



MoMo
from MTN

Uniting Against Digital Fraud

**Strengthening Ecosystem Collaboration in
Ghana's Digital Financial Services Sector**

A Strategic White Paper from the MobileMoney Fintech
Partner Exchange



MobileMoney Fintech LTD (MMFL)
April 2026

Table of Contents

1. Executive Summary	1
2. Introduction and Background	2
3. Evolution of Ghana's Digital Financial Ecosystem	2
4. Fraud Landscape Analysis	3
5. Forum Overview	4
6. Methodology	4
7. Key Themes Emerging from the Forum	5
• Speed Disparity	5
• Channel Security	5
• Legal and Institutional Fragmentation	5
• The Human Dimension	5
• Role of MobileMoney Fintech LTD	5
8. Executive Summary	6
9. Introduction and Background	6
• Policy Innovation	6
• Collaborative Approaches	6
10. Stakeholder Recommendations	7
• Role of MobileMoney Fintech LTD	7
• Governance Platforms	7
11. Implementation Pathways	7
• Near-Term Priorities	7
• Medium-Term Efforts	7
• Long-Term Transformation	7
12. Implications and Expected Impact	8
• Economic Benefits	8
• Trust and Confidence	8
13. Regional and Global Comparisons	8
• Regional Context	8
• Global Insights	8
14. Comprehensive Fraud Prevention Tactics	09
• Multifaceted Strategies	09
15. Technology Innovations in Fraud Prevention	09
• Blockchain Technology	09
• Machine Learning Algorithms	09
• Identification Techniques	09
16. The Importance of User Education	10
• Empowering Consumers	10
• Engaging Communities	10
17. Legal and Regulatory Framework Gaps	10
• Current State of Regulation	10
• Proposed Legal Framework Enhancements	10
18. Future Trends in Digital Finance and Fraud	10
• Evolving Threats	10
• Adaptive Strategies	10
19. Implementation Challenges and Mitigation Strategies	10
• Anticipated Challenges	10
• Mitigation Strategies	10
20. Conclusion	11
21. Acknowledgements	11
22. White Paper/ Project Team	11

Executive Summary

Ghana's digital financial ecosystem has entered a critical phase in its development. Over the past decade, mobile money and fintech innovations have expanded financial inclusion, accelerated digital commerce, and strengthened economic participation across all segments of the Ghanaian society. Digital financial services function now as essential national infrastructure, supporting millions of daily transactions and underpinning significant portions of economic activity across the entire country. Indeed, today, it is almost impossible to imagine the Ghanaian economy without the transformative impact of mobile money.

As scalability has increased, however, systemic risks have evolved in parallel. Digital fraud has transitioned from isolated incidents to coordinated, technology-enabled operations capable of exploiting institutional and operational gaps across interconnected platforms. Fraud is no longer confined to individual use cases or organizational boundaries; it moves across the ecosystem, affecting multiple institutions simultaneously and exposing structural weaknesses in coordination and response mechanisms.

In response to these emerging risks, MobileMoney Fintech LTD convened the Fintech Partner Exchange in April 2026, bringing together senior leaders from banks, fintech companies, payment service providers, regulatory authorities, law enforcement agencies, and agent networks. The forum aimed to examine shared vulnerabilities, strengthen institutional alignment, and identify collective strategies to enhance ecosystem resilience.

A central insight emerged from stakeholder engagement: the ecosystem operates at mismatched speeds. Financial transactions are executed instantaneously through advanced digital infrastructure, while fraud response mechanisms remain largely sequential, manual, and institutionally fragmented. This imbalance creates operational advantages for fraud actors and perpetrators, who exploit delays in coordination and decision-making.

Participants further observed that collaboration across institutions already exists but is predominantly informal, relying on personal relationships rather than standardized systems or legally supported intelligence-sharing frameworks. While such cooperation has mitigated losses, it is insufficient for an ecosystem operating at national scale.

The continued reliance on USSD transaction channels also represents a structural vulnerability. Although USSD has been instrumental in driving financial inclusion, its security limitations are increasingly apparent in an environment characterized by sophisticated fraud techniques. Transition toward secure application-based channels thus represents both a modernization priority and a cybersecurity imperative.

Stakeholders emphasized that human actors, particularly agents and consumers, remain central to ecosystem security. Social engineering attacks continue to bypass technical safeguards, highlighting the need for improved tools, faster response mechanisms, and coordinated education initiatives.

