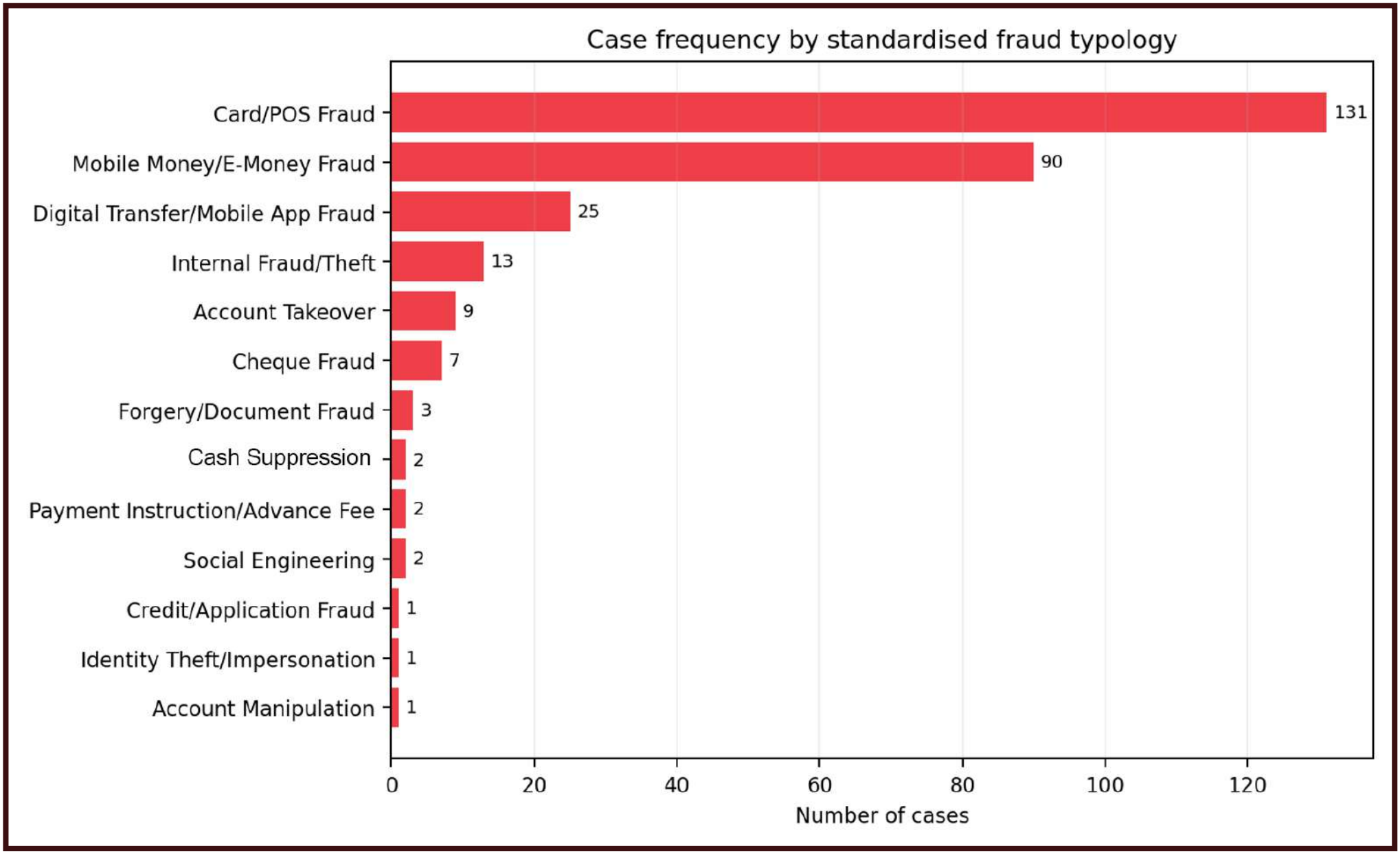
The analysis is presented at an aggregated typology level and excludes bank and customer-identifying information. It is intended for risk analysis, not for attributing blame or deciding liability.

