Q1 2026 EDITION

GHANA FINTECH & INNOVATION REPORT

A SUSTINERI ATTORNEYS QUARTERLY FINTECH AND INNOVATION REPORT

CONTENT

01

FOREWORD

Dear Esteemed Readers,

We are delighted to present the Q1 2026 edition of The Ghana Fintech and Innovation Report, a publication that continues to reflect the pulse of Ghana's rapidly evolving digital finance and innovation ecosystem. This edition captures a period defined by accelerating digital transformation, stronger regulatory engagement, and the emergence of more intelligent, inclusive, and data-driven financial systems.

This edition opens with Inclusive Technology – The Role of Regulators, where we explore the evolving responsibilities of regulatory institutions in shaping Ghana's digital financial landscape. This section features insights on the Virtual Assets Regulatory Office (VARO) and its role in advancing regulatory clarity, innovation oversight, and responsible ecosystem development.

Our Emerging Products and Business Models section highlights breakthrough innovations redefining how financial services are designed and delivered. We examine the rise of AI CFO Dashboards, offering businesses real-time financial intelligence and decision support; the growth of White-Label Digital Banking Platforms for Non-Bank Brands, enabling new entrants to offer embedded financial services; and the emergence of Invisible Checkout Systems, which are reshaping the future of seamless, frictionless payments.

The Trends and Innovations section explores the foundational shifts shaping the next phase of Ghana's digital economy. Key developments include Federated Data Infrastructure, enabling secure and collaborative data ecosystems; Digital-by-Design Government Models, which reimagine public service delivery through technology; Usage-Based Financial Services (UBFS), which align pricing with real-time consumption patterns; AI Financial Co-Pilots, supporting individuals and businesses in financial decision-making; and Predictive Compliance Systems, which are transforming regulatory monitoring through proactive intelligence.

As part of our commitment to practical financial awareness, our Consumer Insights feature focuses on "Lost Phone, Lost Money? Securing Your Digital Wallets." This piece provides essential guidance on safeguarding mobile money accounts and digital wallets in an increasingly mobile-first financial environment.

Our Insights section brings together analytical and thought-provoking articles from contributors across the team, offering deeper reflections on fintech, artificial intelligence, and innovation trends shaping the Ghanaian and broader African digital economy.
This quarter's Industry Players' Spotlight features FIDO, highlighting its contributions to expanding access to inclusive digital financial services and strengthening trust within the ecosystem.
Finally, we present key Past and Upcoming Events, documenting important engagements that continue to foster collaboration between regulators, industry leaders, innovators, and stakeholders across the fintech landscape.

As we reflect on the progress of this quarter and look ahead to the opportunities of 2026, we remain committed to documenting the ideas, institutions, and innovators shaping the future of finance in Ghana. We extend our sincere appreciation to our readers, contributors, and partners. May this edition inspire continued innovation, collaboration, and impact.

Warm regards,
The Editorial Team

02

PUBLISHERS AND CONTRIBUTORS

SUSTINERI
— ATTORNEYS —

ABOUT THE FIRM – SUSTINERI ATTORNEYS PRUC

We are Ghana's foremost Fintech and Start-up focused law firm, committed to providing differentiated legal services by leveraging our experience as proven entrepreneurs, business managers, and business lawyers which allows us to think and act like the entrepreneurs, business owners, and managers we work with at all times.

As a team of young legal practitioners, **SUSTINERI ATTORNEYS PRUC** takes pride in acting with integrity, avoiding conflicts, and working with clients to design innovative legal solutions that meet their specific needs.

At **SUSTINERI ATTORNEYS PRUC**, we consider every client's brief as an opportunity to use our sound understanding of Ghana's business, commercial and legal environment, professional experience, and sound commercial knowledge to provide solutions that do not only address immediate legal needs but also anticipate future challenges and opportunities.

Our pride as the foremost Fintech and Start-up focused law firm stems not only from our understanding of the potentials of emerging technologies and our belief in the ideas of many young people but also, from the difference our network of resources and experience can make when working closely with founders and entrepreneurs. To this end, we operate a 24-hour policy urging our clients to reach out to us at any time and on any issue.

We strive for excellence, ensuring that our solutions provide sustainable paths for our clients' businesses by adopting a common-sense and practical approach in our value-added legal service delivery – and employing our problem-solving skills.

Our goal is to help businesses to become commercially sound and viable, as well as regulatory compliant, by engaging in legal and beneficial transactions to promote their business competitiveness for sustained operations and investments.

And as our name implies, our priority is to always leverage legal means to promote the sustainability (long-term viability) of our clients' businesses.

We are different, and the preferred partner for growth.

CONTRIBUTORS

Harold Kwabena Fearon,
Associate

harold@sustineriattorneys.com

Adwoa Birago Nyantakyi,
Associate

birago@sustineriattorneys.com

Dennis Akwaboah,
Associate

a.dennis@sustineriattorneys.com

Dede Wobil,
Associate

dede@sustineriattorneys.com

03

INCLUSIVE FINANCIAL TECHNOLOGY (FINTECH)

VIRTUAL ASSETS REGULATORY OFFICE (VARO)

The Virtual Assets Regulatory Office (VARO) was established under the Virtual Assets (Service Providers) Act, 2025 (Act 1154) as Ghana's dedicated authority for overseeing and regulating virtual asset service providers (VASPs) and related activities. VARO operates under the aegis of the Bank of Ghana and is tasked with ensuring that the rapidly evolving virtual assets ecosystem in Ghana develops within a sound, transparent, and consumer-protective regulatory framework. Its creation reflects Ghana's recognition that digital finance including cryptocurrencies, tokenised assets, and blockchain-based financial products requires a specialised regulatory body capable of responding to both the opportunities and risks inherent in this space.

The key mandates of VARO are multifacet. Firstly, it is responsible for the licensing and registration of virtual asset service providers, ensuring that only entities meeting prescribed financial, technical, and governance standards are permitted to operate. This gatekeeping function is critical for protecting consumers and maintaining confidence in the emerging sector. Secondly, VARO sets conduct-of-business standards for VASPs, including requirements around anti-money laundering (AML), counter-financing of terrorism (CFT), cybersecurity, and customer due diligence. Thirdly, it is empowered to supervise, investigate, and sanction non-compliant entities, thereby ensuring ongoing adherence to regulatory obligations. VARO also serves as a point of coordination with international standard-setting bodies such as the Financial Action Task Force (FATF), aligning Ghana's virtual assets framework with globally accepted norms.

The virtual assets industry in Ghana is at an inflection point. With a young, tech-savvy population and high mobile penetration rates, Ghana presents fertile ground for the adoption of blockchain-based financial services. VARO's establishment signals the government's commitment to harnessing the transformative potential of virtual assets while mitigating associated risks such as fraud, market manipulation, and illicit financial flows. This article examines the regulatory landscape being built by VARO, the role of technology in expanding inclusive

access to financial services, and the opportunities this regulatory evolution presents for fintech innovators in Ghana.

THE NEED FOR A DEDICATED VIRTUAL ASSETS REGULATOR

Prior to the enactment of Act 1154, Ghana's virtual assets space operated in a regulatory grey area. While the Bank of Ghana had issued cautionary notices regarding the use of cryptocurrencies, there was no comprehensive legislative or supervisory framework governing VASPs. This vacuum created risks not only for consumers who engaged with unregulated platforms but also for the integrity of Ghana's financial system more broadly. Reports of fraud, Ponzi schemes, and exchange collapses underscored the urgent need for a structured regulatory response.

The global regulatory landscape also influenced Ghana's approach. The FATF's revised Recommendation 15, which extended AML/CFT obligations to VASPs, placed international pressure on jurisdictions to bring virtual asset activities within the regulatory perimeter. Ghana, as a member of the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA), has a particular obligation to implement FATF standards. VARO's creation was therefore not only a response to domestic market realities but also a fulfilment of Ghana's international commitments to financial integrity. By establishing a purpose-built office, Ghana has demonstrated its intent to be a responsible and forward-looking participant in the global digital economy.

THE ROLE OF VIRTUAL ASSETS IN DRIVING FINANCIAL INCLUSION

Virtual assets hold considerable promise as instruments of financial inclusion in Ghana. A significant proportion of the Ghanaian population remains underserved by traditional banking institutions, particularly in rural and peri-urban areas where bank branch density is low. Mobile money has already demonstrated how technology can bridge this gap, and virtual assets—particularly stablecoins and blockchain-based payment systems—offer an additional layer of functionality that can extend financial access further. Remittances, for example, represent a major financial flow for many Ghanaian households, and virtual asset solutions have the potential to reduce the cost and increase the speed of cross-border transfers relative to conventional wire transfer services.

Furthermore, the tokenisation of real-world assets such as agricultural commodities, real estate, and government securities on blockchain platforms presents opportunities for previously excluded communities to participate in investment markets. By lowering the minimum investment threshold and enabling fractional ownership, tokenised assets can democratise wealth-building opportunities. VARO's regulatory framework, by providing clarity and consumer protections, is intended to create the conditions of trust necessary for mainstream adoption of these innovations. A well-regulated virtual assets market can attract reputable international platforms, stimulate domestic fintech entrepreneurship, and provide Ghanaians with access to a broader range of financial products tailored to their needs.