The forum concluded that sustainable ecosystem security requires a shift from institution-centric defense models toward coordinated, intelligence-led collaboration. Priority actions include; i) establishing a joint fraud command center; ii) enabling real-time intelligence sharing; iii) accelerating secure digital adoption; iv) deploying predictive analytics, and v) strengthening frontline protection mechanisms. Collective implementation of these measures will reinforce trust in Ghana's digital financial system, support continued innovation, and position the country as a regional leader in secure digital finance.

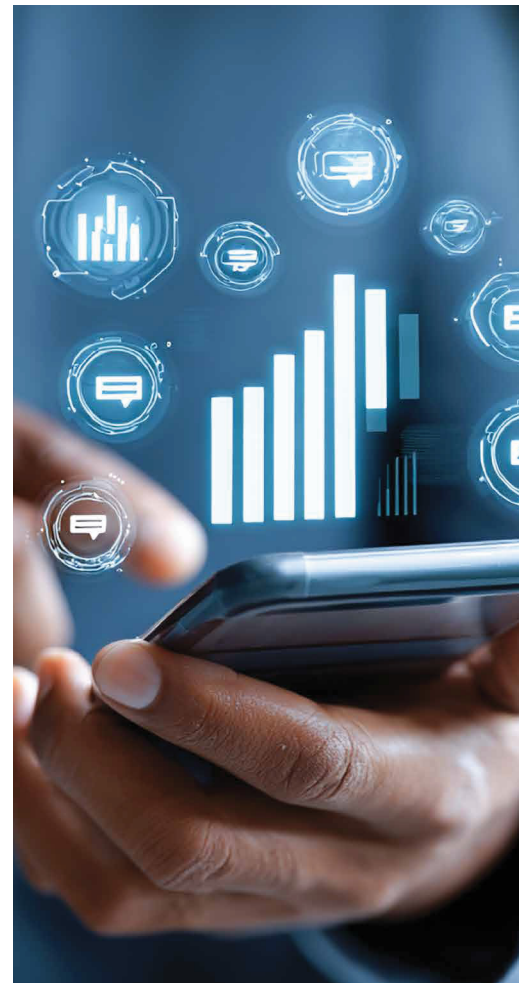
Introduction and Background

Ghana's digital financial services sector has become a cornerstone of economic transformation, representing a vital tool for socio-economic growth. Since the introduction of mobile money by MTN Ghana in 2009, mobile money platforms have expanded access to financial services, enabled microenterprise growth, facilitated remittances, and supported digital payments across urban and rural communities alike. The ecosystem's expansion reflects sustained collaboration and partnerships among telecommunications providers, financial institutions, regulators, and technology innovators.

MobileMoney Fintech LTD occupies a central role within this ecosystem, operating infrastructure that processes billions of transactions annually and supports economic activity at a national scale. The reliability and security of this infrastructure are therefore directly linked to broader economic stability. Rapid growth has increased interdependence among ecosystem participants. Transactions frequently traverse multiple institutional environments, including banks, fintech platforms, merchants, agents, and telecommunications networks. As connectivity deepens, vulnerabilities within one node can propagate rapidly across the system.

Simultaneously, fraud methodologies have become more sophisticated, combining technological exploitation with behavioural manipulation. These developments challenge traditional institutional defense models designed around organizational boundaries rather than ecosystem interconnectedness.

The Fintech Partner Exchange was convened to address this emerging reality by encouraging structured dialogue among decision-makers capable of driving coordinated change. The forum sought to align stakeholders around shared risks and establish a foundation for collective action that ensures safety and security in the digital financial ecosystem.



Evolution of Ghana's Digital Financial Ecosystem

The expansion of digital financial services in Ghana has progressed through distinct stages characterized by increasing complexity and integration. Early adoption focused primarily on access expansion, utilizing USSD technology to enable basic financial transactions on feature phones. This phase prioritized reach and affordability, successfully extending services to previously unbanked populations. Subsequent development emphasized interoperability, connecting mobile money platforms with banking systems and enabling seamless transfers across networks. This integration significantly increased transaction volumes while improving user convenience, but it also expanded the pathways through which fraudulent activity could occur.



The ecosystem later evolved toward digital commerce enablement, with merchants, small businesses, and service providers increasingly adopting mobile payments. Digital wallets began to function not merely as transfer tools but as broader financial platforms integrating savings, lending, insurance, and payment functionalities, further solidifying the important role that fintech plays in the Ghanaian economy.