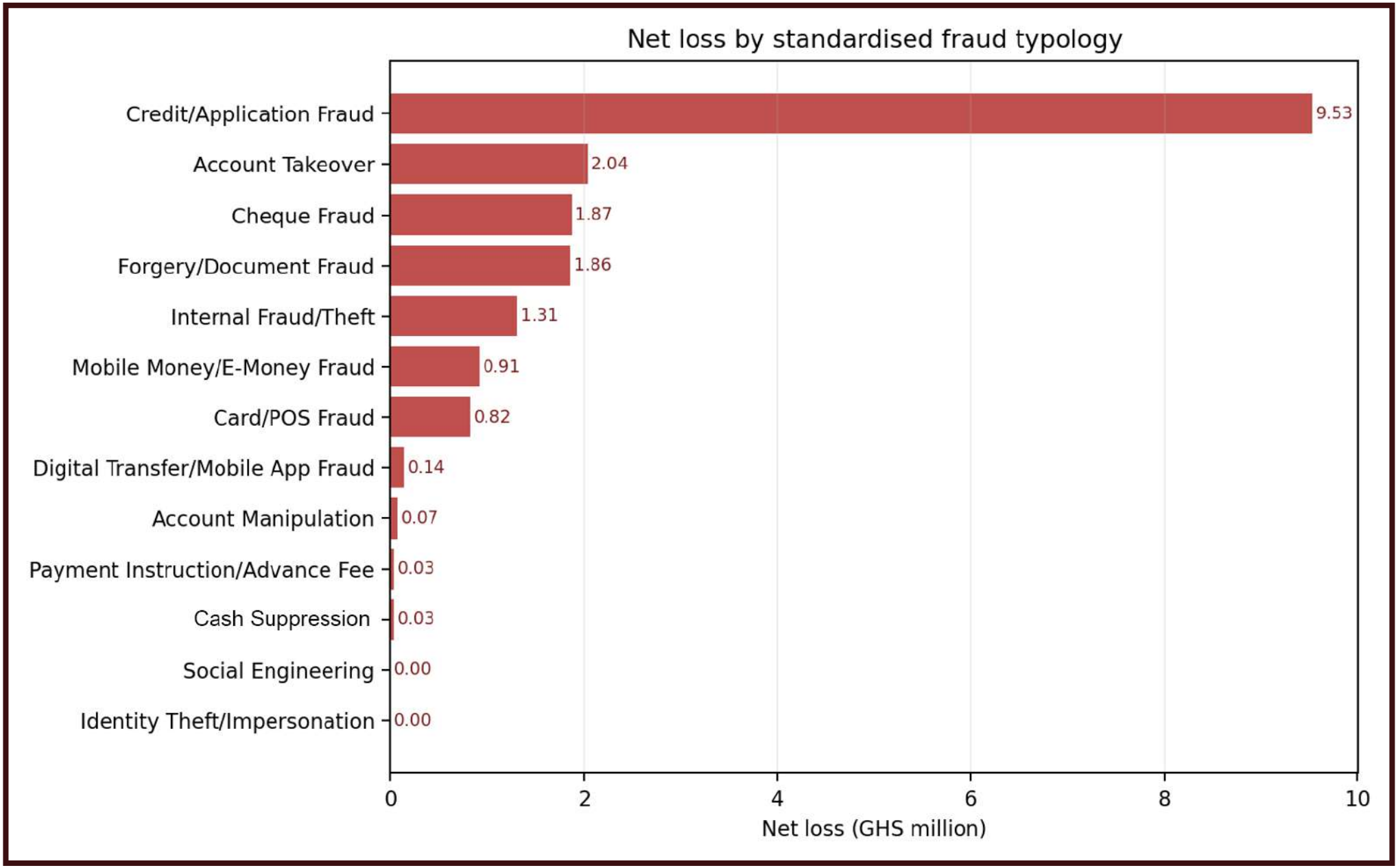
QUARTERLY FRAUD POSITION

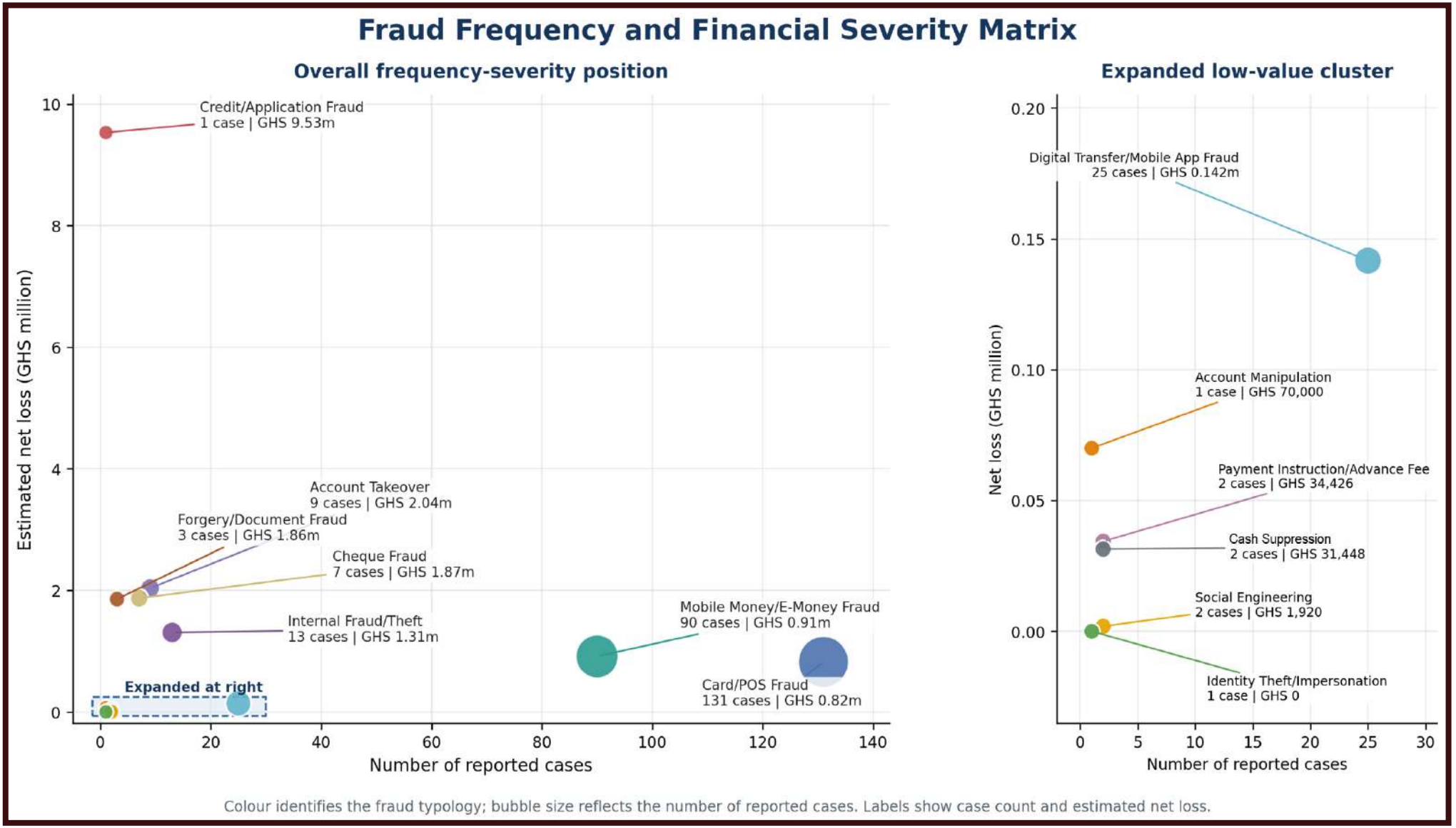
Month	No. of Banks	Cases	Exposure (GH¢)	Successful (GH¢)	Recovered (GH¢)	Net loss (GH¢)	Recovery rate
April	19	23	2,092,656.87	2,092,656.87	104,536.38	1,988,820.49	5.0%
May	23	134	3,636,914.50	3,636,914.50	98,652.71	3,538,261.81	2.7%
June	20	130	13,243,088.78	13,212,088.78	120,161.04	13,095,336.89	0.9%
Total	—	287	18,972,660.15	18,941,660.15	323,350.13	18,622,419.19	1.7%

CONSOLIDATED TYPOLOGICAL DISTRIBUTION AND LOSS ANALYSIS

Typology	Cases	Exposure	Recovered	Net loss	Case share	Loss share
Credit/Application Fraud	1	9,530,000.00	0.00	9,530,000.00	0.3%	**51.2%**
Account Takeover	9	2,071,096.00	5,600.00	2,036,496.00	3.1%	**10.9%**
Cheque Fraud	7	1,962,631.55	89,520.38	1,873,111.17	2.4%	**10.1%**
Forgery/Document Fraud	3	1,856,980.00	0.00	1,856,980.00	1.0%	**10.0%**
Internal Fraud/Theft	13	1,454,294.00	146,360.00	1,307,934.00	4.5%	**7.0%**
Mobile Money/E-Money Fraud	90	927,627.09	13,911.77	914,415.32	31.4%	**4.9%**
Card/POS Fraud	131	888,566.66	67,957.98	824,017.85	45.6%	**4.4%**
Digital Transfer/Mobile App Fraud	25	141,670.61	0.00	141,670.61	8.7%	**0.8%**
Account Manipulation	1	70,000.00	0.00	70,000.00	0.3%	**0.4%**
Payment Instruction/Advance Fee	2	34,426.19	0.00	34,426.19	0.7%	**0.2%**
Cash Suppression	2	31,448.05	0.00	31,448.05	0.7%	**0.2%**
Social Engineering	2	1,920.00	0.00	1,920.00	0.7%	**0.0%**
Identity Theft/Impersonation	1	2,000.00	0.00	0.00	0.3%	**0.0%**
TOTAL	**287**	**18,972,660.15**	**323,350.13**	**18,622,419.19**	**100.0%**	**100.0%**


Case frequency by standardised fraud typology
Card/POS Fraud
Mobile Money/E-Money Fraud
Digital Transfer/Mobile App Fraud
Internal Fraud/Theft
Account Takeover
Cheque Fraud
Forgery/Document Fraud
Cash Suppression
Payment Instruction/Advance Fee
Social Engineering
Credit/Application Fraud
Identity Theft/Impersonation
Account Manipulation
131
90
25
13
9
7
3
2
2
2
1
1
1
0
20
40
60
80
100
120
Number of cases


Net loss by standardised fraud typology
Credit/Application Fraud
Account Takeover
Cheque Fraud
Forgery/Document Fraud
Internal Fraud/Theft
Mobile Money/E-Money Fraud
Card/POS Fraud
Digital Transfer/Mobile App Fraud
Account Manipulation
Payment Instruction/Advance Fee
Cash Suppression
Social Engineering
Identity Theft/Impersonation
9.53
2.04
1.87
1.86
1.31
0.91
0.82
0.14
0.07
0.03
0.03
0.00
0.00
0
2
4
6
8
10
Net loss (GHS million)



The matrix presents beyond single ranking. Typologies in the lower-right impose a high operational workload through repeated incidents; those in the upper-left may be rare but can produce severe losses. Controls and management attention should therefore be allocated using both dimensions.

