International Journal of Innovative Inventions in Social Science and Humanities

ISSN(print): 3050-6921, ISSN(online): 3050-693X

Volume 03 Issue 08 August 2026

DOI: 10.58806/ijiissh.2026.v3i8n05

Page No: 976-985

Mobile Money Fraud and Financial Integrity in Africa: Towards a Context-Sensitive Framework for Forensic Accounting and Digital Auditing

Dr. Gaduga Godwin, Esq

Lecturer at Accra Institute of Technology Adjunct Lecturer at Blue Crest University College

ABSTRACT

Mobile money has become the dominant channel through which ordinary Africans store, send and receive value, with sub-Saharan Africa accounting for roughly two-thirds of the more than two trillion United States dollars that flowed through mobile money wallets worldwide in 2025 (GSMA, 2026). The same architecture that has delivered this expansion in financial inclusion, namely agent networks, USSD interfaces, SIM-based identity and near-instant settlement, has also produced a distinctive fraud ecology that conventional forensic accounting and audit methodologies, developed for formal corporate environments in high-income economies, are poorly equipped to address. Drawing on regulatory data from the Bank of Ghana, industry reporting from the GSMA, and the scholarly literature on fraud examination and mobile financial services, this article maps the principal typologies of mobile money fraud, interrogates the limits of the fraud triangle and its successors when transposed into informal, cash-adjacent and agent-mediated economies, and proposes a five-pillar context-sensitive framework for forensic accounting and digital auditing of mobile money ecosystems. The framework treats the agent, rather than the corporate entity, as a primary unit of audit attention, integrates behavioural and social engineering evidence into the forensic process, and anchors evidentiary practice in the statutory regimes governing electronic transactions and cybersecurity in African jurisdictions. The article closes with implications for practitioners, regulators and researchers.

KEYWORDS: Mobile Money, Fraud, Forensic Accounting, Digital Auditing, Financial Integrity, Africa, Ghana, Agent Networks.

ARTICLE DETAILS

Published On:
15 August 2026

Available on:
https://ijiissh.com/

INTRODUCTION

The story of mobile money in Africa is usually told as a story of triumph, and on the numbers, it is difficult to argue otherwise. A service that began in 2007 as a modest person-to-person transfer product on the Safaricom network in Kenya has grown into a continental payments infrastructure that now touches more lives than the formal banking system ever managed to reach. By the end of 2025, there were 2.3 billion registered mobile money accounts worldwide, of which more than half were held in Africa, and the value transacted globally passed two trillion United States dollars in a single year, with sub-Saharan Africa alone accounting for approximately 1.4 trillion dollars of that total (GSMA, 2026). The developmental dividends are well documented. Access to mobile money has been shown to improve household risk sharing in the face of income shocks (Jack & Suri, 2014), and the most widely cited estimate attributes to M-PESA the movement of roughly two per cent of Kenyan households out of extreme poverty (Suri & Jack, 2016). The Global Findex data confirm that mobile money is now the principal driver of account ownership growth in sub-Saharan Africa, where a third of adults hold a mobile money account and where, in several economies, more adults hold mobile money accounts than bank accounts (Demirgüç-Kunt et al., 2022).

There is, however, a second story running underneath the first, and it is the concern of this article. The same design features that made mobile money transformative, which is to say its reliance on vast networks of independent cash-in cash-out agents, its accessibility through basic USSD menus on inexpensive handsets, its use of the SIM card as the effective locus of identity, and its capacity to move value across a network in seconds, have created an environment in which fraud flourishes in forms that the established apparatus of forensic accounting and auditing struggles to see, let alone to prevent, detect or prove. The Bank of Ghana's fraud reporting illustrates the trajectory with uncomfortable clarity. Reported fraud cases across banks, specialized deposit-taking institutions and payment service providers in Ghana rose from 16,733 in 2024 to 24,778 in 2025, an increase of forty-eight per cent in a single year, and payment service providers, the category that includes mobile money operators and fintech platforms, accounted

for approximately ninety-seven per cent of all reported cases in 2025 (Bank of Ghana, 2026). Over the four years to 2025, fraud cases in the payment service provider sector nearly doubled while cases in the traditional banking sector declined, a migration that tracks precisely the migration of transaction volume itself. Of the total value exposed to fraud in 2025, only about five per cent was recovered (Bank of Ghana, 2026). Fraud, in other words, has followed the money into the mobile channel, and the recovery figures suggest that once value leaves a victim's wallet it is, for practical purposes, gone.

The problem this article addresses is therefore both practical and conceptual. At the practical level, forensic accountants, internal auditors, fraud examiners, financial investigators and the lawyers who work with them need methods that are fitted to the actual architecture of mobile money ecosystems, which differ from the corporate environments for which the discipline's standard tools were built in almost every respect that matters. The classic forensic engagement presumes an entity with a general ledger, segregated duties, documentary trails, an internal control environment that can be tested, and a population of employees whose conduct is governed by contract and policy. The mobile money ecosystem presents instead a distributed network of tens of thousands of semi-formal agents transacting in cash, a customer base with widely varying levels of digital and financial literacy, an identity layer that depends on SIM registration regimes of uneven integrity, and a fraud population dominated not by insiders manipulating records but by outsiders manipulating people. At the conceptual level, the dominant theoretical frames of fraud examination, above all the fraud triangle inherited from Cressey (1953) and its later elaborations, were derived from studies of occupational offenders in formal Western organizations, and their transposition into African informal and semi-formal financial economies is neither automatic nor innocent. A framework is needed that takes the African context seriously as a source of theory and method rather than merely as a site of application.