Each phase strengthened economic participation while simultaneously increasing system complexity. Fraud methodologies evolved in parallel, adapting to new capabilities introduced by technological innovation. As the ecosystem matured, fraud actors have shifted from sporadic, opportunistic schemes to coordinated operations capable of exploiting scale, sophistication and mimicking or mirroring legitimate platforms to perpetrate fraud.

Fraud Landscape Analysis

Digital fraud within Ghana's financial ecosystem increasingly reflects global cybercrime dynamics adapted to local contexts. Fraud actors combine technological exploitation with behavioural manipulation, enabling attacks that bypass traditional security controls. Social engineering remains the most prevalent fraud vector, relying on deception rather than technical intrusion. Fraudsters impersonate trusted institutions or authority figures, persuading users to disclose credentials or authorize transactions. SIM swap fraud and account takeover schemes further enable unauthorized access to digital wallets.

Emerging trends indicate increasing professionalization among fraud networks. Automation tools allow fraudsters to scale outreach efforts, while synthetic identity techniques complicate verification processes. Cross-border coordination enables rapid movement of funds beyond immediate recovery channels, making it difficult to trace funds back to the original source. These developments underscore the necessity for predictive, intelligence-led approaches capable of identifying risk patterns before significant financial losses occur.

Moreover, the toll of fraud on individuals and organizations alike extends beyond mere financial losses; it can severely undermine public confidence in digital financial services, stymying the very financial inclusion that these platforms aim to promote.

Forum Overview



The Fintech Partner Exchange took place on April 2, 2026, at the Mövenpick Ambassador Hotel in Accra. The event was designed as a high-level engagement platform that combined keynote presentations, expert discussions, moderated panel dialogue, and stakeholder interaction sessions, promoting an environment conducive to critical dialogue among participants.

Representatives from the full spectrum of Ghana's digital financial ecosystem attended, including commercial banks, payment service providers, regulatory agencies, law enforcement institutions, telecommunications stakeholders, agent associations, and corporate partners. Senior executives and operational leaders were deliberately engaged to ensure discussions reflected implementation realities rather than theoretical perspectives, thereby grounding ideas in practical applicability.

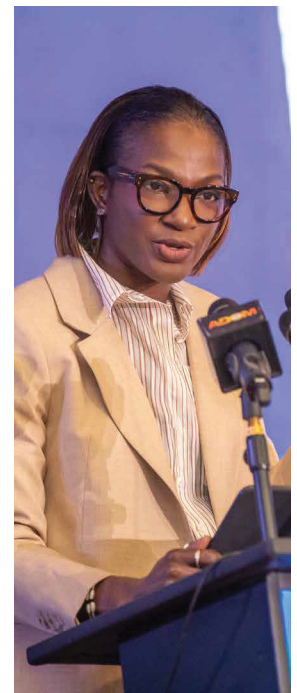


The central panel discussion, themed "Uniting Against Fraud: Strengthening Ecosystem Collaboration," focused on operational experiences, emerging fraud patterns, and coordination challenges across institutions. Discussions emphasized shared accountability and solution-oriented dialogue rather than institutional attribution. The forum reinforced the significance of structured collaboration as a prerequisite for sustainable ecosystem growth.

Methodology

This white paper synthesizes insights derived from structured stakeholder dialogue conducted during the forum. To encourage and facilitate cross-sector participation, discussions were moderated to maintain an analytical focus on systemic issues.

Stakeholder perspectives were analyzed alongside ecosystem performance data and operational observations to identify recurring themes, areas of convergence, and strategic priorities. The analysis prioritizes synthesis and interpretation rather than verbatim reporting, translating participant insights into ecosystem-level conclusions. While the findings reflect the perspectives of participating stakeholders, they provide a representative assessment of current challenges facing Ghana's digital financial ecosystem.



Key Themes Emerging from the Forum



Speed Disparity

A dominant theme was the widening disparity between the operational speed of fraud and institutional response capabilities. Fraud actors increasingly operate through coordinated digital networks leveraging automation and artificial intelligence, while institutional defenses remain predominantly reactive. Participants concurred that reliance on post-incident intervention is increasingly unsustainable; predictive, intelligence-led approaches must become the new standard.