REGULATORY FRAMEWORK FOR VIRTUAL ASSET SERVICE PROVIDERS

The Virtual Assets (Service Providers) Act, 2025 (Act 1154) provides the legislative foundation upon which VARO's regulatory architecture rests. Under this framework, any entity wishing to provide virtual asset services in or from Ghana including exchange services, transfer services, custody, administration, or participation in token offerings is required to obtain the appropriate licence from either the Bank of Ghana or the Securities and Exchange Commission (SEC), depending on the nature of the activity. The Bank of Ghana supervises payment and custody services, while the SEC oversees trading and investment activities. VARO acts as a coordinating office within the Bank of Ghana, bridging government oversight and the industry. The Act establishes distinct licence categories corresponding to different types of virtual asset activities, with each category carrying specific capital adequacy requirements, operational standards, and governance obligations.

A notable feature of the regulatory framework is its risk-based approach to supervision. VARO is empowered to calibrate its supervisory intensity based on the risk profile of individual VASPs, taking into account factors such as transaction volumes, customer base, product complexity, and cross-border exposure. This proportionality ensures that innovative start-ups and smaller operators are not disproportionately burdened by compliance requirements designed primarily for systemically significant entities. At the same time, the framework incorporates robust provisions for consumer protection, including requirements for clear disclosure of risks, segregation of client assets, and the maintenance of adequate reserves to meet redemption obligations.

THE VARO REGULATORY SANDBOX AND INNOVATION SUPPORT

Recognising that overly rigid regulation can stifle the very innovation it seeks to govern, VARO has introduced a regulatory sandbox framework that enables fintech start-ups and established virtual asset businesses to test novel products and business models under relaxed regulatory conditions for a defined period. The sandbox is designed to generate real-world evidence about the risks and benefits of new virtual asset applications, thereby enabling VARO to develop proportionate and evidence-based permanent rules. Participants in the sandbox benefit from direct regulatory engagement, reduced compliance burdens during the testing phase, and a pathway to full licensing upon successful conclusion of their sandbox tenure.

The Virtual Assets Regulatory Office (VARO) was established under the Virtual Assets (Service Providers) Act, 2025 (Act 1154) as Ghana's dedicated authority for overseeing and regulating virtual asset service providers (VASPs) and related activities.

VARO has also established a dedicated innovation office to provide guidance and pre-application support to businesses seeking to enter the Ghanaian virtual assets market. This office serves as a point of contact for entrepreneurs and investors who require clarity on licensing requirements, conduct obligations, and the regulatory perimeter. By lowering the information asymmetry that often acts as a barrier to market entry for innovative businesses, VARO aims to foster a competitive and dynamic virtual assets ecosystem in Ghana. These initiatives reflect an understanding that effective regulation in the digital economy requires not only enforcement capability but also a posture of active engagement with the market participants it oversees.

ANTI-MONEY LAUNDERING AND CONSUMER PROTECTION IMPERATIVES

A central pillar of VARO's mandate is the prevention of

money laundering, terrorist financing, and other financial crimes facilitated through virtual asset channels. VASPs operating in Ghana are required to implement robust know-your-customer (KYC) and customer due diligence procedures, maintain comprehensive transaction records, and report suspicious activities to the Financial Intelligence Centre (FIC). VARO works in close coordination with the FIC, the Securities and Exchange Commission (SEC), the Ghana Revenue Authority (GRA), and the National Communications Authority (NCA) to ensure that supervisory intelligence flows effectively across the relevant public agencies. The Travel Rule which requires VASPs to pass originator and beneficiary information along with virtual asset transfers above a specified threshold has been incorporated into Ghana's regulatory requirements in alignment with FATF Recommendation 16.

Consumer protection is equally prioritised within VARO's regulatory framework. Many participants in the virtual assets market are retail investors with limited financial literacy and a poor understanding of the technical and market risks associated with virtual assets. VARO has therefore mandated that VASPs provide clear, accurate, and non-misleading information about the products and services they offer, including explicit risk warnings about the volatility and speculative nature of many virtual assets. VARO also maintains a public register of licensed VASPs, enabling consumers to verify whether a platform they intend to use is authorised and subject to regulatory oversight, thereby reducing the risk of exposure to fraudulent or unregulated operators.

THE IMPORTANCE OF TECHNOLOGY AND DIGITAL INFRASTRUCTURE

The effectiveness of VARO's regulatory mandate is closely tied to Ghana's broader digital infrastructure. The expansion of reliable internet connectivity, the widespread adoption of mobile devices, and the growing sophistication of Ghana's technology sector collectively create an enabling environment for the growth of virtual asset services. The government's Digital Ghana Agenda and its associated investments in broadband infrastructure, digital identity systems, and e-government services provide a complementary foundation upon which the virtual assets ecosystem can be built. In particular, the Ghana Card national identification system offers a ready-made tool for VASPs to fulfil their KYC obligations efficiently and reliably, reducing onboarding friction for consumers while meeting regulatory requirements.

VARO has also invested in its own supervisory technology (SupTech) capabilities, developing data-sharing protocols and reporting systems that enable VASPs to submit regulatory returns electronically and allow VARO to monitor market developments in near real time. This investment in digital supervisory infrastructure is essential for keeping pace with the speed and complexity of the virtual assets market. By leveraging technology in its own operations, VARO not only improves the efficiency and effectiveness of its oversight function but also signals to the market that it is a modern, capable, and credible regulator, a signal that is itself conducive to attracting reputable operators to the Ghanaian market.

THE FUTURE OF VIRTUAL ASSETS REGULATION IN GHANA

Ghana's establishment of VARO represents a signifi-

cant milestone in the country's journey towards becoming a leading digital finance hub in Africa. As the virtual assets landscape continues to evolve with emerging developments in decentralised finance (DeFi), non-fungible tokens (NFTs), and central bank digital currencies (CBDCs), VARO will need to continuously update its regulatory framework to address new products, risks, and market structures. The Bank of Ghana's own exploration of a digital cedi further underscores the extent to which virtual and digital assets are becoming central to the future of Ghana's financial system, and VARO's role in this ecosystem is likely to expand accordingly.

International collaboration will also be critical to VARO's long-term effectiveness. Virtual assets are inherently cross-border in nature, and the risks they pose particularly in relation to financial crime cannot be addressed by any single jurisdiction acting alone. VARO's active participation in regional and global regulatory forums, including GIABA, the African Development Bank's financial inclusion networks, and bilateral engagement with regulators in jurisdictions hosting major virtual asset platforms, will be essential for developing a coherent and effective international supervisory architecture. Through these partnerships, Ghana can contribute to the shaping of global norms while also ensuring that its own regulatory framework remains fit for purpose in a rapidly changing environment.

CONCLUSION

The establishment of the Virtual Assets Regulatory Office marks a transformative chapter in Ghana's financial regulatory history. By creating a dedicated, specialised, and technologically equipped regulator for the virtual assets sector, Ghana has positioned itself to harness the considerable potential of digital assets to deepen financial inclusion, stimulate innovation, and attract investment, while managing the attendant risks with rigour and sophistication.

04

EMERGING PRODUCTS AND BUSINESS MODELS

WHITE-LABEL DIGITAL BANKING PLATFORMS FOR NON-BANK BRANDS: THE QUIET TRANSFORMATION OF FINANCIAL SERVICES

Across the global financial services industry, one of the most significant developments in recent years has been the rise of white-label digital banking platforms. Increasingly, companies that were never traditionally seen as financial institutions are now offering banking and payment services directly to customers under their own brands.

Today, airlines offer wallets and virtual cards. Ride-hailing companies provide digital payments and lending. Retail chains launch mobile money and savings products. Telecommunications companies operate financial ecosystems that rival traditional banks in customer activity and reach.

What is becoming clear is that banking is no longer confined to banks. Instead, financial services are gradually becoming embedded within broader digital ecosystems, allowing non-bank brands to integrate payments, savings, lending, insurance, and other financial products directly into their customer journeys through white-label infrastructure provided by licensed financial institutions and fintech providers.

For Ghana and the broader African market, this trend is becoming increasingly important as digital adoption grows, financial inclusion expands, and consumers demand faster, simpler, and more integrated financial experiences.

WHAT ARE WHITE-LABEL DIGITAL BANKING PLATFORMS?

A white-label digital banking platform is essentially a banking infrastructure solution developed by one provider but rebranded and offered by another company under its own identity. In practical terms, the underlying banking technology, compliance systems, payment rails, and regulatory infrastructure are operated by a licensed financial institution or fintech infrastruc-

ture provider, while the customer-facing experience carries the branding of a non-bank business.