The argument proceeds in five movements. The article first describes the scale and architecture of mobile money in Africa and locates the points at which that architecture generates vulnerability. It then maps the principal typologies of mobile money fraud as they appear in the regulatory data, the industry literature and the small but growing body of empirical scholarship. The third movement interrogates the received theoretical apparatus of fraud examination and explains why it requires adaptation rather than mere adoption. The fourth and central movement proposes a context-sensitive framework for forensic accounting and digital auditing of mobile money ecosystems, organised around five pillars and a cross-cutting evidentiary spine. The final movement draws out the implications for practice, regulation and research. Ghana supplies the primary jurisdictional anchor because its regulatory disclosure is unusually rich and because the author writes from within its legal system, but the analysis draws throughout on Kenyan, Nigerian, Tanzanian and continental material, and the framework is offered for adaptation across African jurisdictions rather than for any one of them alone.

MOBILE MONEY IN AFRICA: SCALE, ARCHITECTURE AND THE ANATOMY OF VULNERABILITY

The Scale of the Ecosystem

Any serious treatment of mobile money fraud must begin with an appreciation of scale, because scale is itself a fraud risk factor. The GSMA's industry reporting records that global transaction values took twenty years to reach one trillion dollars a year and then only four further years to double, passing two trillion dollars in 2025, with monthly active accounts rising fifteen per cent in that year to 593 million (GSMA, 2026). Sub-Saharan Africa remains the centre of gravity of the industry, hosting more than half of all registered accounts, roughly three-fifths of monthly active accounts and about two-thirds of global transaction value, with East Africa alone transacting on the order of 806 billion dollars in 2025 and West Africa approximately 498 billion dollars (GSMA, 2026). The 2024 data already showed the industry supporting some 28 million registered agents, the overwhelming majority of them in sub-Saharan Africa, whose cash-in operations accounted for more than half of the funds entering the ecosystem (GSMA, 2025). Mobile money is estimated to have added about 190 billion dollars to the gross domestic product of sub-Saharan African economies in 2023, and in a band of countries stretching from Senegal to Kenya its contribution to output exceeds five per cent (GSMA, 2025). These are no longer figures that describe a niche product for the unbanked. They describe systemically significant financial infrastructure, and the integrity of that infrastructure is accordingly a matter of financial stability and not merely of consumer protection.

The Architecture and Its Points of Vulnerability

The vulnerability of the ecosystem is best understood by walking through its architecture layer by layer. At the base sits the identity layer, which in most African deployments is the registered SIM card, increasingly tied to a national identity credential such as the Ghana Card under the SIM registration regimes that many jurisdictions adopted during the past decade. The SIM is, in effect, the key to the wallet, and this design decision means that any weakness in SIM issuance, replacement or swap procedures is a weakness in the financial system itself. Fraudulent SIM swaps executed with forged identity documents, or with the connivance of registration agents, permit an offender to take over a victim's wallet, intercept one-time passwords and transaction alerts, and drain both mobile money balances and any linked bank accounts before the victim has even discovered that their own SIM has gone dead. Security research on mobile money authentication has repeatedly shown that the prevailing combination of a four-digit personal identification

number and SIM-based session identity offers thin protection against interception, shoulder surfing and social engineering, particularly on USSD channels that transmit without end-to-end encryption (Ali et al., 2020).

Above the identity layer sits the agent network, which is the feature that most sharply distinguishes mobile money from card or bank-transfer systems and which deserves far more forensic attention than it customarily receives. The agent is a hybrid figure, a private trader who is simultaneously the human interface of a regulated financial service, holding a float of electronic value and a float of physical cash and converting continuously between the two. Agents are where customers are made and where they are unmade. Field research from the earliest days of M-PESA documented how heavily customers rely on agents for guidance, how frequently agents handle transactions on customers' behalf, and how much trust is reposed in them as neighbourhood figures (Morawczynski, 2009). That trust is an asset to the system and simultaneously its softest target, because an agent who is corrupt, colluding or merely careless can facilitate direct theft, identity harvesting, unauthorized SIM registrations, split deposits designed to skim fees, and the cash-out end of laundering chains. The industry's own early diagnostic work recognized this clearly, classifying mobile money fraud according to whether the victim or perpetrator is the customer, the agent, the provider's employee or the system itself, and observing that agent-level fraud is both the most common and the least visible to head-office controls (Mudiri, 2013).

The third layer is the transactional and technological core, the switching, wallet-management and settlement systems operated by the mobile money provider and, increasingly, the application programming interfaces through which banks, fintechs and merchants connect to it. Interoperability between wallets, between providers and between wallets and banks has been a policy triumph, and Ghana's interoperability infrastructure is frequently cited as a continental model, but every new interconnection is also a new attack surface and a new route along which stolen value can be moved, layered and dissipated within minutes. The Bank of Ghana's 2025 reporting records that fraudulent withdrawals more than doubled year on year and that electronic money fraud rose by roughly a third even as older channels such as automated teller machine fraud declined, a pattern consistent with offenders following both the transaction volumes and the points of least resistance (Bank of Ghana, 2026). The final layer is the human layer, the customer, and it is here that the centre of gravity of mobile money fraud actually lies, because the great majority of successful attacks do not breach the technology at all. They persuade the victim to operate it against their own interest; a point developed at length in the next section.