CREDIT/APPLICATION FRAUD

This category recorded 1 cases, total exposure of GHS 9,530,000.00, recoveries of GHS 0.00, and estimated net loss of GHS 9,530,000.00. It represented 0.3% of cases and 51.2% of estimated net loss.

ACCOUNT TAKEOVER

This category recorded 9 cases, total exposure of GHS 2,071,096.00, recoveries of GHS 5,600.00, and estimated net loss of GHS 2,036,496.00. It represented 3.1% of cases and 10.9% of estimated net loss.

CHEQUE FRAUD

This category recorded 7 cases, total exposure of GHS 1,962,631.55, recoveries of GHS 89,520.38, and estimated net loss of GHS 1,873,111.17. It represented 2.4% of cases and 10.1% of estimated net loss.

FORGERY/DOCUMENT FRAUD

This category recorded 3 cases, total exposure of GHS 1,856,980.00, recoveries of GHS 0.00, and estimated net loss of GHS 1,856,980.00. It represented 1.0% of cases and 10.0% of estimated net loss.

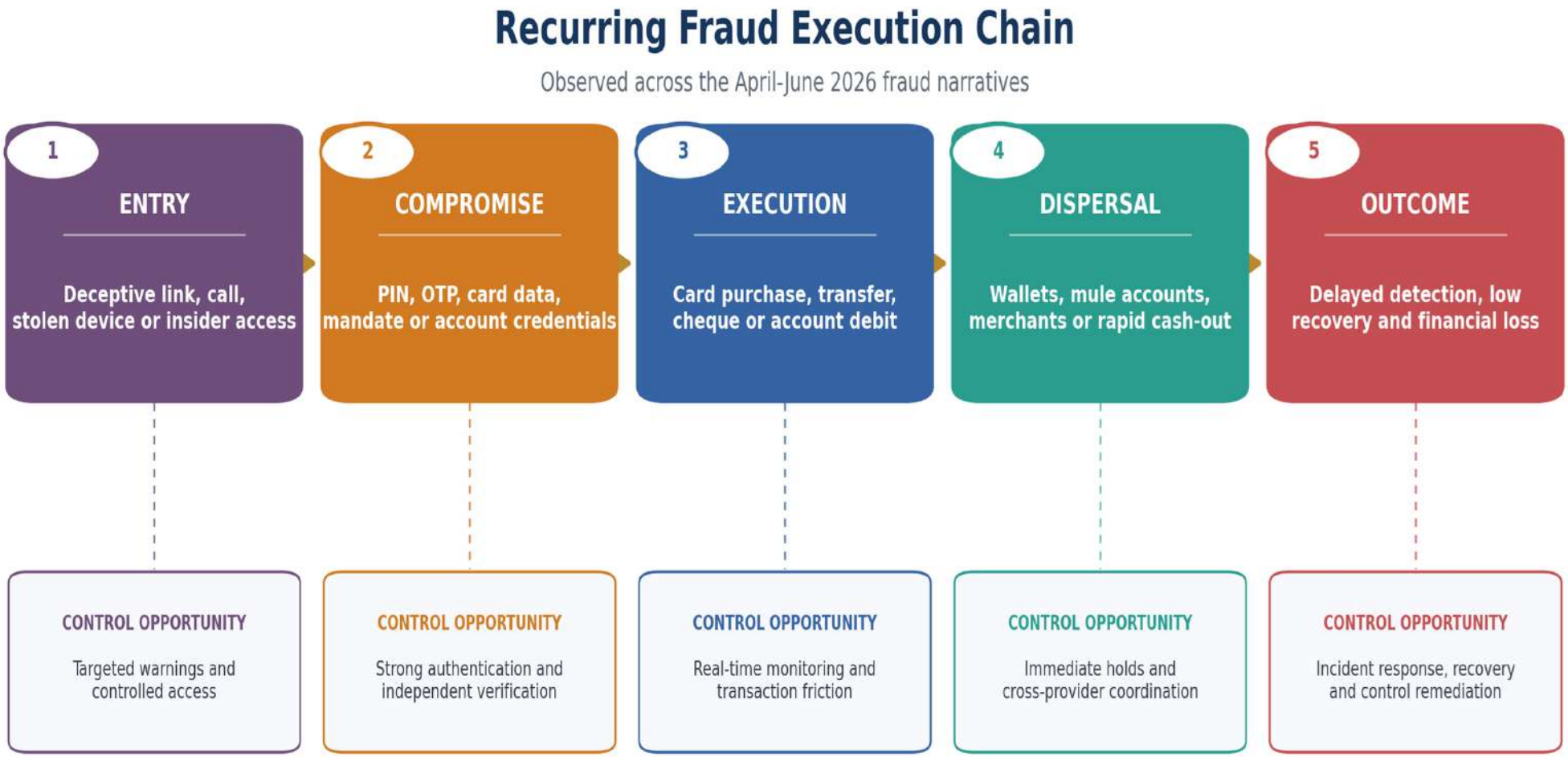
INTERNAL FRAUD/THEFT

This category recorded 13 cases, total exposure of GHS 1,454,294.00, recoveries of GHS 146,360.00, and estimated net loss of GHS 1,307,934.00. It represented 4.5% of cases and 7.0% of estimated net loss.

HOW THE FRAUDS WERE EXECUTED: MODUS OPERANDI

RECURRING FRAUD EXECUTION CHAIN

April-June 2026



The probability of recovery falls sharply after funds enter the dispersal stage; prevention and early intervention therefore remain critical.

Interpretation: The chain shows how an initial point of entry can progress into credential or process compromise, transaction execution, rapid dispersal and eventual financial loss.

CARD/POS FRAUD

Observed method: Card details were obtained through deceptive merchant pages, social-media purchases, compromised websites, stolen cards or earlier credential exposure. Fraudsters then initiated card-not-present purchases, often across several merchants or in rapid succession.

Control implication: Merchant risk scoring, transaction velocity, 3-D Secure or equivalent step-up checks, instant customer alerts, card-freeze tools and conservative online limits.

MOBILE MONEY AND E-MONEY FRAUD

Observed method: Customers were persuaded to disclose wallet PINs or banking credentials, or fraudsters exploited a lost or compromised phone. Funds were moved from a bank account to a linked wallet and quickly dispersed to other wallets or cashed out.

Control implication: New-device controls, wallet-linkage confirmation, beneficiary cooling-off, behavioural monitoring and immediate bank-MNO hold procedures.

DIGITAL TRANSFER AND ACCOUNT TAKEOVER

Observed method: Attackers combined phishing, impersonation, stolen devices, weak recovery processes or trusted assistance to gain control of mobile or internet banking. They behaved like the customer and transferred funds to new beneficiaries or mule accounts.

Control implication: Out-of-band verification, device binding, SIM-change intelligence, new-beneficiary friction, impossible-travel checks and risk-based transaction holds.

CHEQUE, FORGERY AND DOCUMENT FRAUD

Observed method: Cloned cheques, altered mandates, forged signatures and manipulated supporting documents were presented as legitimate instructions. High-value events exploited gaps in callback, image review, mandate validation or independent document confirmation.