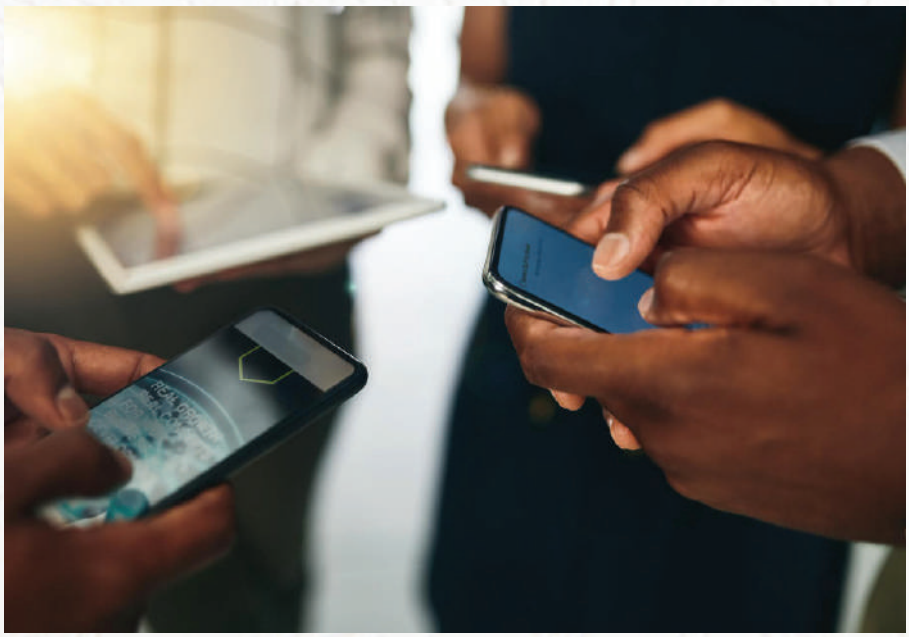
This model allows companies that are not traditional banks to offer financial products without building a full banking infrastructure from scratch or obtaining a complete banking license themselves.
Globally, this model has grown rapidly through the broader rise of Banking-as-a-Service (BaaS) and embedded finance. For example, Shopify offers financial services to merchants through embedded banking partnerships. Uber has introduced driver-focused banking and payment solutions in several markets. Apple entered financial services through products such as Apple Card and integrated payment ecosystems developed in partnership with regulated financial institutions.

In Africa, the model is becoming increasingly visible within fintech, telecommunications, retail, and platform-based businesses.

WHY NON-BANK BRANDS ARE ENTERING FINANCIAL SERVICES

The attraction is relatively straightforward. Financial services deepen customer engagement, improve transaction visibility, generate additional revenue streams, and increase customer retention. For many businesses, payments and financial products are no longer viewed as separate services. They are becoming part of the overall customer experience.

A ride-hailing platform that enables driver wallets, fuel financing, and instant payments becomes more valuable to drivers. An e-commerce platform that offers merchant payments and working capital financing creates stronger platform loyalty. A telecommunications company that provides payments, savings, and micro-lending becomes embedded within everyday economic activity.



This is exactly what has happened across much of Africa. The success of mobile money ecosystems such as MTN Mobile Money and M-Pesa demonstrated that consumers are often more interested in convenience, accessibility, and trust than whether a provider is technically a traditional bank. That shift in consumer behavior is now influencing the next phase of fintech development across the continent.

THE GHANAIAN CONTEXT: WHY THIS MODEL MATTERS

In Ghana, the growth of digital payments, fintech innovation, and mobile money adoption has created an environment where white-label banking models are becoming increasingly commercially viable.
Consumers are already accustomed to digital wallets, QR payments, mobile-based transactions, and platform-driven financial services. As a result, businesses outside the traditional banking sector are beginning to recognise financial services as an extension of their core offerings. Retail businesses, telecommunications operators, e-commerce platforms, savings groups, transport platforms, agritech companies, and even educational institutions are exploring ways to integrate embedded financial products into their ecosystems.

For startups and SMEs in particular, white-label banking

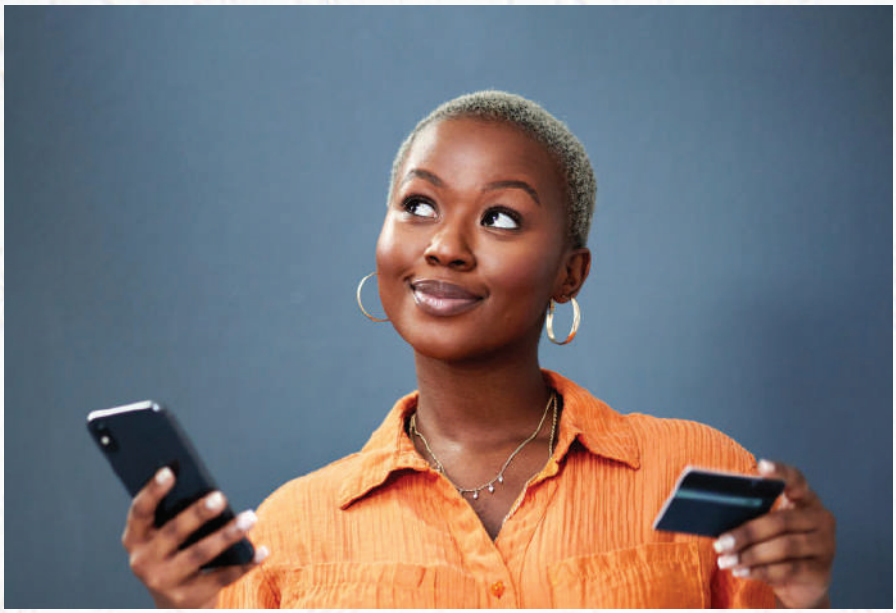
infrastructure significantly lowers the barriers to entry into financial services. Rather than investing heavily in banking infrastructure, licensing, compliance systems, cybersecurity architecture, and payment integrations, businesses can partner with licensed institutions and fintech infrastructure providers to launch financial products much faster and at lower cost.

This creates opportunities for innovation, particularly in underserved sectors and informal markets where traditional banking penetration remains limited.

REGULATORY AND LEGAL CONSIDERATIONS

While the opportunities are significant, white-label banking models also create important legal and regulatory considerations. One of the biggest misconceptions in the market is that outsourcing banking infrastructure removes regulatory exposure. In reality, financial services regulation continues to apply regardless of who owns the customer-facing brand.

In Ghana, businesses operating within these arrangements may trigger obligations under frameworks administered by the Bank of Ghana, particularly in areas relating to payment services, electronic money issuance, consumer protection, anti-money laundering compliance, cybersecurity, outsourcing, and data protection.
Questions around licensing



structures are especially important. Depending on how a platform is structured, the business may require authorization as a Payment Service Provider, Dedicated Electronic Money Issuer, or may need to operate strictly through agency and partnership arrangements with licensed entities.

Data governance is another major issue. Because white-label models involve multiple parties sharing customer data, transaction information, and operational infrastructure, businesses must pay close attention to compliance obligations under Ghana's data protection framework, cybersecurity requirements, and contractual risk allocation arrangements.

Liability allocation also becomes critical when service failures, fraud incidents, or operational disruptions occur. Customers usually associate the financial product with the visible brand rather than the underlying infrastructure provider. This creates reputational and legal exposure for non-bank brands entering the financial services space.

As a result, partnership agreements within white-label banking arrangements must clearly address:
a. regulatory responsibilities;
b. customer onboarding obligations;
c. KYC and AML compliance allocation;
d. dispute resolution mechanisms;
e. cybersecurity responsibilities;
f. data ownership and processing rights; and
g. operational risk management procedures.

THE RISE OF EMBEDDED FINANCE IN AFRICA

The broader trend driving white-label digital banking is embedded finance. Financial services are gradually disappearing into everyday digital experiences rather than existing as standalone banking products. Across Africa, this is already happening in

agriculture, mobility, retail, logistics, healthcare, and telecommunications.

For instance, a farmer receiving embedded crop financing through an agritech platform may never directly interact with a traditional bank. A merchant accepting platform-based payments may receive working capital financing within the same application. Consumers increasingly access financial services within apps and ecosystems they already use daily.

This shift is likely to accelerate significantly as open banking frameworks, API infrastructure, artificial intelligence, and digital identity systems continue to evolve across African markets.

KEY RISKS BUSINESSES MUST NOT IGNORE

Despite the excitement surrounding embedded finance and white-label banking, businesses must approach the model carefully. Operational dependency on third-party infrastructure providers can create serious continuity risks. A compliance failure or technical outage affecting one provider can disrupt the entire customer experience.

Cybersecurity exposure is another growing concern, particularly as fraud sophistication increases across digital financial ecosystems. There is also the risk of regulatory uncertainty. Across Africa, regulators are still adapting to the rapid convergence of technology companies and financial services. Rules around digital assets, cross-border payments, data localization, open banking, and platform liability continue to evolve.