Two features of this architecture deserve emphasis because they condition everything a forensic accountant or digital auditor can do. The first is that mobile money is cash-adjacent. Every fraudulent gain is convertible to anonymous physical cash at any of millions of agent points, usually within minutes of the predicate transaction, which compresses the window for detection and freezing to a degree unknown in card or correspondent-banking fraud. The second is that the evidentiary record, although voluminous, is fragmented across institutions that do not naturally share it. The transaction log sits with the mobile money provider, the call and SMS records with the network operator, the identity records with the registration authority, the complaint with the police or the economic crime agency, and the victim's narrative with the victim. Reconstructing a single fraud therefore requires assembling evidence across at least four custodians, each with its own retention practices, disclosure gateways and data protection obligations. Any framework that ignores this fragmentation will produce elegant methodology and empty courtrooms.

TYPOLOGIES OF MOBILE MONEY FRAUD

Customer-Facing Fraud and Social Engineering

The most prevalent category of mobile money fraud, by case volume in every jurisdiction that publishes data, is fraud perpetrated against customers through deception rather than through technical compromise. The repertoire is familiar to any practitioner in the field. Offenders send messages or place calls impersonating the provider, the regulator, a charity or a promotion, announcing a prize, a mistaken transfer that must be returned, a registration exercise or a security update, and they walk the victim through USSD prompts until the victim has authorized a transfer or disclosed a personal identification number. Variants include the false reversal request, in which the offender sends a counterfeit credit alert and then telephones the victim demanding the return of money that was never actually sent, and wangiri-style missed-call baiting that draws victims into premium or fraudulent interactions. Ghanaian exploratory research found this pattern precisely, identifying impersonation, false promotions and reversal scams as the dominant modes of attack and observing that weak customer awareness, rather than weak technology, is the principal enabling condition (Akomea-Frimpong et al., 2019). The criminological literature on cyber-enabled fraud reaches the same conclusion at a general level, namely that these offences succeed by exploiting cognitive shortcuts, authority cues, urgency and reciprocity, and that victimization is spread across the population rather than confined to the naive (Button & Cross, 2017). The consequences for victims in low-income settings are severe out of all proportion to the sums involved, a point made forcefully in Nigerian research on electronic fraud victims whose life savings, school fees and working capital were extinguished in single incidents (Tade & Adeniyi, 2017).

Identity-Layer Fraud: SIM Swap and Account Takeover

The second category attacks the identity layer directly. In a SIM swap fraud, the offender procures a replacement SIM for the victim's number, whether by presenting forged identity documents at a registration point, by socially engineering a customer-service

channel, or by corrupting an insider, and thereby inherits the victim's wallet, one-time passwords, and alerts. Investigators at Ghana's Economic and Organised Crime Office have publicly described forged national identity cards being used as the basis for fraudulent swaps, with victims discovering the takeover only when their own SIM is deactivated, by which time linked balances have been emptied and moved across networks. Account takeover of this kind is especially damaging where customers have linked bank accounts and banking applications to the compromised number, because the mobile number has become, in practice, a master credential for the victim's entire financial life. The Bank of Ghana's 2024 fraud report recorded a steep year-on-year escalation in identity theft and impersonation exposure within the banking sector, an escalation that moves in step with the growth of digital onboarding (Bank of Ghana, 2025). The forensic significance of this category is that it generates a rich technical trail, including the swap request record, the device and cell-site data of the new SIM, and the cascade of post-takeover transactions, but that trail is distributed between the network operator and the financial institutions and decays quickly if not preserved.

Agent-Level and Insider Fraud

The third category is fraud committed by, through or against agents and insiders. Agents commit fraud against customers by direct misappropriation of deposits, by manipulating transactions entrusted to them, by charging unauthorized fees and by harvesting registration data for later misuse. Customers and third parties commit fraud against agents with counterfeit cash, false credit alerts and staged reversals, and agent losses of this kind, though individually small, aggregate into a significant tax on the viability of the distribution network. More seriously still, corrupt insiders within providers and network operators sell customer data, process irregular swaps and reversals, and provide the access that turns opportunistic street fraud into organised, scalable crime. Ghanaian investigative reporting and official commentary have repeatedly identified insider collusion as a major aggravating factor in the fraud statistics, and the Bank of Ghana's reporting for 2025 records 219 staff of banks and specialized deposit-taking institutions implicated in fraud in a single year, a figure that had in fact improved substantially on the year before (Bank of Ghana, 2026). The global fraud examination literature consistently finds that occupational fraud is most often detected by tips rather than by audit, and that formal reporting mechanisms materially shorten fraud duration (Association of Certified Fraud Examiners, 2024), findings that carry directly into the mobile money context and that argue for treating whistleblowing channels and agent-level intelligence as core audit infrastructure rather than as peripheral compliance decoration.