Control implication: Independent callbacks using trusted records, image and signature analytics, maker-checker enforcement, source-document validation and enhanced review of unusual beneficiaries.

INTERNAL FRAUD, THEFT AND ACCOUNT MANIPULATION

Observed method: Trusted access was used to suppress deposits, divert proceeds, process unauthorised debits, override controls or manipulate dormant, deceased-customer or operational accounts. Concealment occurred within normal workflows.

Control implication: Strict segregation, privileged-access analytics, staff-account linkage checks, forced leave and role rotation, daily reconciliation and independent exception review.

SOCIAL ENGINEERING, IDENTITY AND ADVANCE-FEE SCHEMES

Observed method: Fraudsters posed as banks, merchants, delivery firms, investment providers, relatives or business counterparties. The victim was induced either to reveal credentials or voluntarily send money for a false transaction.

Control implication: Context-specific warnings at the point of payment, verified contact channels, payee-name confirmation, staff scripts for vulnerable customers and targeted public education.

KEY MODUS OPERANDI OBSERVED ACROSS THE QUARTER

The case narratives show that the reported incidents were not isolated techniques. They followed recurring attack scenarios in which fraudsters exploited trust, weak verification, payment speed and gaps between banks and external platforms. The principal scenarios are set out below.

1. DECEPTIVE-LINK AND CREDENTIAL-HARVESTING ATTACKS

Fraudsters circulated links through WhatsApp, SMS, social media and online advertisements. The links were presented as food-ordering pages, parcel-delivery updates, subscription-payment pages, shopping platforms or investment opportunities. Customers entered card details, mobile-banking credentials, wallet PINs or OTPs into the false page. The captured information was then used to initiate online card purchases, mobile-app transfers or bank-to-wallet transactions. The fraudulent transaction often occurred immediately, leaving little time for the customer to recognise that the original page was false.

The decisive control point is before or at credential use. Banks should combine malicious-link intelligence, transaction risk scoring, step-up authentication and immediate alerts. Customer education should use the specific scenarios observed, rather than broad instructions merely telling customers to be careful online.

2. CARD-NOT-PRESENT MERCHANT EXPLOITATION

Compromised card credentials were used on online merchant platforms without the physical card. Transactions were sometimes processed in rapid succession, across several merchants or after the card information had been compromised earlier and stored for later use. In some cases, the original point of compromise was unclear, which indicates that exposure may arise well before the unauthorised transaction appears.

Controls should focus on merchant category, transaction velocity, unusual geography, first-time online use and deviation from the customer profile. Tokenisation, dynamic authentication, customer-defined online limits and instant self-service card blocking can reduce both the likelihood and duration of loss.

3. BANK-TO-WALLET TRANSFER AND RAPID CASH-OUT

After obtaining banking or wallet credentials, fraudsters moved money from a bank account into a mobile-money wallet. The proceeds were then transferred to additional wallets, withdrawn through agents or routed to third parties. The speed and fragmentation of this process reduced the effectiveness of recall attempts and made it difficult to establish where the final beneficiary was located.

This method requires a joint bank-MNO response. High-risk wallet linkage, a new device, a new beneficiary and an unusual transfer amount should be assessed together. Rapid freeze procedures, common fraud references and clear response timelines are necessary before the proceeds are dispersed.

4. LOST PHONE, STOLEN DEVICE AND TRUSTED-ASSISTANCE COMPROMISE

Some incidents began when a customer

lost a phone, handed it to another person for assistance or allowed a third party to observe a PIN. Where the same or a weak PIN protected several channels, the fraudster could enter the wallet, USSD service or mobile-banking application and transact as though they were the customer. Familiarity gained during account setup or previous assistance also created opportunities for later misuse.

Banks should strengthen device binding, PIN-reset controls, session-risk monitoring and rapid lost-device reporting. Sensitive

KEY MODUS OPERANDI OBSERVED ACROSS THE QUARTER (Cont...)

assistance should be performed through controlled channels, and customers should be warned against allowing third parties to operate their devices or observe authentication information.

5. ACCOUNT TAKEOVER THROUGH COMBINED IDENTITY AND TELECOM COMPROMISE

More developed attacks combined phishing or impersonation with control of the customer communication channel. Fraudsters obtained credentials and then used a changed SIM, disrupted mobile service or access to the customer device to receive authentication prompts and suppress warnings. Once the account was controlled, transfers to new beneficiaries appeared technically authorised.

New-device enrolment, SIM change, credential reset and new-beneficiary creation should form one connected risk event. Out-of-band verification should use a previously trusted channel, while high-risk transactions should be delayed or independently confirmed.

6. CLONED CHEQUE, FORGED MANDATE AND DOCUMENT ALTERATION

Fraudsters presented cloned cheques, altered instructions, forged signatures or manipulated supporting documents as genuine customer mandates. The method relied on the visual similarity of documents, gaps in callback procedures, weak comparison with mandate records or inadequate validation of the beneficiary and underlying commercial purpose.

High-value cheques and unusual written instructions require independent confirmation using contact details already held by the bank. Image analytics, serial-number checks, signature comparison, source-document validation and strict maker-checker review should be combined rather than applied separately.

7. CREDIT AND APPLICATION-DOCUMENT FRAUD

A high-value exposure arose where allegedly forged supporting documents were used in obtaining a credit facility and expected repayments did not materialise. This differs from ordinary payment fraud because the loss develops through the credit process and may only become visible after disbursement and repayment failure.

The response should include independent verification of business activity, financial records, collateral, supplier relationships and beneficial ownership before disbursement. Early post-disbursement monitoring is equally important because it can reveal diversion of funds or inconsistencies before the full exposure crystallises.

8. INTERNAL ACCESS ABUSE, CASH SUPPRESSION AND ACCOUNT MANIPULATION

Staff-related cases involved failure to credit customer deposits, diversion of funds, unauthorised debits, override of controls, misuse of privileged access and manipulation of dormant, deceased-customer or operational accounts. Because the activity occurred within legitimate systems and processes, it could be concealed among normal transactions and remain undetected until reconciliation, complaint or investigation.

Effective controls include strict segregation of duties, daily reconciliation, privileged-user analytics, monitoring of staff-linked beneficiaries, forced leave, rotation of sensitive duties and independent review of overrides. Management should treat repeated exceptions and unexplained lifestyle or account linkages as risk signals.