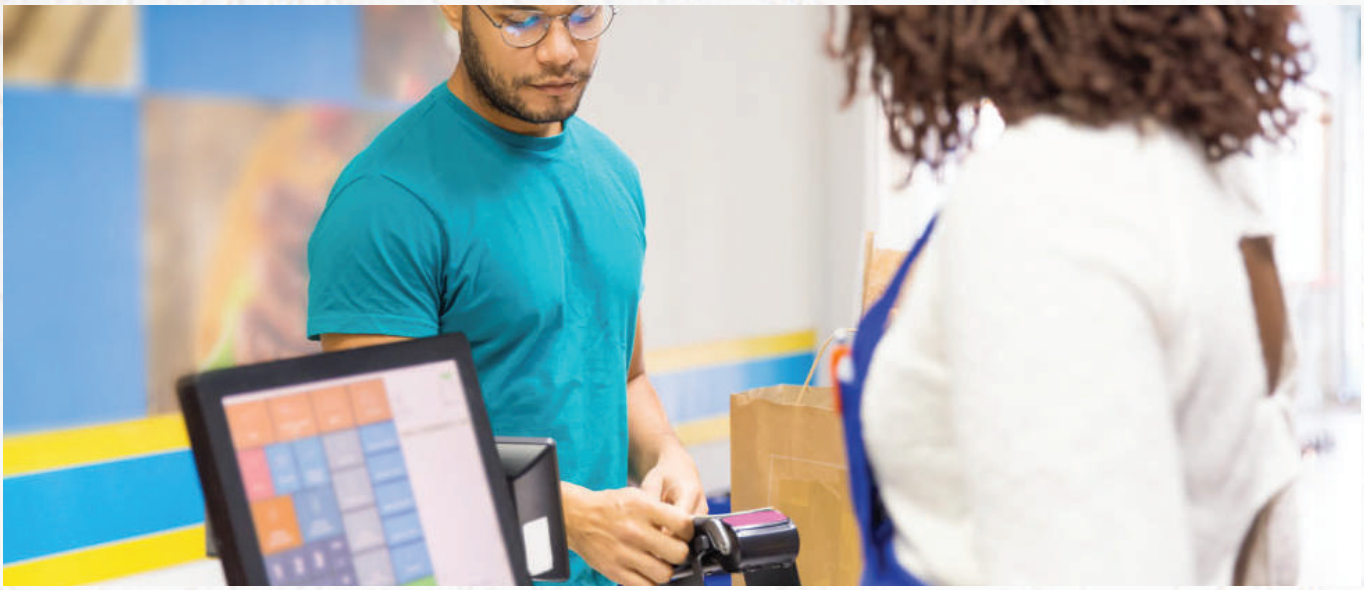
For businesses entering this space, legal structuring and regulatory planning are therefore no longer secondary considerations. They are central to the sustainability of the business model itself.

CONCLUSION

White-label digital banking platforms are reshaping the structure of financial services globally and Africa is increasingly becoming part of that transformation. The traditional distinction between banks and non-bank businesses is gradually becoming less clear as financial services become embedded within digital platforms, consumer ecosystems, and everyday commercial activity.

For Ghana, the opportunities are significant. White-label infrastructure can accelerate financial inclusion, support innovation, expand access to digital finance, and create entirely new business models across sectors.

At the same time, the model introduces complex regulatory, operational, and legal considerations that businesses cannot afford to overlook. The next generation of financial services in Africa may not necessarily be led only by banks. Increasingly, it may be driven by platforms, ecosystems, and non-traditional brands that understand how to integrate finance seamlessly into everyday life.



INVINCIBLE CHECKOUT SYSTEMS: WHY BUSINESSES ARE RETHINKING THE MOST IMPORTANT STAGE OF DIGITAL COMMERCE

In digital commerce, very few things damage a business faster than a failed checkout process.

A customer may spend several minutes browsing products, comparing prices, adding items to cart, and preparing to pay, only for the transaction to fail at the final stage. Sometimes the payment gateway freezes. Sometimes a mobile money prompt delays. Sometimes the system crashes completely. In other cases, customers abandon purchases simply because the checkout process feels too complicated.

For businesses, these are no longer minor technical inconveniences. They are revenue, trust, and retention problems.

As digital payments and e-commerce continue to grow across Ghana and Africa, businesses are beginning to focus more seriously on what many now describe as "invincible checkout systems." These are checkout infrastructures designed to remain fast, stable, secure, seamless, and resilient even under pressure, high transaction volumes, poor internet conditions, fraud attempts, or payment interruptions.

Increasingly, the success of digital commerce is no longer determined only by the quality of products or services being sold. It is determined by whether customers can complete payments quickly and without friction.

WHAT MAKES A CHECKOUT SYSTEM "INVINCIBLE"?

The term does not suggest perfection. Rather, it refers to checkout systems designed to minimize friction, reduce payment failures, recover quickly from disruptions, and maintain customer confidence across different devices, payment methods, and network conditions. An effective checkout system today must do far more than pro-

cess card payments.

It must integrate mobile money, bank transfers, QR payments, digital wallets, recurring payments, tokenisation, fraud detection systems, customer authentication layers, and real-time transaction monitoring, all while remaining simple enough for an ordinary customer to use comfortably.
Globally, companies such as Amazon, Stripe, and Shopify have invested heavily in frictionless checkout experiences because they understand a simple reality: every additional second or extra click increases the likelihood of customer abandonment.This trend is now becoming increasingly relevant in African markets.

WHY CHECKOUT INFRASTRUCTURE MATTERS MORE IN AFRICA

In Africa, checkout systems operate within a far more complicated payment environment than many developed markets. Businesses must deal with inconsistent internet connectivity, multiple payment methods, mobile-first users, fragmented banking systems, transaction reversals, network downtimes, and varying levels of digital literacy.

In Ghana, for example, a customer may expect to pay through mobile money, bank transfer, debit card, QR code, or wallet balance depending on convenience and network reliability at that moment.
A checkout system that accommodates only one payment option immediately limits transaction success rates. This explains why interoperability and payment flexibility are becoming central features of modern African fintech infrastructure.

Payment providers such as Flutterwave, Paystack, and Hubtel have gained traction partly because they simplify multi-channel payment acceptance for businesses operating in fragmented payment environments. For many SMEs and online businesses, checkout efficiency is now directly tied to business survival.

THE BUSINESS COST OF FAILED PAYMENTS

One of the biggest misconceptions among businesses is that customers who experience failed payments will simply return later to try again. In reality, most do not. Digital commerce operates heavily on immediacy and convenience. The moment a checkout process becomes frustrating, trust begins to decline.

Customers may worry that their money will be debited without confirmation. Others become concerned about fraud or system reliability. Some simply move to a competitor offering a smoother payment experience. For subscription-based platforms, failed checkout systems can also affect recurring revenue and customer retention rates.

This is particularly important for African startups operating in highly competitive digital markets where customer loyalty remains fragile and switching costs are low. A poor checkout experience today can quietly destroy months of customer acquisition efforts.

THE RISE OF "INVISIBLE PAYMENTS"

One of the most important global fintech trends influencing checkout systems is the rise of invisible payments.

Increasingly, businesses are trying to eliminate as many payment steps as possible. Consumers are becoming accustomed to one-click purchases, saved payment credentials, biometric authentication, auto-renewals, and embedded wallet payments that happen almost automatically within digital platforms.

Services such as Uber and Netflix helped normalise payment experiences where customers barely think about the payment process itself.

In Africa, this transition is happening more gradually due to infrastructure and regulatory considerations, but the direction is becoming clearer. Consumers increasingly prefer payment experiences that feel instant, simple, and predictable. The businesses that remove friction most effectively are likely to retain customers more successfully.

SECURITY VS CONVENIENCE: THE CONSTANT BALANCE

One of the biggest challenges in checkout design is balancing security with convenience. The easier a payment experience becomes, the greater the potential fraud exposure. Conversely, excessive security layers can frustrate legitimate customers and increase cart abandonment rates. This tension is becoming more visible across African digital commerce ecosystems as fraud attempts continue to evolve.

Businesses are therefore investing more heavily in:

- tokenised payments;
- behavioural fraud monitoring;
- device recognition tools;
- AI-driven transaction analysis;
- biometric authentication; and
- real-time fraud detection systems.

At the same time, regulators are also becoming more active in strengthening digital payment security frameworks.

In Ghana, institutions operating payment infrastructure remain subject to regulatory oversight from the Bank of Ghana, particularly regarding cybersecurity, electronic money operations, consumer protection, anti-money laundering obligations, and payment systems oversight. As checkout systems become more embedded across sectors, compliance and operational resilience are becoming as important as speed and convenience.

THE NEXT PHASE OF DIGITAL COMMERCE

The future of checkout systems will likely move beyond simple payment acceptance into predictive and adaptive payment ecosystems. Artificial intelligence will increasingly personalise checkout experiences based on customer behaviour, device usage, location, and transaction history. Systems will automatically reroute failed payments through alternative rails, detect fraud in real time, and optimise transaction success rates dynamically.

Open banking frameworks, embedded finance, central bank digital currencies, and interoperable payment ecosystems may further reshape how checkout infrastructure operates across Africa in the coming years. For businesses, this means checkout systems are no longer merely operational tools. They are strategic infrastructure.

CONCLUSION

Invincible checkout systems are gradually becoming one of the most important competitive advantages in digital commerce. In a world where customers expect instant, seamless, and secure transactions, businesses can no longer afford weak payment infrastructure, unstable gateways, or overly complicated checkout processes. For Ghana and the broader African fintech ecosystem, the challenge is not simply about enabling digital payments. It is about building resilient payment experiences capable of operating effectively within the realities of African markets while still meeting global consumer expectations.