Systemic Abuse: Laundering, Mule Networks and Cross-Border Flows

The final category consists of the use of the mobile money system as infrastructure for other crime, and it is the category with the most serious implications for financial integrity in the technical sense of that term. The velocity, ubiquity and cash-convertibility of mobile money make it attractive for the placement and layering stages of money laundering, for the rapid dispersal of proceeds through networks of recruited or fictitious mule wallets, and for the collection ends of romance fraud, investment fraud and business email compromise schemes whose victims may be on other continents. The Financial Action Task Force recognized at an early stage that new payment products of this kind present a distinctive risk profile, and recommended a risk-based response calibrated to transaction limits, identification regimes and monitoring capacity rather than the wholesale application of bank-style rules (Financial Action Task Force, 2013). Scholarly analysis of the Kenyan experience framed the resulting dilemma precisely, namely that the proportionate, tiered know-your-customer regimes that make inclusion possible are the very regimes that determined offenders' probe for weakness, so that financial inclusion and financial integrity must be pursued as a joint optimization rather than as a trade-off in which one simply yields to the other (Buku & Meredith, 2013). Continental threat assessments now consistently rank mobile-channel fraud and business email compromise among the most prevalent and most lucrative forms of cybercrime affecting African states (INTERPOL, 2024), and the sums recorded in national statistics, substantial as they are, understate the phenomenon because a large share of victims never report, whether from shame, from fatalism about recovery or from distance from the reporting institutions.

Three observations emerge from this typological survey and set the agenda for what follows. First, the centre of gravity of mobile money fraud is behavioural rather than technical, which means that a forensic and audit practice built exclusively around systems and records will systematically miss the mechanism of most offences. Second, the agent network is simultaneously the system's greatest asset and its most porous membrane, which means that the agent, and not only the corporate provider, must become a unit of audit attention in his or her own right. Third, the evidence of any given fraud is scattered across custodians and decays quickly, which means that evidentiary strategy cannot be an afterthought appended to investigation but must be designed into the assurance framework from the beginning. These observations motivate the theoretical reassessment to which the article now turns.

The Limits of Imported Theory: Rethinking the Fraud Triangle for African Mobile Money Ecosystems

Forensic accounting education and professional practice across Africa remain organised, to a remarkable degree, around a small canon of imported explanatory models. The oldest and most influential is the fraud triangle, distilled from Cressey's interviews with convicted embezzlers in mid-century America, which locates the genesis of fraud in the conjunction of a non-shareable financial pressure, a perceived opportunity and a rationalization that permits the offender to preserve a law-abiding self-image (Cressey,

1953). The triangle was later extended into a fraud diamond by the addition of capability, the recognition that opportunity is inert unless the offender possesses the position, competence and confidence to exploit it (Wolfe & Hermanson, 2004). These models have earned their longevity. They give auditors a disciplined vocabulary of risk factors, they underpin the fraud risk assessment requirements of the international auditing standards, and they retain genuine explanatory purchase for the insider frauds, cash suppressions and document forgeries that continue to afflict African banks and deposit-taking institutions. The difficulty is not that the triangle is wrong but that it is parochial, and the scholarly literature has said so with increasing directness. Critical reviews have observed that the triangle was derived from a specific offender population, the trusted occupational insider, and that it travels poorly to collusive fraud, to predatory and organised offending and to contexts far removed from the mid-century American firm (Free, 2015). Sociological work on fraud risk has gone further, arguing that the triangle survives less because of its explanatory power than because it is administratively convenient, a device that renders fraud governable by checklists (Power, 2013).

Three specific mismatches matter for mobile money. The first concerns the identity of the offender. The triangle models the trusted insider who occupies a position and betrays it, whereas the paradigmatic mobile money fraudster is an outsider, frequently organised, often operating across borders, who never held a position of trust within any audited entity and whose pressure, opportunity and rationalization are not observable through any internal control lens. For this predatory population, the relevant analytical questions are criminological rather than occupational. They concern recruitment into fraud economies, the social organization of offender networks, the marketplaces in which compromised data and mule wallets are traded, and the situational features of the payment system that make offences easy, quick and low-risk. Situational crime prevention, with its focus on increasing the effort and risk of offending and reducing its rewards, speaks more directly to USSD scams and SIM swaps than the triangle ever can, and a context-sensitive framework must make room for it.

The second mismatch concerns the unit of analysis. Audit methodology presumes an entity boundary within which controls operate and can be tested, but mobile money fraud arises in the seams between entities, between the network operator and the wallet provider, between the provider and its agents, between wallets and banks, and between all of these and the identity infrastructure of the state. An assurance model that stops at the corporate boundary certifies each fragment while the ecosystem as a whole remains unexamined. This is not a hypothetical concern. The SIM swap sequence described earlier traverses at least three institutional domains before the first fraudulent debit occurs, and in each domain, considered alone, the activity can appear routine. Only an ecosystem-level view, assembled from data across custodians, reveals the offence pattern, and no single incumbent has both the visibility and the incentive to assemble it unaided.

The third mismatch is cultural and socioeconomic, and it must be stated with care because the point is easily caricatured. The claim is not that African users are peculiarly credulous, a proposition the victimology literature refutes, but that the trust architecture of African financial life differs in ways that both explain mobile money's success and shape its fraud ecology. Mobile money prospered in Ghana and its neighbours in part because it grafted onto existing informal financial institutions and habits, including the susu traditions of rotating and collected savings in which value is routinely entrusted to known intermediaries, and empirical work on adoption confirms the continuity between those traditions and the new channel (Osei-Assibey, 2015). Communitarian accounts of African moral life, of the kind developed in the Ghanaian philosophical tradition, describe personhood and obligation as constituted in community, with trust extended through webs of relation rather than through institutional verification (Gyekye, 1997). That relational trust is a genuine social asset, and it is exactly the asset that impersonation fraud converts into a vulnerability, because the fraudster's telephone call succeeds by simulating precisely the relational cues, the familiar greeting, the invocation of a shared institution, the performance of helpfulness, on which everyday economic cooperation legitimately depends. A fraud framework that treats users as isolated rational actors defended only by passwords will misread both the mechanism of victimization and the most promising avenues of prevention, which run through the same communal channels that the offenders exploit, including agent forums, market associations, religious congregations and community radio. Anthropological work on payment systems has long insisted that money technologies are social technologies before they are anything else (Maurer, 2012), and fraud control must be designed accordingly.