Channel Security

Channel security emerged as a second critical issue. Despite increasing smartphone penetration, transaction volumes remain heavily concentrated on USSD channels. While essential to early inclusion efforts, these channels lack advanced authentication mechanisms available in application-based environments. Stakeholders thus emphasized an accelerated migration toward secure digital applications as a risk-reduction priority.

Legal and Institutional Fragmentation

Legal and institutional fragmentation also constrains response effectiveness. Fraud investigations often require formal procedural steps before information can be shared across institutions. Although these safeguards protect consumer rights, they can delay interventions during active fraud incidents. Participants highlighted the need for frameworks that enable rapid cooperation while maintaining data protection standards.

The Human Dimension

The human dimension of fraud prevention featured prominently in discussions. Agents and consumers remain primary targets of social engineering attacks, underscoring the importance of strengthening frontline capacity through improved tools, streamlined support processes, and sustained public education.

Role of MobileMoney Fintech LTD

Finally, stakeholders recognized an evolving ecosystem dynamic in which MobileMoney Fintech LTD's role is shifting from being a Fintech market leader to enabling the ecosystem and anchoring sustainable partnerships to drive economic growth and financial trust rather than platform dominance alone. Long-term resilience depends on shared solutions and collective accountability among all participants.



Key Challenges Identified

The forum identified structural, technological, behavioural, and risk-related challenges hampering effective cohesive response to fraud.

- Institutional silos limit visibility across transaction chains, obstructing comprehensive risk assessment.
- Data asymmetry restricts the capacity of initiating platforms to evaluate recipient risk profiles in real-time, creating exploitable gaps.
- Technological limitations persist due to uneven adoption of advanced analytics and reliance on legacy transaction channels.
- Behavioural factors, including credential sharing and operational pressures on agents, continue to weaken technical safeguards.

Meanwhile, fraud itself is evolving rapidly, integrating artificial intelligence, synthetic identities, and cross-border coordination. These trends significantly increase the urgency for coordinated ecosystem responses to fraud that can undermine confidence in financial systems.



Opportunities and Strategic Insights

Despite these challenges, stakeholders highlighted substantial opportunities to strengthen ecosystem resilience. Advances in behavioural analytics and machine learning present channels toward predictive fraud prevention capable of interrupting suspicious activity before significant financial losses occur. Intelligence sharing between ecosystem participants i.e. Banks, EMIs and PSPs can also enhance detection and mitigate losses from identified fraud incidents.

Policy Innovation

Policy innovation represents a critical opportunity for ensuring all Institutional Partners maintain standardized anti-financial crime mechanisms and are equipped to resolve fraud incidents especially where attacks traverse multiple platforms. Legally supported intelligence-sharing frameworks where Regulators define the scope, conditions and methods for sharing could enable rapid collaboration while preserving privacy protections.

Coordinated public education initiatives would further reduce vulnerability to social engineering attacks, addressing the human element of fraud.

Collaborative Approaches

Participants asserted that collaboration itself constitutes a strategic asset. Shared investment in ecosystem security infrastructure offers a scalable approach to risk reduction while supporting continued innovation. Emphasizing collaboration will not only fortify defenses but also catalyze a shared sense of responsibility among all participants.

Stakeholder Recommendations

Stakeholders emphasized the necessity for coordinated action across institutional roles. Regulatory authorities are well-positioned to enable secure intelligence-sharing frameworks and standardized reporting mechanisms. Financial institutions and fintech firms must integrate collaborative detection systems and invest in predictive analytics capabilities.

Role of MobileMoney Fintech LTD

MobileMoney Fintech LTD is uniquely positioned to catalyze ecosystem coordination by facilitating shared infrastructure, accelerating secure digital adoption, and strengthening agent support systems. Law enforcement agencies require expanded digital forensic capabilities and enhanced international cooperation mechanisms to tackle increasingly globalized fraud networks effectively.

Governance Platforms

Cross-sector collaboration through governance platforms, unified educational initiatives, and standardized response protocols was identified as essential to ensuring long-term success in combating fraud. These platforms can facilitate ongoing dialogues, resource sharing, and the establishment of best practices that promote security across the ecosystem.



Implementation Pathways

Transformation will require phased implementation strategies that commence with immediate action and evolve toward long-term systemic change.