The businesses that succeed in the next phase of digital commerce may not necessarily be those with the biggest platforms or the widest product selection. Increasingly, they may be the ones that make paying feel effortless.

AI CFO DASHBOARDS (BUSINESS MODEL)

AI CFO Dashboards represent a new category of financial business model where companies provide AI-powered executive-level financial intelligence platforms as a service. Instead of hiring or relying solely on a traditional Chief Financial Officer function for analysis and reporting, businesses subscribe to an AI-driven system that simulates CFO-level oversight.

These platforms consolidate financial data from multiple sources—banking systems, accounting software, payroll tools, and revenue platforms—and generate real-time executive insights. They provide forecasting, scenario modeling, risk analysis, and strategic financial recommendations in a single interface.

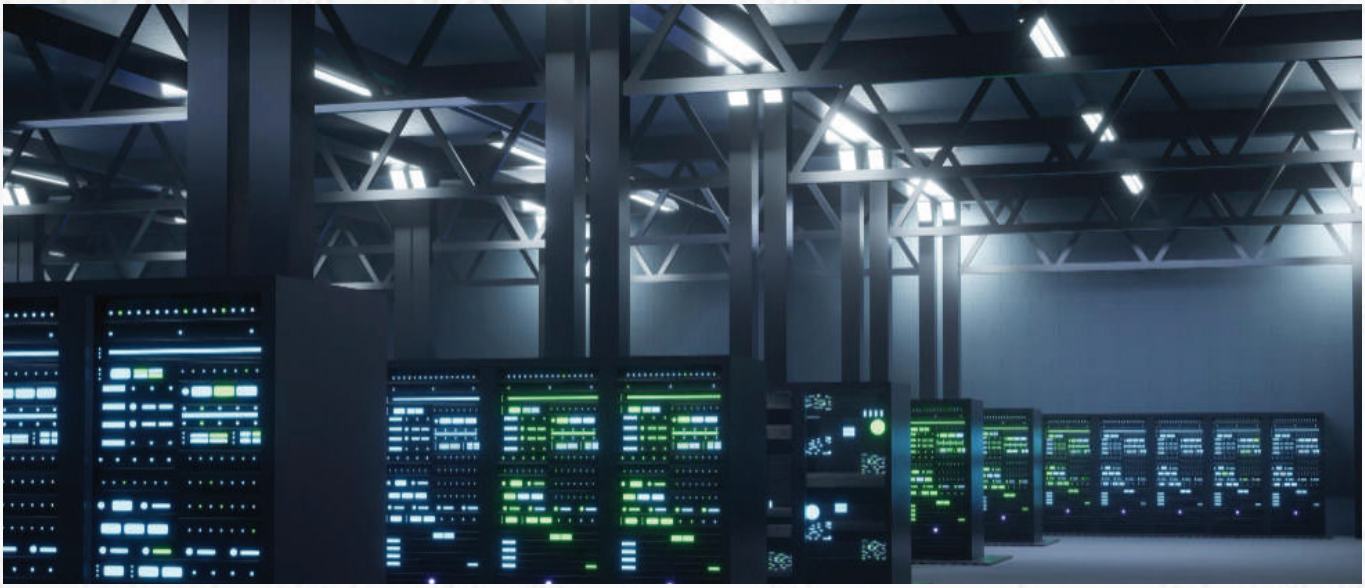
The business model is typically subscription-based or usage-based, often layered with premium tiers for advanced analytics, forecasting depth, and integration capabilities. Some platforms also incorporate AI agents that can autonomously perform financial tasks such as budgeting adjustments, liquidity management suggestions, and cost optimization recommendations.

What makes this model powerful is its scalability. Instead of CFO-level expertise being limited to large corporations, AI CFO dashboards democratize strategic financial intelligence for SMEs, startups, and creator-led businesses.

In essence, this model shifts financial leadership from a human-only executive function to a hybrid system where AI provides continuous financial strategy support, while human decision-makers retain final control and oversight.

05

TRENDS AND INNOVATION



FEDERATED DATA INFRASTRUCTURE: A NEW ARCHITECTURE FOR SECURE DATA COLLABORATION

Over the past decade, the global digital economy has become increasingly dependent on data. Financial institutions, healthcare providers, governments, insurers, technology companies, logistics platforms, and telecommunications operators now rely heavily on data sharing to improve services, train artificial intelligence systems, manage risk, detect fraud, and make commercial decisions.

At the same time, organizations are facing growing pressure around data privacy, cybersecurity, data sovereignty, and regulatory compliance. Businesses want to collaborate and extract value from data, but they are also increasingly reluctant to hand over sensitive information to third parties or centralized systems.

This tension is gradually driving one of the most important structural shifts in modern digital infrastructure: the rise of federated data systems.Rather than moving all data into one central repository, federated data infrastructure allows organizations to collaborate, analyze, and share insights while the underlying data remains within the control of the original owner.Globally, this model is beginning to reshape how institutions think about data governance, artificial intelligence, cybersecurity, and cross-border digital cooperation.

WHAT IS FEDERATED DATA INFRASTRUCTURE?

Federated data infrastructure refers to a decentralized data architecture where multiple organizations or systems can securely collaborate and exchange insights without necessarily pooling or transferring raw data into a single central database. Under traditional models, organizations often aggregate large volumes of data into centralized platforms before analysis occurs. While efficient in some respects, this approach creates major concerns around privacy, cybersecurity exposure, operational concentration risks, and regulatory compliance. Federated systems work differently.

Data remains within each institution's environment while authorized algorithms, queries, or analytical models interact across the network in a controlled manner. Instead of sharing the data itself, organizations may share only outputs, patterns, or insights derived from the data.

This architecture is becoming particularly important in sectors where confidentiality, privacy, and data sensitivity are critical.

Healthcare institutions, financial services providers, governments, defence systems, and artificial intelligence developers are increasingly exploring federated models as a way to balance innovation with security and regulatory compliance.

WHY CENTRALISING DATA IS BECOMING A PROBLEM

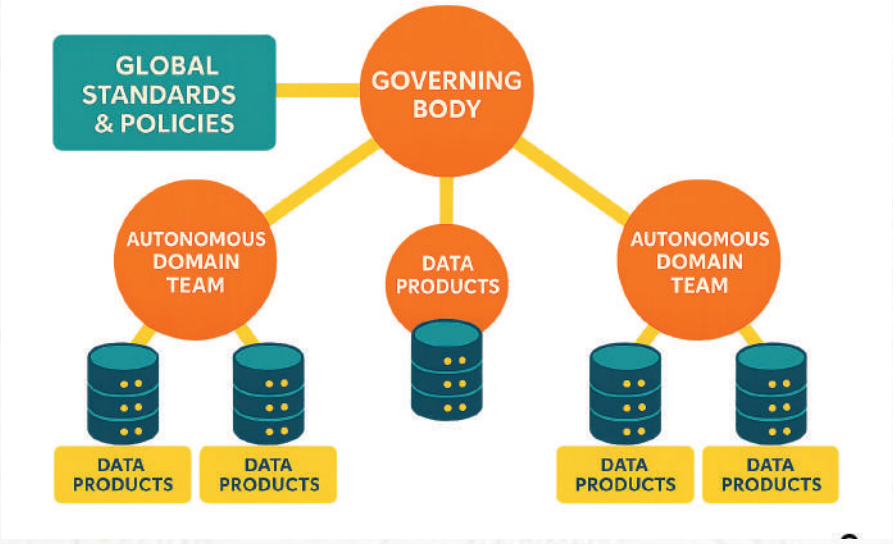
For years, centralisation dominated digital infrastructure thinking. Large-scale cloud systems and central data lakes were viewed as the most efficient way to process and monetise information.

However, the rapid growth of cyber threats, ransomware attacks, and global privacy regulation is exposing the weaknesses of heavily centralized systems.

A single breach within a centralized environment can compromise millions of users simultaneously.

Recent global cyber incidents affecting financial institutions, healthcare systems, and technology companies have demonstrated how dangerous concentrated data exposure can become. Increasingly, regulators and organizations are beginning to question whether unlimited centralization is sustainable in a world of escalating cyber risk.

At the same time, data sovereignty concerns are becoming more politically sensitive. Countries are becoming more cautious about allowing sensitive national or citizen data to leave their jurisdictions, particularly in sectors involving financial services, healthcare, telecommunications, defence, and critical infrastructure. This is one of the major reasons federated systems are gaining traction globally.



THE ROLE OF ARTIFICIAL INTELLIGENCE

One of the biggest drivers behind federated infrastructure is artificial intelligence. Modern AI systems require enormous amounts of data to function effectively. However, many organizations are unwilling or legally unable to share raw datasets due to privacy restrictions and commercial sensitivities.

Federated learning attempts to solve this problem. Under this approach, AI models are trained across multiple decentralised datasets without requiring the actual data to leave the organisation that owns it. Only the model updates or learning outputs are shared across the network.This allows institutions to collectively improve AI systems while maintaining stronger privacy controls.