None of these counsels the abandonment of the received models. For insider fraud within providers and banks, the triangle and diamond remain serviceable, and the general fraud examination literature, with its accumulated knowledge of red flags, interviewing and evidence handling, remains foundational (Albrecht et al., 2019). The argument is for theoretical pluralism disciplined by context. The occupational models should govern the insider domain, situational and network criminology should govern the predatory domain, and an ecosystem perspective attentive to African trust architectures should govern the whole. It is on this pluralist foundation that the framework proposed in the next section is built.

A Context-Sensitive Framework for Forensic Accounting and Digital Auditing of Mobile Money Ecosystems

The framework proposed here is organised around five pillars, each defining a domain of forensic and audit attention, together with a cross-cutting evidentiary spine that disciplines all five. It is offered as a practitioner's architecture rather than as a formal model, and it is deliberately statute-aware, taking Ghana's legal regime as its worked example while remaining adaptable to the cognate

regimes of other African jurisdictions. The five pillars are transactional forensics, agent network assurance, behavioural and social engineering analysis, institutional and identity-layer assurance, and communal engagement and restitution. The evidentiary spine concerns admissibility, chain of custody and inter-institutional data assembly. Each is developed in turn.

Pillar One: Transactional Forensics and Continuous Digital Auditing

The first pillar applies data-analytic methods to the transaction log itself, which is the one place where every mobile money event, however deceptively procured, must eventually leave a trace. The core practices are familiar from modern digital auditing but require recalibration for the mobile money environment. Full-population analysis should replace sampling, since the marginal cost of testing every transaction in a digital ledger is trivial and fraud in this environment hides in patterns rather than in individual anomalies. The pattern library must be built from the typologies described earlier rather than from bank-derived templates, and it should include, at a minimum, structuring behaviour just beneath tier limits and reporting thresholds, bursts of incoming transfers to newly registered wallets followed by immediate cash-out, fan-in and fan-out topologies characteristic of mule dispersal, transaction sequences that follow SIM replacement events within short windows, reversal requests correlated with counterfeit alert campaigns, dormant wallets that awaken to receive single large credits, and velocity anomalies at particular agent tills. Graph analytics deserve particular emphasis because mobile money fraud is a network phenomenon, and the relevant object of analysis is often not the transaction but the subgraph, the community of wallets, devices, SIMs, and agent tills among which value circulates. Machine-assisted anomaly detection has a place, but the auditor must retain interpretive command of the models, both because opaque scoring will not survive adversarial scrutiny in court and because model performance degrades quickly as offenders adapt. The output of this pillar should be conceived not as a periodic report but as a continuous monitoring capability whose alerts feed both the provider's operational fraud desk and the forensic function's case-building process.

Pillar Two: Agent Network Assurance

The second pillar elevates the agent to a primary unit of audit attention, a deliberate departure from frameworks that treat the agent network as a distribution detail. Agent-level assurance has three components. The first is analytic, a per-till risk profile assembled from the transaction log, comprising float turnover patterns, deposit-splitting incidence, registration volumes and quality, reversal frequencies, after-hours activity, and the till's position within the network graphs generated under pillar one, so that outlier tills are surfaced for attention on evidence rather than on rumours. The second component is physical and procedural, an inspection programme adapted from cash-count and branch-audit traditions to the realities of a kiosk economy, covering identity verification practice at the till, the handling and secrecy of customer personal identification numbers during assisted transactions, the security of registration materials, and the reconciliation of electronic float against physical cash. The third component is relational, and it is the one most often neglected. Agents are the richest human intelligence source in the ecosystem, the first to hear of new scam scripts circulating in a market town and the first to be approached by launderers seeking compliant cash-out points, and a well-designed assurance programme therefore builds structured channels through which agent observations flow to the fraud function, protects agents who report, and feeds anonymized intelligence back to the network so that agents become sensors and allies rather than merely subjects of inspection. The industry's foundational diagnostic on mobile money fraud reached this conclusion essentially more than a decade ago (Mudiri, 2013), and the intervening years of loss data suggest the lesson has still not been fully institutionalized.

Pillar Three: Behavioural and Social Engineering Analysis

Because most mobile money fraud is accomplished through the victim rather than through the system, the forensic function must treat behavioural evidence as first-class evidence. This pillar has an investigative face and a preventive face. On the investigative face, complaint narratives, scam scripts, voice recordings, message content and the timing relationships between contact events and transaction events should be captured in structured form and mined with the same seriousness as the transaction log, because script families identify offender groups, shared telephone numbers and message templates link cases across victims and across networks, and the evolution of scripts maps the offenders' response to control changes. On the preventive face, the analysis of victimization patterns should drive targeted, evidence-based education rather than generic awareness campaigns, directing the right warning to the right population through the right channel, which in the African context frequently means local-language radio, market association meetings, congregational announcements and the agents themselves rather than corporate media. The victimology literature is clear that shame and self-blame suppress reporting and prolong offender careers (Button & Cross, 2017), so complaint channels must be designed to be reachable by basic-phone users, free of cost, and free of humiliation, and the institutional habit of treating defrauded customers as negligent authors of their own loss should be recognized as itself a fraud-enabling control weakness, since every unreported case is intelligence forgone.