Near-Term Priorities

- Establishing a pilot project aimed at creating a joint fraud command center, facilitating real-time sharing of intelligence regarding fraud related incidents.
- Implementing rapid-response coordination to activate immediate action among stakeholders when fraudulent activity is detected, permitting timely intervention.

Medium-Term Efforts

Medium-term efforts should focus on institutionalizing shared risk-scoring systems, enabling more effective evaluations of risks among financial institutions. Create and maintain regular engagements/workshops on typologies and relevant trends to fashion standardized detection criteria as well as standardized workflows for fraud reporting and escalation should be established to enhance collaboration. Regular training programs for agents emphasizing operational protocols and fraud detection techniques are also key priorities.

Long-Term Transformation

Long-term transformation will depend on embedding predictive security models into routine operations, fostering a culture of continuous improvement in fraud prevention strategies. Strengthening collaborative frameworks between technology developers, regulators, and financial institutions will be crucial for adapting to future challenges.

Implications and Expected Impact



Enhanced ecosystem collaboration will generate myriad economic benefits through reduced fraud losses and strengthened investor confidence. Socially, improved protection mechanisms will reinforce consumer trust and sustain financial inclusion gains—a critical focus for national development.

Economic Benefits

The implications of a more secure digital financial ecosystem extend deeply into Ghana's economy, facilitating smoother economic transactions and encouraging further investment in the fintech sector. A more resilient ecosystem will attract both local and foreign investments, enhancing innovation and competition while deepening the financial markets.

Trust and Confidence

Institutionally, coordinated frameworks will deepen trust among regulators, industry participants, and law enforcement agencies. Conversely, failure to adapt risks allowing fraud sophistication to erode confidence in digital financial services and slow adoption momentum. The societal implications are profound; a loss of trust could lead to increased cash-based transactions, undermining the digital economy's growth potential.

Regional and Global Comparisons

Regional Context

When comparing Ghana's digital financial ecosystem with other countries in West Africa, such as Nigeria and Côte d'Ivoire, similarities in challenges abound. However, successful regional models can provide key takeaways. For example, Nigeria's regulatory framework supports agile intelligence sharing among financial institutions, enhancing responsiveness to emerging threats.

Global Insights

Globally, cases like those in Singapore and Sweden emphasize the importance of strong legal frameworks, public-private partnerships, and ongoing innovation in technology as critical success factors in combating digital fraud. These insights offer valuable lessons for Ghana as it aims to elevate its own capabilities and ultimately become a leader in secure digital finance.





Comprehensive Fraud Prevention Tactics

Multifaceted Strategies

Preventing fraud requires multifaceted strategies that extend beyond technological solutions. Some of the effective tactics include:

- **Behavioural Analytics:** Employing predictive analytics to identify unusual transaction behaviours indicative of fraud.
- **Tailored Training Programs:** Regular training programs for agents, merchants and employees on the latest fraud tactics, emphasizing the importance of vigilance and proactive reporting.
- **Consumer Education Initiatives:** Ongoing public campaigns focused on informing consumers about potential fraud schemes and safe digital practices.
- **Collaboration with Law Enforcement and Investigative Bodies:** Driving intelligence and investigations with Cyber-Security Unit and Regional Police Investigative Divisions will aid remediation of known fraudulent activities.

These actions will bolster the overall preventative posture of the ecosystem while enhancing consumer confidence.

Technology Innovations in Fraud Prevention

Emerging technologies offer exciting opportunities for enhancing fraud prevention efforts.

Blockchain Technology

Blockchain technology has shown promise in enhancing security by creating immutable records of transactions that are visible to relevant parties. This transparency allows for better tracking of transactions and quicker identification of fraudulent patterns.

Machine Learning Algorithms

Machine learning algorithms can analyze large datasets to identify unusual patterns indicative of fraudulent activity. These insights can enable institutions to act proactively instead of reactively, pre-empting fraud before it occurs.

Identification Techniques

Techniques such as biometric identification can significantly reduce instances of account takeovers, making it more difficult for fraudsters to impersonate individuals. These innovations represent vital components of a robust fraud prevention strategy.

The Importance of User Education

Empowering Consumers

Consumers remain pivotal in the fight against fraud. As such, educational programs must empower them to recognize and mitigate risks. Key areas of focus should include:

- **Identifying Phishing Attempts:** Educating consumers on recognizing suspicious emails or text messages that request sensitive information; and
- **Safeguarding Personal Information:** Encouraging consumers to avoid sharing credentials, such as one-time passwords and PIN's, with anyone.