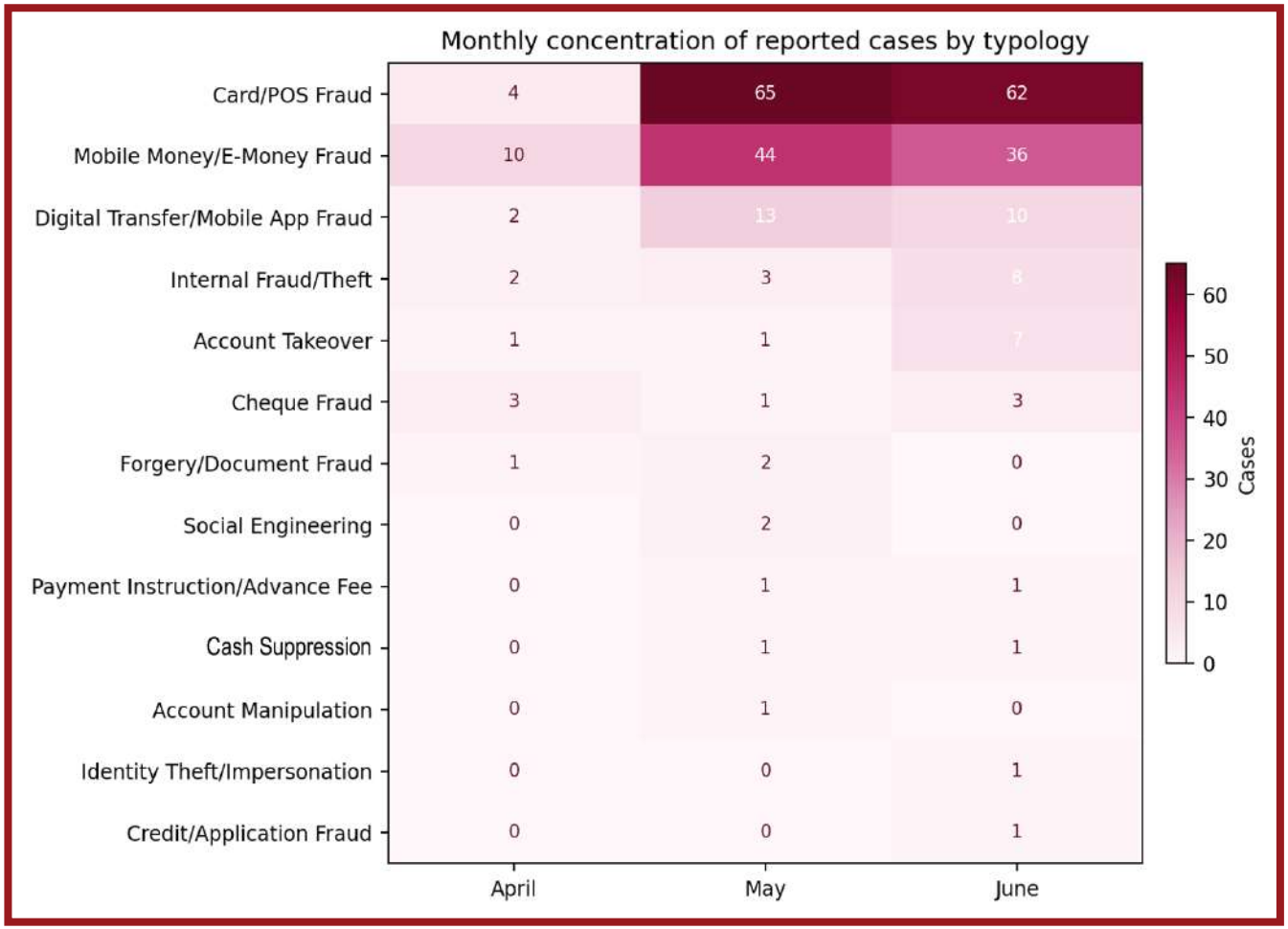
KEY MODUS OPERANDI OBSERVED ACROSS THE QUARTER (Cont...)

9. MULE ACCOUNTS AND MULTI-BENEFICIARY DISPERSAL

Across several typologies, the receiving account or wallet was not necessarily controlled by the principal fraudster. Funds passed through third-party accounts, multiple wallets, merchants or cash-out points. This layering obscured the origin and destination of the proceeds and delayed recovery efforts.

Banks and payment providers should detect rapid incoming-and-outgoing movement, unrelated third-party transfers, sudden activity in previously quiet accounts and repeated links to reported fraud. Industry-wide intelligence is essential because the full pattern may not be visible within one institution.

MONTHLY NARRATIVES AND STRATEGIC INSIGHTS



The heatmap shows where reported case concentration changed across the quarter. It should be interpreted as a pattern in submissions, not a complete measure of industry incidence, because reporting coverage may differ by month.

MONTHLY NARRATIVES AND STRATEGIC INSIGHTS (CONT...)

APRIL 2026

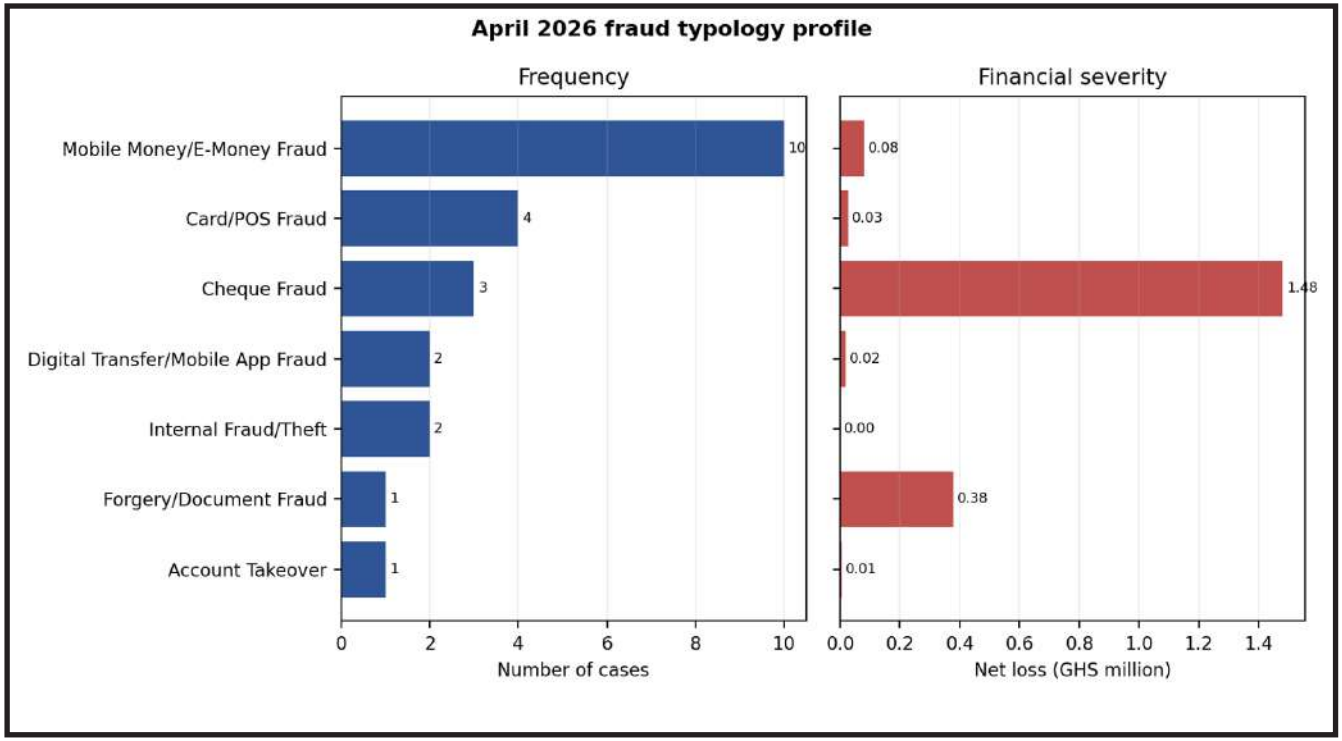
April contained 23 distinct cases with exposure of GHS 2,092,656.87, reported recoveries of GHS 104,536.38, and estimated net loss of GHS 1,988,820.49. The leading categories by frequency were Mobile Money/E-Money Fraud (10), Card/POS Fraud (4), Cheque Fraud (3).