Pillar Four: Institutional and Identity-Layer Assurance

The fourth pillar addresses the provider, the network operator and the identity infrastructure on which both depend. Within providers and operators, the classical apparatus of occupational fraud control retains its force, including segregation of duties around swap

processing, reversals and float management, privileged-access monitoring, mandatory leave, vetting of staff in sensitive roles, and protected whistleblowing channels, whose effectiveness the global data consistently confirm (Association of Certified Fraud Examiners, 2024). To this must be added identity-layer assurance, which audits the integrity of the processes by which SIMs are issued, replaced and swapped, and by which customers are onboarded against national identity databases. The auditable questions are concrete. What proportion of swap requests are verified biometrically against the national register rather than documentarily, what controls detect clustering of swaps at particular registration points or under particular staff credentials, what latency separates a swap event from the reactivation of financial services on the new SIM, and does that latency give the true owner a fighting chance to object? A cooling-off interval between SIM replacement and the restoration of wallet and banking functionality, with active notification to registered alternative contacts, is among the cheapest and most effective structural controls available, and testing its operation should be a standard element of any digital audit of a mobile financial service. Regulatory developments in Ghana, including the strengthening of verification against the national identity database and the central bank's revision of its cyber and information security directives, point in this direction, and the forensic profession should regard the testing of these controls as squarely within its remit rather than as the exclusive province of information technology audit (Bank of Ghana, 2025).

Pillar Five: Communal Engagement, Recovery and Restitution

The fifth pillar draws the consequence of the cultural analysis offered earlier. If trust in African financial life is relational and communal, then the restoration of integrity after fraud must also run through relational and communal channels, and a framework that ends at detection and prosecution leaves most of the harm unaddressed. Three practices belong here. The first is rapid interdiction and recovery, which requires pre-agreed protocols among providers, operators and law enforcement for the freezing of suspect wallets across networks within the minutes that matter, since the Ghanaian data showing recovery rates of roughly five per cent of value at risk (Bank of Ghana, 2026) are as much an indictment of interdiction speed as of investigative capacity. The second is restitution practice, the deliberate design of compensation and loss-allocation rules among provider, agent and customer that are publicly known and consistently applied, because opaque and discretionary loss allocation corrodes the confidence on which the entire inclusion project depends. The third is the enlistment of communal institutions in prevention and in the rehabilitation of trust, which returns the analysis to the communitarian insight that the individual is protected through the community (Gyekye, 1997). None of this is soft decoration around the hard core of forensics. Confidence is the asset that mobile money monetizes, and its maintenance is therefore a proper object of assurance in exactly the way that capital adequacy is for a bank.

The Evidentiary Spine: Admissibility, Custody and Data Assembly

Running through all five pillars is the discipline of evidence, and here the framework is deliberately legalistic, because a forensic practice whose product cannot be admitted and believed in court is an expensive form of description. In Ghana, the admission of electronic records is governed by the Electronic Transactions Act, 2008 (Act 772), read with the general law of evidence under the Evidence Act, 1975 (NRCD 323), and the statutory scheme ties the weight of an electronic record to the reliability of the manner in which it was generated, stored and communicated, and to the integrity of the system that produced it. The practical consequences for the digital auditor are direct. Transaction logs, swap records and cell-site data should be extracted under documented procedures that preserve hash-verifiable integrity, the operational custodians who can speak to the generating systems should be identified at the moment of extraction and not on the eve of trial, and the analytic transformations applied to raw data should be recorded step by step so that the path from source record to expert conclusion is reproducible before a tribunal. The surrounding statutory environment, including the Payment Systems and Services Act, 2019 (Act 987), which brought payment service providers within the central bank's regulatory perimeter, the Cybersecurity Act, 2020 (Act 1038), which establishes the incident-reporting and sectoral response architecture, the Anti-Money Laundering Act, 2020 (Act 1044), which imposes the suspicious transaction reporting obligations on which pillar one's analytics ultimately feed, and the Data Protection Act, 2012 (Act 843), which conditions every act of inter-institutional data assembly, must be treated as part of the auditor's method rather than as background regulation. Cognate structures exist across the continent, and in each jurisdiction the framework calls for the same exercise, the mapping of the forensic workflow onto the local evidentiary and data protection statutes before the first byte of evidence is collected.

Taken together, the five pillars and the evidentiary spine restate the task of forensic accounting and digital auditing in this environment. The object of assurance is not an entity but an ecosystem, the unit of analysis is as often a network or a human interaction as a ledger entry, and the test of success is not the elegance of the working papers but the integrity, in every sense, of the channel through which a market woman in Makola or a farmer in Karaga now holds and moves the whole of her liquid wealth.

IMPLICATIONS FOR PROFESSIONAL PRACTICE

For Forensic Accountants and Fraud Examiners

For the individual practitioner, the framework implies a widened competence set and a reordered workflow. The competence set now necessarily includes data analytics at the level of full-population testing and network analysis, working familiarity with telecommunications records, including SIM lifecycle events and cell-site data, and enough command of the local electronic evidence

statutes to design collection procedures that will survive challenge. It also includes skills that the discipline has historically undervalued, above all the structured interviewing of victims and agents in local languages and with cultural fluency, since in this fraud ecology the human narrative is frequently the only direct evidence of the deceptive mechanism, the transaction log recording only its financial consequence. The reordered workflow begins from the recognition that evidence in this environment decays in days rather than years. The first hours after a complaint should be devoted to preservation requests across all relevant custodians, the provider, the network operator, the receiving institutions along the dissipation chain and the identity authority, and only then to the leisurely work of analysis. Engagement letters and investigative protocols should provide in advance for this multi-custodian reality, and practitioners who serve providers should press for standing data-sharing and freezing arrangements to be concluded before the cases arrive rather than negotiated during them.