Globally, companies such as Google have explored federated learning in areas such as smartphone personalisation and predictive text systems. Healthcare research institutions are also using federated models to collaborate on medical AI development without exposing sensitive patient records. In financial services, federated systems

are increasingly being explored for fraud detection, anti-money laundering analysis, and risk modelling across institutions.

WHY THIS MATTERS FOR FINANCIAL SERVICES

For banks, fintech companies, insurers, and payment service providers, federated infrastructure presents significant opportunities. Financial institutions operate in highly regulated environments where customer confidentiality and data protection obligations are critical. Yet, many industry challenges such as fraud detection, financial crime monitoring, credit scoring, and cybersecurity intelligence require collaboration across multiple institutions. Traditionally, this created difficult trade-offs between cooperation and confidentiality.

Federated systems offer a middle ground. Multiple institutions can contribute to shared analytical models without exposing raw customer data to competitors or external parties. Fraud patterns, suspicious transactions, or emerging cyber threats can be identified collectively while maintaining stronger privacy safeguards.

This is becoming increasingly important as digital financial ecosystems grow more interconnected globally. Open banking, embedded finance, digital identity systems, and cross-border payment networks all depend heavily on trusted and secure data-sharing

mechanisms. Federated architecture may eventually become one of the foundational structures supporting that ecosystem.

REGULATORY AND PRIVACY CONSIDERATIONS

The growth of federated systems is also closely linked to the evolution of global data protection laws.
Regulations such as the European Union's General Data Protection Regulation (GDPR), along with similar privacy frameworks emerging across multiple jurisdictions, are forcing organizations to rethink how data is collected, stored, transferred, and processed.

Federated systems can help organizations reduce unnecessary data movement while improving compliance with localization and privacy requirements.

However, these systems are not free from legal complexity.
Questions still arise around:

- data ownership;
- algorithmic accountability;
- liability allocation;
- cross-border processing rights;
- cybersecurity standards;
- consent management; and
- governance oversight.

There is also the issue of trust. Federated ecosystems only function effectively when participating organisations trust the governance framework, security standards, and technical integrity of the network itself. As a result, legal structuring, interoperability standards, and governance protocols become critically important.

THE CHALLENGE OF IMPLEMENTATION

Despite the growing interest, federated infrastructure remains technically and operationally demanding. Interoperability between different systems can be

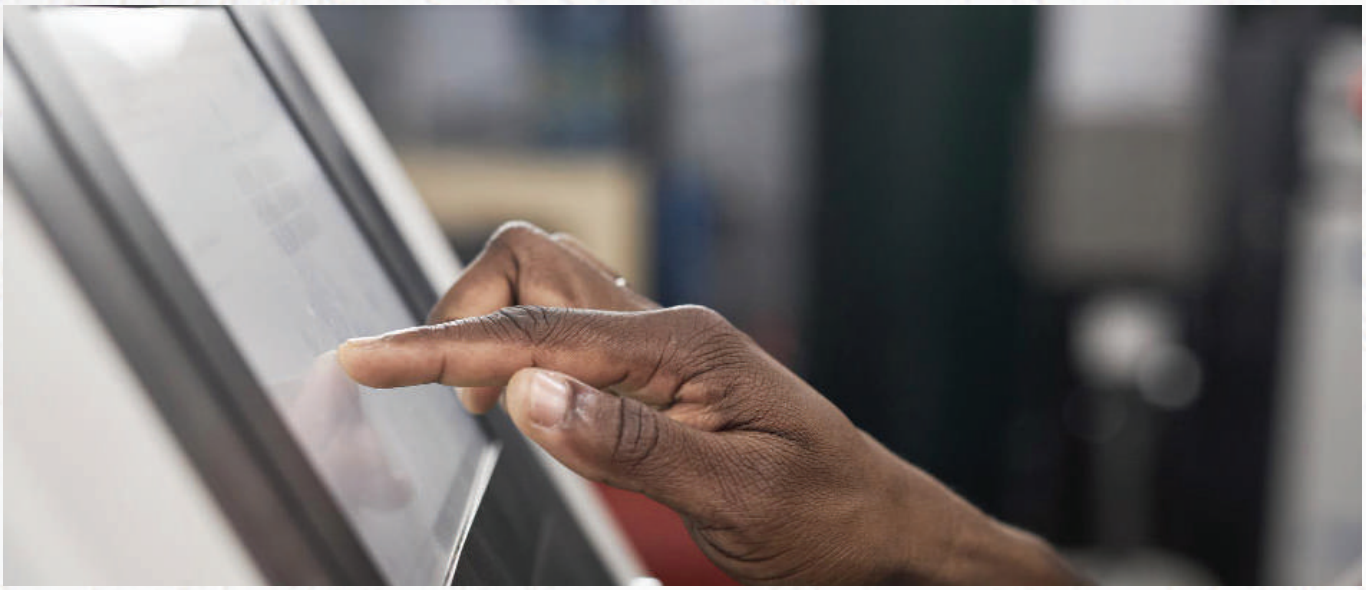
difficult. Organizations may use different data formats, compliance frameworks, cybersecurity standards, and technological architectures.There are also concerns around computational costs, latency, and standardization. Smaller institutions may struggle to invest in the infrastructure and expertise required to participate effectively in federated ecosystems.

Additionally, governance failures within one participant institution can still introduce vulnerabilities across the broader network. For many organizations, the challenge is no longer understanding the value of federated systems. The challenge is operational execution.

CONCLUSION

Federated data infrastructure is gradually emerging as one of the most important architectural shifts shaping the future of the digital economy. As cybersecurity risks increase, privacy regulation expands, and artificial intelligence systems become more data-intensive, organizations are searching for ways to collaborate without sacrificing security, confidentiality, or control. Federated models offer a practical pathway toward that balance.

For financial institutions, governments, healthcare systems, and technology companies, the implications are significant. These systems could fundamentally reshape how data is governed, shared, analysed, and monetised in the coming years. The long-term future of digital innovation may not belong solely to organizations that collect the most data. Increasingly, it may belong to those capable of collaborating securely while still preserving trust.



DIGITAL-BY-DESIGN GOVERNMENT MODELS: THE GLOBAL SHIFT TOWARDS SMARTER PUBLIC SERVICE SYSTEMS

Around the world, governments are under growing pressure to become faster, smarter, and more responsive. Citizens increasingly expect public services to work with the same speed and simplicity they experience in digital banking, e-commerce, and mobile applications. Long queues, paper-heavy processes, fragmented government databases, and slow approvals are becoming harder to justify in a highly digital global economy.In response, many countries are moving towards what is now commonly described as "digital-by-design" government models.

Unlike traditional digitization efforts, which simply convert existing manual processes into electronic formats, digital-by-design governance involves building public systems around digital infrastructure from the very beginning. It treats technology not as an add-on, but as the foundation upon which public administration, service delivery, regulation, and citizen engagement are structured.

This shift is gradually redefining how governments operate globally.

WHAT DOES "DIGITAL-BY-DESIGN" ACTUALLY MEAN?

A digital-by-design government is one where public services, administrative systems, and citizen interactions are intentionally developed around integrated digital infrastructure. The objective is not merely to place government forms online. Rather, it is to redesign how the state functions using digital systems as the primary operating architecture. Under this model, services such as identity verification, tax filing, licensing, healthcare access, public procurement, immigration processes, social welfare payments, and regulatory compliance become digitally integrated and interconnected.

Ideally, citizens should not repeatedly provide the same information across multiple government agencies. Systems communicate with each other securely, processes become automated, and services become significant-

ly faster and more accessible. Globally, countries such as Estonia are frequently cited as leading examples of digital-first governance. Estonia's digital identity ecosystem allows citizens to access a wide range of public services online, including voting, healthcare records, taxation, and company registration.

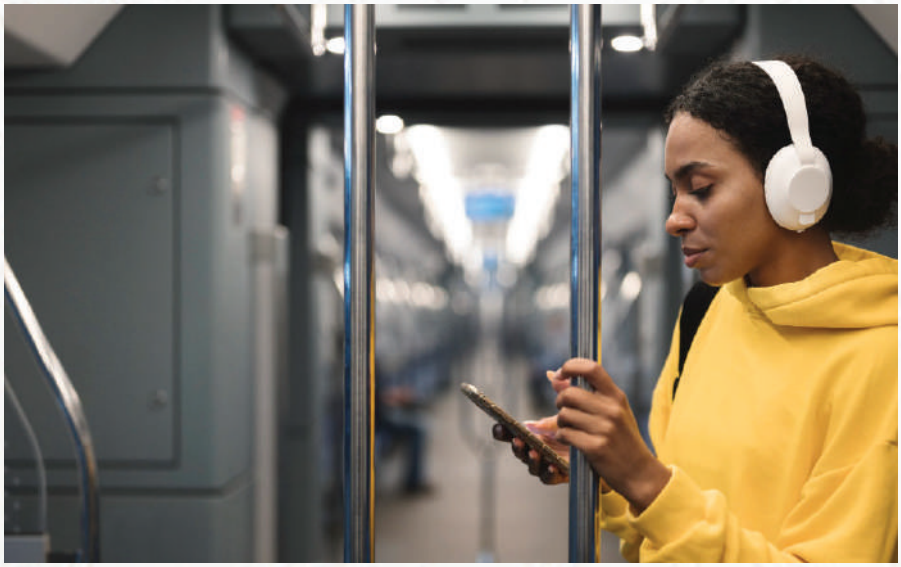
Similarly, Singapore has heavily invested in integrated digital public infrastructure, while countries such as India have built large-scale digital identity and payment systems supporting millions of citizens.
The broader lesson is becoming increasingly clear. Governments that successfully integrate digital infrastructure into public administration often improve efficiency, transparency, accessibility, and economic participation simultaneously.