The April incidents presented a mixed fraud structure. Retail digital cases were frequent, but the largest values arose from cloned cheques, forged or manipulated instructions and staff-related misconduct. Fraudsters also exploited mobile-money linkage, compromised phones, remote-access assistance and deceptive online interactions. In several cases, funds moved from bank accounts into wallets or third-party accounts soon after access was obtained.

The cheque cases show that traditional instruments remain material. Cloned cheques were presented through the clearing system using altered customer information and beneficiary details. The internal and document-related cases involved unauthorised initiation, approval or diversion of customer funds. These events point to weaknesses in maker-checker controls, signature verification, callback procedures and staff access monitoring.

From a control perspective, April demonstrates why fraud surveillance cannot focus only on digital channels. Banks require layered controls covering cards, wallets, clearing instruments, staff privileges and physical access. High-value instructions should receive independent confirmation, while unusual beneficiary accounts and rapid outward transfers should trigger immediate review.

The largest loss concentrations were Cheque Fraud (GHS 1,481,000.00), Forgery/Document Fraud (GHS 377,840.00), Mobile Money/E-Money Fraud (GHS 79,490.75). This supports a risk-based response that considers both case frequency and potential severity.



MONTHLY NARRATIVES AND STRATEGIC INSIGHTS (CONT...)

MAY 2026

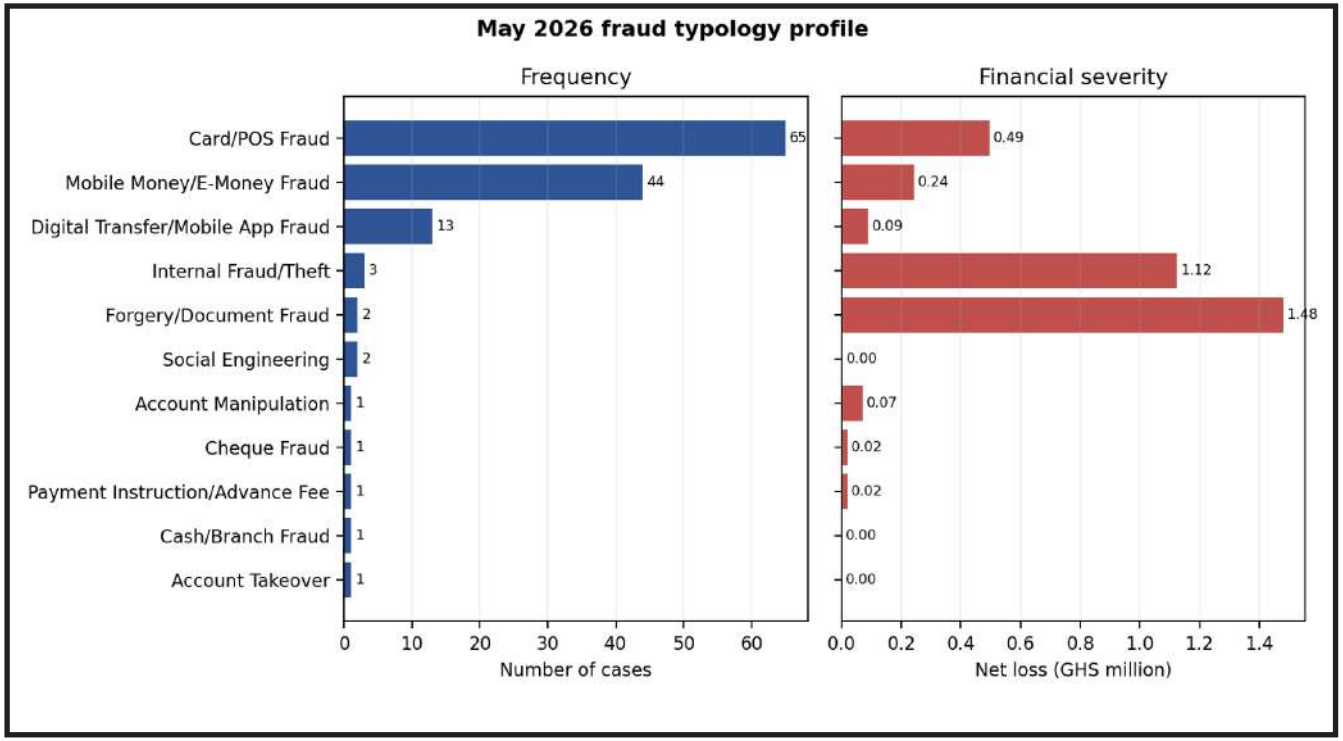
May contained 134 distinct cases with exposure of GHS 3,636,914.50, reported recoveries of GHS 98,652.71, and estimated net loss of GHS 3,538,261.81. The leading categories by frequency were Card/POS Fraud (65), Mobile Money/E-Money Fraud (44), Digital Transfer/ Mobile App Fraud (13).

May was dominated by card-not-present and mobile-money-related complaints. The common entry points were deceptive links, fake online merchants, social-media advertisements, investment offers, food-ordering scams and calls from persons pretending to represent trusted institutions. Customers were induced to disclose card details, PINs or OTPs, after which transactions were executed on online merchant platforms or funds were transferred into mobile wallets.

A second pattern involved compromised or changed devices. Fraudsters registered or used mobile-banking services on unfamiliar devices, sometimes after a phone was lost or after the customer responded to a fraudulent prompt. Several cases also displayed mule-account behaviour: incoming funds were quickly transferred to third parties or cashed out, reducing the possibility of recovery.

May also contained high-value document alteration and internal fraud. These cases show that high case frequency and high financial severity can arise from different channels. Card and wallet fraud create a heavy operational burden, while a small number of insider or document cases can generate much larger individual losses.

The largest loss concentrations were Forgery/Document Fraud (GHS 1,479,140.00), Internal Fraud/ Theft (GHS 1,121,754.00), Card/POS Fraud (GHS 494,255.73). This supports a risk-based response that considers both case frequency and potential severity.



MONTHLY NARRATIVES AND STRATEGIC INSIGHTS (CONT...)