For Internal Audit and Risk Functions Within Providers

For internal audit functions within mobile money providers and the banks connected to them, the framework implies an audit universe redrawn around the five pillars. The annual plan should treat the agent network, the SIM lifecycle interface and the social engineering complaint stream as auditable entities with their own risk assessments, rather than burying them within generic operations audits. Key risk indicators should be built from the pattern library of pillar one and reported to board level with the same discipline as credit and liquidity indicators, because the fraud loss and confidence data reviewed in this article describe a risk that is material to the franchise and not merely to the customer. Internal audit should also test the institution's posture toward victims as a control in its own right, examining whether complaint channels are genuinely reachable by the customer base, whether loss-allocation decisions follow published principles, and whether complaint intelligence is actually mined and acted upon, since a fraud desk that treats complaints as a public relations burden is discarding its richest detection asset.

For Educators and the Profession

For the universities and professional bodies that train Africa's accountants, auditors and financial investigators, the implication is curricular. Forensic accounting syllabi across the continent still transmit the occupational fraud canon of the North American textbooks with little adaptation, and graduates meet the agent kiosk, the USSD scam and the SIM swap for the first time in practice rather than in the classroom. A context-sensitive curriculum would set the received canon alongside the typologies and statutes of the students' own jurisdictions, would teach transaction analytics on realistic mobile money datasets, and would treat the sociology of trust in African economies as examinable professional knowledge rather than as humanities decoration. The research community, for its part, confronts an unusual opportunity, because the mobile money ecosystem generates data of a richness that fraud researchers in cash economies could never have imagined, and partnerships between providers, regulators and universities, structured to protect privacy under the applicable data protection statutes, could give African scholarship the empirical leadership of a field whose subject matter is, for once, centred on the continent.

Implications for Regulation and Policy

Four regulatory implications follow from the analysis. The first concerns disclosure. The Bank of Ghana's practice of publishing annual fraud statistics disaggregated by sector and typology (Bank of Ghana, 2025, 2026) is, by continental standards, admirably transparent, and its emulation elsewhere would give researchers, practitioners and the public the shared factual baseline without which policy debate degenerates into anecdote. Disclosure regimes should, however, evolve toward standardized typologies and toward the publication of recovery and interdiction performance, since what is measured against a five per cent recovery rate is likely, eventually, to improve. The second implication concerns interdiction architecture. The minutes-long window between fraudulent debit and cash-out means that the decisive regulatory intervention is not heavier ex post punishment but the construction of real-time, cross-network freezing and recall protocols with clear legal footing, defined liability rules and audited response times, and central banks are the natural conveners of such protocols. The third implication concerns the identity layer. Because the SIM has become a financial credential, SIM lifecycle regulation is financial regulation, and the verification of swap and replacement events against national biometric registers, together with mandated cooling-off intervals before financial functionality revives on a replaced SIM, should be treated as core financial integrity measures and their operation subjected to independent audit. The fourth implication concerns proportionality. The Financial Action Task Force's risk-based approach to new payment products (Financial Action Task Force, 2013) remains the correct frame, and the lesson of the inclusion literature is that controls which price the poor out of the formal channel do not eliminate risk but merely return it to the shadows of the cash economy, so that every proposed control should be tested not only for its effect on fraud but for its effect on access, with the joint optimization of integrity and inclusion, in the spirit urged by Buku and Meredith (2013), adopted as the explicit regulatory objective.

Limitations and Directions for Future Research

The limitations of this article suggest its research agenda. The analysis rests principally on regulatory disclosures, industry reporting and the published literature, and each of these sources undercounts the phenomenon differently: the regulatory data because reporting is incomplete and unevenly enforced, the industry data because providers face obvious disincentives to candour, and the

literature because the empirical study of mobile money fraud remains thin relative to the scale of the subject. The framework proposed here is, accordingly, an architecture derived from typology and doctrine rather than a model validated against outcome data, and its five pillars stand as hypotheses inviting test. Field validation studies within providers willing to open their loss and complaint data to researchers, victimization surveys designed to measure the dark figure of unreported fraud, evaluations of specific controls such as swap cooling-off intervals and agent intelligence channels, and comparative doctrinal work on the admissibility of mobile money records across African evidence regimes would each carry the field forward. There is also a genuinely theoretical task awaiting African scholarship, the construction of a fraud explanation that begins from African economic sociology rather than arriving at it by way of exception, and the intellectual resources for that task, in the continent's philosophical and empirical traditions, are considerably richer than the imported textbooks suggest.