WHY GOVERNMENTS ARE MOVING IN THIS DIRECTION

Several factors are driving the rise of digital-by-design governance globally. First is efficiency. Traditional public administration systems are often slow, fragmented, and expensive to maintain. Paper-based processes increase delays, duplication, and administrative overhead. Digital systems reduce processing times, improve data management, and simplify interactions between governments, businesses, and citizens.

Second is public expectation. Citizens increasingly compare government services to private-sector digital experiences. A person who can open a bank account or order products online within minutes naturally expects similar convenience from public services. Third is economic competitiveness.

Governments increasingly recognise that efficient digital infrastructure supports investment, entrepreneurship, financial inclusion, and innovation. Business registration systems, digital tax platforms, electronic procurement systems, and online licensing frameworks all contribute to a more efficient business environment.



Finally, digital government systems are becoming increasingly important for transparency and accountability. Properly designed digital systems can reduce opportunities for corruption, improve record keeping, and strengthen regulatory oversight.

THE ROLE OF DIGITAL PUBLIC INFRASTRUCTURE

At the centre of most digital-by-design government models is digital public infrastructure.

This includes systems such as:
- digital identity platforms;
- interoperable payment systems;
- government data exchanges;
- cybersecurity frameworks;
- digital registries; and
- secure cloud infrastructure.

Without these foundational systems, large-scale digital governance becomes difficult to sustain.
One of the clearest global trends today is the growing importance of digital identity systems.

Digital identity allows governments to authenticate citizens securely across multiple services. It also enables financial inclusion, digital payments, healthcare access, and electronic verification systems.

Countries that have invested heavily in digital identity infrastructure are increasingly seeing broader economic benefits beyond government administration itself.

THE AFRICAN CONTEXT

Across Africa, digital government initiatives are accelerating, although implementation levels vary significantly between countries. Governments are increasingly digitizing tax systems, passport applications, land registration, business incorporation, social intervention payments, and national identification programmers.

The COVID-19 pandemic also accelerated digital public service adoption across many jurisdictions by exposing weaknesses within manual administrative systems. Countries such as Rwanda, Kenya, and Nigeria have made substantial investments in digital service delivery infrastructure in recent years. In Ghana, initiatives around digital property addressing, mobile money interoperability, online business registration, and digital identification systems reflect broader efforts to modernize public administration and improve service accessibility.
However, the continent still faces important structural challenges, including inconsistent internet access, cybersecurity vulnerabilities, digital literacy gaps, fragmented databases, and infrastructure limitations. These realities mean that digital transformation within government must remain inclusive and carefully implemented to avoid widening existing inequalities.

THE FUTURE OF GOVERNMENT MAY BE API-DRIVEN

One of the more interesting developments globally is the emergence of governments that increasingly function like interconnected digital platforms.Public agencies are beginning to use APIs, automation tools, artificial intelligence, cloud computing, and interoperable databases to improve coordination and service delivery.

This could eventually reshape how citizens interact with the state entirely. In the future, tax filings may become largely automated. Licences may renew digitally without manual intervention. Welfare systems may use real-time verification tools. Regulatory reporting may become integrated directly into digital business systems. In many respects, governments are slowly evolving from administrative institutions into digital service ecosystems.

CONCLUSION

Digital-by-design government models are no longer futuristic policy concepts. They are becoming practical governance realities across both developed and emerging economies. The shift reflects a broader understanding that effective governance in the digital age requires more than simply putting services online. It requires redesigning public systems around connectivity, interoperability, efficiency, and citizen experience.

For governments globally, the challenge is not whether digital transformation will happen. It is whether it will happen in a way that is secure, inclusive, transparent, and sustainable.The countries that succeed in this transition are likely to build not only more efficient governments, but also more competitive economies and more resilient public institutions in the years ahead.

AI FINANCIAL CO-PILOTS

AI Financial Co-Pilots are intelligent assistants embedded into financial workflows that help individuals, teams, and businesses make faster and more informed financial decisions. Unlike traditional dashboards or reporting tools, these systems actively interpret financial data, generate insights, and suggest actions in real time.

In 2026, AI co-pilots are becoming central to financial operations in both start-ups and enterprise environments. They are being integrated into accounting systems, banking platforms, investment tools, and treasury management systems.

These tools can perform tasks such as forecasting cash flow, analyzing spending patterns, optimizing budgets, recommending investment strategies, and even drafting financial reports. In more advanced systems, they can also execute actions such as scheduling payments, reallocating budgets, or flagging financial risks subject to human approval or automated thresholds.

The key shift is from passive financial dashboards to interactive, decision-support systems. Businesses are increasingly relying on AI co-pilots to reduce cognitive load on finance teams and improve speed, accuracy, and strategic clarity in financial management.

PREDICTIVE COMPLIANCE SYSTEMS

Predictive Compliance Systems represent a shift from traditional reactive compliance to proactive, AI-driven risk anticipation. Instead of detecting breaches after they occur, these systems continuously analyze financial transactions, user behavior, regulatory updates, and internal workflows to predict where compliance risks are likely to emerge.

In 2026, this trend is being driven by the growing complexity of global regulation, the scale of digital financial transactions, and the use of AI in financial decision-making. Businesses are no longer dealing with compliance as periodic reporting; compliance is becoming a real-time, embedded function within operational systems.

These systems typically combine machine learning models, natural language processing for regulatory updates, and behavioral analytics to flag anomalies before they escalate into violations. For example, they can identify suspicious transaction patterns, anticipate AML risks, or detect inconsistencies in cross-border financial flows.

The strategic value is significant: businesses reduce regulatory exposure, avoid penalties, improve audit readiness, and build stronger trust with regulators and investors. Predictive compliance is effectively transforming compliance from a legal obligation into a strategic intelligence layer within financial systems.

06

CONSUMER INSIGHTS – WHAT CONSUMERS NEED TO KNOW

LOST PHONE, LOST MONEY? SECURING YOUR DIGITAL WALLETS.

In our increasingly connected world, smartphones have become essential tools for managing our daily lives. They serve not only as communication devices but also as gateways to our banking and financial information. With a simple tap, we can transfer money, pay bills, access digital wallets like Apple Pay, Google Pay and banking apps.

While smartphones offer unparalleled convenience, they also pose a significant risk in the event of loss or theft, as your financial assets and sensitive information become susceptible to unauthorized access. A lost device can potentially lead to substantial monetary losses, identity theft, and a prolonged hassle to regain control of your accounts. Therefore, understanding the right steps to take immediately after losing your phone and implementing preventive measures is important to safeguard your digital wallets and financial security. Below are some practical tips and steps to help safeguard your financial assets and sensitive information in the event your smartphone is lost or stolen.

1. Act Quickly and Stay Calm

The first and most important step when you realize your phone is missing is to remain calm. Panic can cloud judgment and lead to reckless actions, increasing the risk of exposing your personal and financial information. Take a few moments to assess the situation logically and remember, prompt action can often prevent unauthorized access and minimize potential damage.

2. Use Remote Tracking and Lock Features

Most smartphones come equipped with built-in security features designed to help locate and secure your device remotely, such as Find My iPhone for Apple devices and Find My Device for Android. To utilize these features, you should log into your account from another trusted device or computer and then locate your phone on the map to determine if it is nearby location. If the device is still powered on and connected to the internet, you can make it ring

loudly to help locate it if it is nearby. In event where you are certain the device has been stolen, then you should immediately select the option to lock it remotely. Once locked, your phone will prevent anyone from unlocking it without your passcode or biometric authentication.

3. Notify Your Financial Institutions Immediately

Your digital wallets and banking apps hold sensitive information that can be exploited if accessed by malicious actors. If you misplace your phone, immediately contact your bank and financial institutions to report the incident. Many banking apps offer options to log out remotely or suspend access temporarily. You should also ask your bank to flag or freeze your accounts if you suspect that the thief has access to your login details. Prompt notification enables the bank to monitor for suspicious transactions, block unauthorized activity, and prevent further financial damage.

4. Change Passwords and Enable Two-Factor Authentication

Once your device is secured or replaced, change all passwords associated with your financial accounts, digital wallets, email, and other sensitive services. This action prevents unauthorized users from using saved login credentials to access your accounts. Additionally, enable two-factor authentication (2FA) for your financial and email accounts. Two factor authentication (2FA) adds an extra layer of security by requiring a second form of verification, such as a code sent to your email or a biometric confirmation. This process ensures that even if someone attempts to use old login details, they will be thwarted by the additional security measures.