JUNE 2026

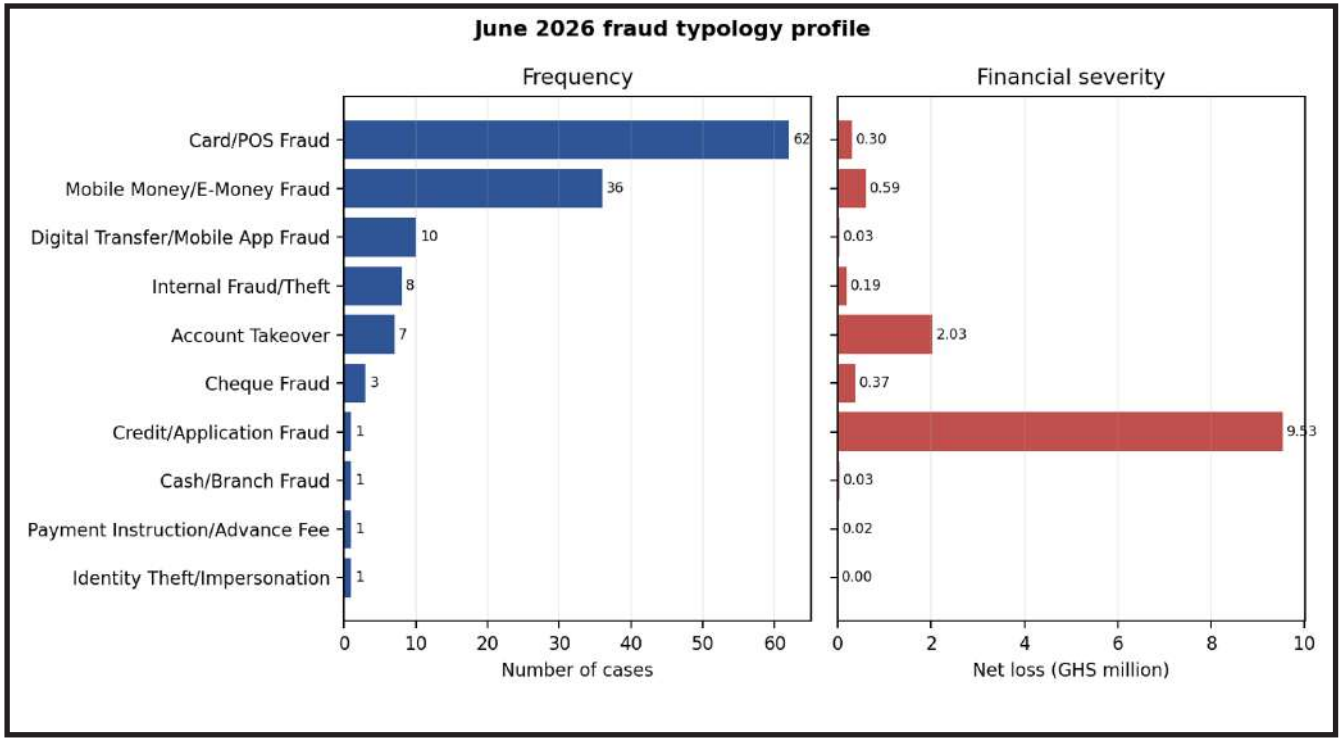
June contained 130 distinct cases with exposure of GHS 13,243,088.78, reported recoveries of GHS 120,161.04, and estimated net loss of GHS 13,095,336.89. The leading categories by frequency were Card/POS Fraud (62), Mobile Money/E-Money Fraud (36), Digital Transfer/ Mobile App Fraud (10).

June recorded the highest reported exposure. Card fraud and bank-to-wallet fraud remained prominent, but the month was heavily influenced by a small number of high-value account-takeover, credit-disbursement, cheque, internal and document-related incidents. This creates a strong concentration effect: the aggregate loss is not explained by retail fraud alone.

The retail cases repeatedly involved fake parcel notices, food-ordering links, online shopping prompts, card credential harvesting, stolen phones and disclosure of OTPs or mobile-money PINs. Once credentials were obtained, fraudsters conducted card-not-present purchases or moved funds through wallets. The speed of cash-out and use of multiple beneficiaries limited recovery.

The high-value cases involved suspected forged supporting documents, manipulation of dormant or deceased-customer accounts, cloned bank cheques, forged mandates, cash suppression and misuse of trusted staff positions. The month therefore reinforces the need for strong credit-document validation, post-disbursement monitoring, deceased-account controls, staff surveillance and independent verification of large-value transactions.

The largest loss concentrations were Credit/Application Fraud (GHS 9,530,000.00), Account Takeover (GHS 2,030,310.00), Mobile Money/E-Money Fraud (GHS 593,469.63). This supports a risk-based response that considers both case frequency and potential severity.



CROSS-CUTTING FINDINGS FOR THE QUARTER : APRIL -JUNE 2026

DIGITAL CONVENIENCE IS ALSO A FRAUD PATHWAY

Bank-to-wallet, mobile-app and card-not-present channels allowed funds to move quickly. Controls must operate at transaction speed.

SOCIAL ENGINEERING REMAINS A PRIMARY ENTRY POINT

Fraudsters used fake merchant links, delivery prompts, investment offers, calls and impersonation to obtain PINs, OTPs and card details.

DEVICE AND TELECOM COMPROMISE INCREASES ACCOUNT-TAKEOVER RISK

Lost or replaced phones, call forwarding, device changes and possible malware featured in several cases.

INTERNAL FRAUD REMAINS LOW-FREQUENCY BUT POTENTIALLY SEVERE

Staff access, forged instructions, uncredited cash and self-authorisation created high-value exposure in a small number of cases.

RECOVERY IS WEAKEST AFTER RAPID DISPERSAL

Once funds reached wallets, mule accounts or overseas merchants, recovery became difficult. Immediate alerts and coordinated holds are therefore critical.

CONSISTENT REPORTING REMAINS IMPORTANT

Common typology definitions, complete financial fields and timely investigation updates improve comparability and support stronger management decisions.

KEY IMPLICATIONS FOR THE BANKING INDUSTRY

OPERATIONAL RESILIENCE

Fraud control should cover the full payment journey, including the originating bank, beneficiary bank, mobile wallet, merchant and telecom channel.

CUSTOMER PROTECTION

Clear warnings should be placed at high-risk moments, especially wallet linkage, new-device registration, OTP entry and first-time beneficiary transfers.

CONTROL GOVERNANCE

High-risk staff entitlements, overrides and self-authorised transactions require stronger segregation of duties and exception monitoring.

INDUSTRY INTELLIGENCE

Common identifiers and rapid case-sharing protocols are needed to identify mule accounts, linked devices and repeat beneficiaries across institutions.

MANAGEMENT INFORMATION

Case counts alone are insufficient. Banks should track attempted exposure, successful loss, recovery, speed of detection, channel, root cause and control failure.

STRATEGIC RECOMMENDATIONS

STANDARDISE INDUSTRY FRAUD REPORTING

Adopt one mandatory taxonomy, field dictionary and validation process. Each incident should have a unique reference and clear amount, status, recovery and loss fields.

STRENGTHEN NEW-DEVICE AND CREDENTIAL CONTROLS

Use risk-based step-up authentication, cooling-off periods and out-of-band verification for new devices, PIN resets and unusual wallet linkage.

IMPROVE REAL-TIME TRANSACTION MONITORING

Apply behavioural analytics to unusual beneficiaries, rapid wallet transfers, repeated small debits, impossible travel and deviations from customer profile.

ACCELERATE INTER-BANK AND TELECOM RESPONSE

Create defined response timelines for beneficiary-account holds, wallet freezes, device checks and recall requests.

TIGHTEN CARD-NOT-PRESENT CONTROLS

Promote tokenisation, merchant-risk scoring, dynamic authentication, customer-controlled card limits and instant card-freeze tools.

REINFORCE CHEQUE AND DOCUMENT VERIFICATION

Apply callback verification, image analytics and independent confirmation for high-value cheques and altered instructions.

STRATEGIC RECOMMENDATIONS (CONT....)

STRENGTHEN STAFF OVERSIGHT

Review privileged access, enforce segregation of duties, monitor overrides, rotate sensitive roles and investigate unexplained staff-account linkages.

CONDUCT QUARTERLY DATA-QUALITY ASSURANCE

Reconcile case registers to financial totals, validate required fields and apply consistent classifications before industry consolidation.

TARGET CUSTOMER EDUCATION AT OBSERVED TACTICS

Campaign messages should focus on fake food-order links, parcel prompts, investment offers, OTP/PIN disclosure, card-detail sharing and remote assistance.

TRACK RECOVERY PERFORMANCE

Measure time-to-detection, time-to-hold and amount recovered by channel. Use the results to identify where partnerships and controls are failing.