CONCLUSION

Mobile money has given Africa something close to a second, parallel financial system, built in under two decades, reaching populations the first system never served, and now moving well over a trillion dollars a year across the continent. The integrity of that system is under sustained attack, not principally through its technology but through its people, its agents and the seams between its institutions, and the professional disciplines charged with defending financial integrity have been slow to refit their methods to the terrain. This article has argued that the refit requires more than incremental adjustment. It requires a change in the unit of analysis from the entity to the ecosystem, a theoretical pluralism that sets situational and network criminology alongside the occupational fraud canon, an audit practice that treats the agent till, the SIM lifecycle and the victim's narrative as first-class objects of assurance, and an evidentiary discipline mapped in advance onto the electronic transactions, cybersecurity and data protection statutes of each jurisdiction. The five-pillar framework proposed here is offered in that spirit, as a practitioner's architecture for a distinctly African problem that African forensic accountants, auditors, investigators and scholars are best placed to solve. The stakes are larger than loss figures. Every successful scam converts a unit of the communal trust on which the inclusion project was built into a unit of the cynicism that could yet unbuild it, and the defence of that trust is the true object of the work.

REFERENCES

1) Akomea-Frimpong, I., Andoh, C., Akomea-Frimpong, A., & Dwomoh-Okudzeto, Y. (2019). Control of fraud on mobile money services in Ghana: An exploratory study. *Journal of Money Laundering Control, 22*(2), 300–317. https://doi.org/10.1108/JMLC-03-2018-0023
2) Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimbelman, M. F. (2019). *Fraud examination* (6th ed.). Cengage Learning.
3) Ali, G., Ally Dida, M., & Elikana Sam, A. (2020). Two-factor authentication scheme for mobile money: A review of threat models and countermeasures. *Future Internet, 12*(10), 160. https://doi.org/10.3390/fi12100160
4) Anti-Money Laundering Act, 2020 (Act 1044) (Ghana).
5) Aron, J. (2018). Mobile money and the economy: A review of the evidence. *The World Bank Research Observer, 33*(2), 135–188. https://doi.org/10.1093/wbro/lky001
6) Association of Certified Fraud Examiners. (2024). *Occupational fraud 2024: A report to the nations*. https://www.acfe.com/report-to-the-nations
7) Bank of Ghana. (2025). *Banks, SDIs and PSPs 2024 fraud report* (Notice No. BG/GOV/SEC/2025/09). https://www.bog.gov.gh
8) Bank of Ghana. (2026). *Banks, SDIs and PSPs 2025 fraud report*. Financial Stability Department. https://www.bog.gov.gh
9) Buku, M. W., & Meredith, M. W. (2013). Safaricom and M-PESA in Kenya: Financial inclusion and financial integrity. *Washington Journal of Law, Technology and Arts, 8*(3), 375–400.
10) Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. Routledge. https://doi.org/10.4324/9781315679877
11) Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press.
12) Cybersecurity Act, 2020 (Act 1038) (Ghana).
13) Data Protection Act, 2012 (Act 843) (Ghana).
14) Demirgüç-Kunt, A., Klapper, L., Singer, D., & Ansar, S. (2022). *The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19*. World Bank. https://doi.org/10.1596/978-1-4648-1897-4
15) Electronic Transactions Act, 2008 (Act 772) (Ghana).
16) Evidence Act, 1975 (NRCD 323) (Ghana).
17) Financial Action Task Force. (2013). *Guidance for a risk-based approach: Prepaid cards, mobile payments and internet-based payment services*. FATF. https://www.fatf-gafi.org
18) Free, C. (2015). Looking through the fraud triangle: A review and call for new directions. *Meditari Accountancy Research, 23*(2), 175–196. https://doi.org/10.1108/MEDAR-02-2015-0009

19) GSMA. (2025). *The state of the industry report on mobile money 2025*. GSMA. https://www.gsma.com/sotir/
20) GSMA. (2026). *The state of the industry report on mobile money 2026*. GSMA. https://www.gsma.com/sotir/
21) Gyekye, K. (1997). *Tradition and modernity: Philosophical reflections on the African experience*. Oxford University Press.
22) INTERPOL. (2024). *African cyberthreat assessment report 2024*. INTERPOL. https://www.interpol.int
23) Jack, W., & Suri, T. (2014). Risk sharing and transactions costs: Evidence from Kenya's mobile money revolution. *American Economic Review, 104*(1), 183–223. https://doi.org/10.1257/aer.104.1.183
24) Maurer, B. (2012). Mobile money: Communication, consumption and change in the payments space. *Journal of Development Studies, 48*(5), 589–604. https://doi.org/10.1080/00220388.2011.621944
25) Morawczynski, O. (2009). Exploring the usage and impact of "transformational" mobile financial services: The case of M-PESA in Kenya. *Journal of Eastern African Studies, 3*(3), 509–525. https://doi.org/10.1080/17531050903273768
26) Mudiri, J. L. (2013). *Fraud in mobile financial services*. MicroSave. https://www.microsave.net
27) Osei-Assibey, E. (2015). What drives behavioral intention of mobile money adoption? The case of ancient susu saving operations in Ghana. *International Journal of Social Economics, 42*(11), 962–979. https://doi.org/10.1108/IJSE-09-2013-0198
28) Payment Systems and Services Act, 2019 (Act 987) (Ghana).
29) Power, M. (2013). The apparatus of fraud risk. *Accounting, Organizations and Society, 38*(6–7), 525–543. https://doi.org/10.1016/j.aos.2012.07.004
30) Suri, T., & Jack, W. (2016). The long-run poverty and gender impacts of mobile money. *Science, 354*(6317), 1288–1292. https://doi.org/10.1126/science.aah5309
31) Tade, O., & Adeniyi, O. (2017). "They withdrew all I was worth": Automated teller machine fraud and victims' life chances in Nigeria. *International Review of Victimology, 23*(3), 313–324. https://doi.org/10.1177/0269758017704027
32) Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal, 74*(12), 38–42.