Engaging Communities

Leveraging mobile platforms for educational outreach can enhance engagement at remote or underserved communities. Mobile workshops, webinars, and interactive platforms can make the education process more dynamic and impactful.

Legal and Regulatory Framework Gaps

Current State of Regulation

While Ghana has made strides in creating a regulatory framework for fintech, gaps must be addressed to bolster fraud prevention and response. Some identified gaps include:

- **Lack of Standardized Reporting Mechanisms:** The absence of uniform guidelines for reporting fraud incidents across institutions complicates collaboration efforts; and
- **Protracted Legal Processes:** Current legal processes impede swift action against fraud, highlighting the need for expedited procedures that allow for immediate intervention.

Proposed Legal Framework Enhancements

To address these challenges, it would be beneficial to establish regulatory bodies specifically focused on fraud prevention and to streamline communication channels between institutions.

Future Trends in Digital Finance and Fraud

Anticipated Challenges

While rolling out the proposed initiatives, several challenges may arise, including:

- **Resistance to Change:** Institutions may exhibit reluctance to alter established processes; and
- **Resource Allocation:** Limited resources may hinder the ability to invest in new technologies.

Mitigation Strategies

Establishing change management plans can facilitate smoother transitions. Strong leadership roles, coupled with transparent communication strategies emphasizing the benefits of new initiatives, will encourage adoption.

Conclusion

Ghana's digital financial ecosystem has achieved remarkable progress in expanding access and enabling innovation. Sustaining this progress now requires a shift from fragmented institutional defence toward coordinated ecosystem security. The Fintech Partner Exchange has demonstrated strong alignment among stakeholders regarding the urgency of this transition. The path moving forward demands collective leadership, technological modernization, regulatory evolution, and sustained collaboration.

The next phase of Ghana's digital financial transformation will be defined not only by innovation and growth but also by the ecosystem's ability to protect itself collectively against increasingly sophisticated threats. By taking coordinated action, Ghana can establish a secure, resilient, and globally competitive digital financial ecosystem.

Acknowledgements

This white paper is the culmination of collaborative efforts and valuable contributions from numerous stakeholders and partners in Ghana's digital financial services landscape. Special gratitude is reserved for the experts, regulatory authorities, and organizations that have dedicated their time and resources to participate in the Fintech Partner Exchange. Their insights were crucial in shaping strategies to combat digital fraud effectively. Recognition is also extended to the speakers and panel of experts who shared valuable and critical insights during the forum. They are Ebenezer Baffour, Head, Internal Affairs (Risk Transactions Monitoring and Revenue Assurance), Hubtel, Nanatunde Davies, Senior Manager, Enterprise Risk, MobileMoney Fintech LTD, Stephen Tefeh, Head, Forensic Services, Stanbic Bank Ghana, Joshua Edmondson, Board Chair, Mobile Money Agents Association of Ghana and Chief Supt. Emmanuel Gyebi, Director of Cybercrime, Ghana Police Service, Shaibu Haruna, Chief Executive Officer of MMFL, Susan Yawson, Chief Financial Officer at MMFL, Sylvia Owusu Ankomah, Chief Executive Officer of the Ghana Chamber of Telecommunications and Clara B. Arthur, Chief Executive Officer of the Ghana Interbank Payment and Settlement Systems (GHIPSS).

As Ghana navigates the complexities of its evolving digital finance ecosystem, the commitment of all participants to continue collaboration and innovation will be critical. The collaborative spirit demonstrated during the forum sets a robust foundation for ongoing engagement and collective success in achieving a secure and prosperous digital marketplace.

White Paper/ Project Team:

Shaibu Haruna – CEO, MobileMoney Fintech LTD.

Godwin Kwame Tamakloe – Chief Regulatory Risk & Compliance, MobileMoney Fintech LTD.

Paapa Osei – Legal & Reputation Management, MobileMoney Fintech LTD.

Moses Tetteh – Senior Manager, Financial Crimes, MobileMoney Fintech LTD.

Rena Ankrah – Manager, AML & CFT, MobileMoney Fintech LTD.

Afua Serwaa Asafo-Adjei – Manager, Communications and Stakeholder Management, MobileMoney Fintech LTD.

Doreen Misrowoda – Advisor, Communications and Stakeholder Management, MobileMoney Fintech LTD.



MoMo
from MTN