CONCLUSION

The analysis of fraud incidents reported for April to June 2026 highlights an increasingly broad, interconnected and operationally complex fraud environment within Ghana's banking industry. The 287 distinct cases covered total reported exposure of GHS 18,972,660.15, recoveries of GHS 323,350.13, and an estimated net loss of GHS 18,622,419.19. Fraud was not concentrated in one channel. It extended across cards, mobile money, digital transfers, customer devices, cheques, credit processes, internal operations and account-management systems.

The quarter displayed two different but connected risk patterns. Card/POS and mobile-money fraud dominated the number of reported incidents and created a persistent operational burden. By contrast, credit/application fraud, account takeover, cheque fraud, document forgery and internal misconduct occurred less frequently but generated substantial financial exposure. Effective fraud management must therefore consider both frequency and severity. A control framework focused only on the most common cases may fail to address the events capable of producing the largest losses.

A recurring concern is the low recovery rate of 1.7% against successful fraud amounts. Once proceeds moved through mobile wallets, mule accounts, merchants or cash-out points, recovery became difficult. This reinforces the need to place greater emphasis on prevention, real-time detection and immediate transaction intervention. Strong authentication, new-device monitoring, beneficiary-risk assessment and rapid holds are more effective when applied before funds are fragmented across the financial ecosystem.

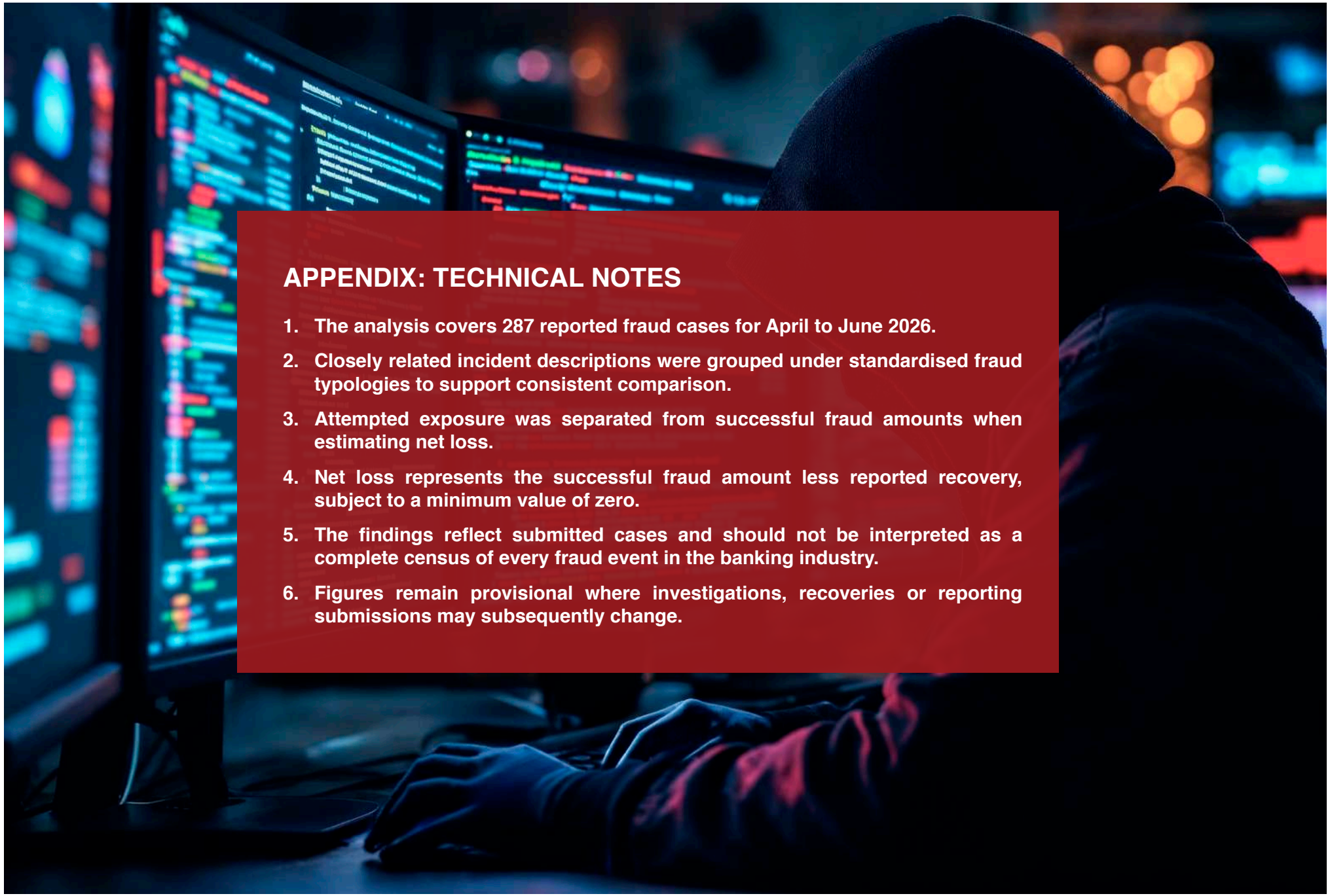
The modus-operandi analysis shows that fraudsters increasingly combine human deception with legitimate banking and payment infrastructure. They use false merchant pages, parcel notices, investment offers, impersonation, stolen devices and compromised credentials to enter the system. They then exploit the speed of card payments, mobile-money transfers and digital banking to execute and disperse transactions. Traditional methods have not disappeared: cloned cheques, altered mandates, forged documents, cash suppression and staff-access abuse remain material sources of loss.

A further lesson is that customer education, although essential, cannot carry the full burden of fraud prevention. Several incidents also reflected process weaknesses, delayed alerts, insufficient document validation, weak segregation of duties, privileged-access risk and slow coordination between institutions. Banks should therefore combine customer awareness with strong system controls, disciplined operations and clear accountability for control exceptions.

Effective detection and response also depend on the speed and quality of information sharing. Many reported patterns crossed the boundaries of a single institution and involved banks, mobile network operators, payment service providers, merchants, beneficiary institutions and law-enforcement agencies. Delays in communicating account, wallet, device and beneficiary information allowed proceeds to move beyond reach. Structured industry protocols and timely fraud intelligence are therefore central to limiting losses.

The detailed presentation of fraud typologies and modus operandi in this report is intended to support risk managers, fraud-control teams and operational leaders in refining detection scenarios, strengthening preventive controls and directing resources toward the areas of greatest risk. It also provides an evidence base for targeted staff training and public education that reflects the actual tactics observed during the quarter.

In line with its coordinating role, the Ghana Association of Banks will continue to promote the nation-wide anti-fraud awareness campaign, encourage stronger industry-wide intelligence sharing and closer collaboration with financial-ecosystem partners and the bank of Ghana to standing against fraud. Sustained cooperation, reliable data and faster intervention remain essential to building a safer, more resilient and trusted banking environment in Ghana.



APPENDIX: TECHNICAL NOTES

1. The analysis covers 287 reported fraud cases for April to June 2026.
2. Closely related incident descriptions were grouped under standardised fraud typologies to support consistent comparison.
3. Attempted exposure was separated from successful fraud amounts when estimating net loss.
4. Net loss represents the successful fraud amount less reported recovery, subject to a minimum value of zero.
5. The findings reflect submitted cases and should not be interpreted as a complete census of every fraud event in the banking industry.
6. Figures remain provisional where investigations, recoveries or reporting submissions may subsequently change.

GAB

GHANA ASSOCIATION OF BANKS

Contact Us:

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

+233-0302-667-138 / 0302-670-62

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