5. Remove Sensitive Apps and Data

If your device supports remote wiping, use the tracking app option to erase all data from your phone, especially if you believe the phone was stolen or cannot be recovered. For digital wallets, ensure that the apps are logged out and that no sensitive information is stored. Some banking apps and digital wallets allow you to disable biometric authentication temporarily until you can regain control of your account. Be cautious to make sure you are confident your device is truly lost or stolen before performing a remote wipe, as it is a permanent action.

6. Monitor Your Accounts for Suspicious Activity

After losing your phone, stay vigilant regularly to review your bank and digital wallet transactions over the subsequent weeks. Look out for any unfamiliar or unauthorized transactions. If you notice anything suspicious,

report it immediately to your bank or digital wallet provider. Early detection can help you take swift action to dispute charges, block further access, and prevent larger financial losses. Monitoring is an ongoing process that reinforces your security and helps catch potential threats early.

7.Implement Preventive Measures for Future Security

To minimize the risk of future incidents, implement preventive measures such as regularly backing up data, using strong, unique passwords with biometric security, installing security apps that can locate, lock, or wipe your device remotely, and avoid storing sensitive financial information directly on your phone unless encrypted and protected.

In conclusion, losing your phone can pose significant risks to your financial security, but by acting swiftly and following the necessary steps such as locating and locking your device remotely, notifying your financial institutions, changing passwords, enabling two factor authentication, removing sensitive data, and monitoring your accounts you can mitigate potential damages. Also, implementing proactive security measures for the future like regular backups, strong passwords, and device protection apps is essential to safeguarding your digital wallets and personal information. Staying vigilant and prepared ensures that you can better protect your assets and recover quickly in the unfortunate event of phone loss or theft.

07

INSIGHTS

THE IMPORTANCE OF RISK AND MITIGATION MEASURES FOR PAYMENT SERVICE PROVIDERS IN GHANA

Introduction

Ghana's payment services landscape has undergone a remarkable transformation over the past decade. From mobile money to digital wallets and payment gateways, the infrastructure supporting financial transactions in the country has expanded at a pace few anticipated. With that expansion comes responsibility. For Payment Service Providers (PSPs), operating in this space is not simply a matter of building good technology or acquiring a licence from the Bank of Ghana. It requires a disciplined, documented approach to identifying, assessing, and mitigating the risks that come with handling other people's money at scale.

Risk is not a theoretical concern. It is baked into the daily operations of every PSP. The question is not whether risk exists but whether the organisation has the frameworks, the culture, and the legal infrastructure to manage it responsibly.

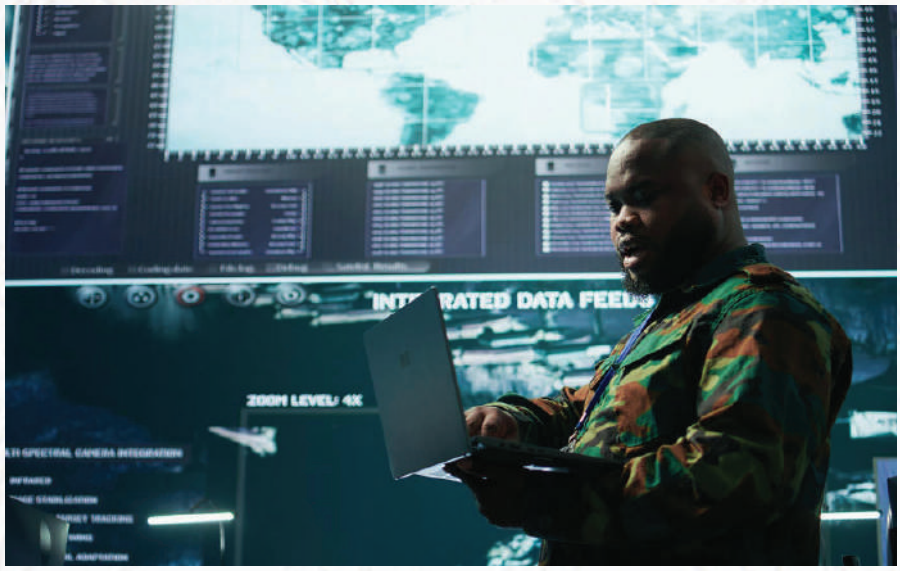
Why Risk Management Matters for PSPs

Payment Service Providers occupy a uniquely sensitive position in the financial ecosystem. They sit between consumers, merchants, banks, and regulators. A single failure, whether it is a fraud incident, a liquidity shortfall, or a regulatory breach, does not stay contained. It ripples. Customers lose trust. Partners reassess their exposure. Regulators take notice. The reputational and financial consequences can be severe and, in some cases, existential.

Ghana's regulatory framework has evolved to reflect this reality. The Payment Systems and Services Act, 2019 (Act 987) establishes the foundational legal framework under which PSPs operate. The Anti-Money Laundering Act, 2020 (Act 1044), imposes specific obligations around customer due diligence and suspicious transaction reporting. The Cybersecurity Act, 2020 (Act 1038) requires incident reporting to the Cyber Security Authority. The Data Protection Act, 2012 (Act 843) governs how customer data must be handled. Together, these instruments signal something important: the

Bank of Ghana and Ghana's broader regulatory architecture expect PSPs to be proactive, not reactive, about risk.

A PSP that treats compliance as a box-ticking exercise is a PSP that is eventually going to be caught out. Proper risk management is not about satisfying a regulatory submission. It is about building an organisation that can actually survive and grow.



The Six Risk Categories Every PSP Must Address

There are six core risk categories that any serious PSP operating in Ghana must have documented measures for.

Market risk arises from changes in interest rates, inflation, exchange rate volatility, and shifts in the competitive landscape. For a PSP operating in Ghana, the depreciation of the Cedi is not an abstract macroeconomic fact. It is a real operational variable that affects liquidity, pricing, and the value of settlement obligations. Without a documented foreign exchange risk policy and defined early warning indicators, a PSP is flying blind.

Liquidity risk is perhaps the most operationally immediate. The inability to meet financial obligations as they fall due is not just a technical accounting problem. It is a crisis. PSPs must maintain documented minimum liquidity thresholds quantified in actual Ghana Cedi terms, not just as a ratio or a percentage of operational costs. Committed credit facilities need to be in place, evidenced, and reviewed regularly. Telling regulators that you maintain access to overdraft facilities means very little if you cannot show which institution has committed to what amount.

Fraud risk is the area where PSPs are most exposed to both financial loss and reputational damage. Internal fraud, external social engineering, transaction manipulation, and identity theft are persistent threats. Robust Know Your Customer procedures, multi-factor authentication, anomaly detection systems, and strict segregation of duties are non-negotiable. Critically, these must align with Ghana's AML framework and the reporting obligations owed to the Financial Intelligence Centre. Legal risk is broader than most PSPs appreciate. It covers not just regulatory non-compliance but also poorly drafted contracts, inadequate data protection practices, and the absence of a clear legal review protocol for material decisions. A PSP that engages legal counsel only when things go wrong has already paid a higher price than necessary. Legal oversight should be embedded in operations, not called in as a fire brigade.

Credit risk is relevant wherever a PSP extends credit, provides post-paid services, or accumulates receivables. The methodology for provisioning must be defensible. The IFRS 9 Expected Credit Loss model is the appropriate standard, and the absence of a documented debt recovery escalation path is a gap that regulators will identify. Periodic customer performance reviews and timely receivables tracking are not optional extras.

Funding risk addresses the fundamental question of whether the PSP can sustain itself. Capital adequacy must be calibrated against the Bank of Ghana's minimum requirements for licensed PSPs under Act 987, with a clear distinction between operating capital and settlement float. These are not the same thing and they should

not be treated as the same thing in any financial or regulatory document.

The Role of Legal Infrastructure

One dimension of risk management that is frequently underweighted by PSPs is the legal infrastructure that underpins the entire framework. Policies and procedures are only as effective as the legal and institutional scaffolding behind them. A compliance register that lists obligations without naming the specific statute and the specific officer responsible for tracking it is not a compliance register. It is a template. PSPs should ensure that their Legal and Compliance function has a clearly defined role in the risk governance structure. This includes regulatory liaison, contract sign-off, incident escalation, and the annual policy review cycle. Monitoring and reporting must have defined frequencies, clear escalation thresholds, and named responsible officers. Quarterly risk reports to management and an annual consolidated report to the Board are a minimum expectation. Where incidents cross the statutory reporting thresholds under Acts 987 and 1038, notification to the relevant authority is not discretionary.

Conclusion

Risk management is not a constraint on growth. Properly designed, it is one of the most powerful enablers of it. A PSP that can demonstrate to the Bank of Ghana, to investors, and to partners that it understands its risk landscape, has documented and functional mitigation measures, and operates within the requirements of Ghana's regulatory framework is a PSP that will attract confidence. That confidence translates into better commercial relationships, stronger licensing positions, and sustainable operations.

The PSPs that will define Ghana's digital financial services sector over the next decade are not necessarily those with the most sophisticated technology. They are the ones that build the right foundations from the outset. Risk management, done properly, is one of those foundations

LIES IN HIGH DEFINITION: THE RISE OF DEEPFAKES, DISINFORMATION AND FAKE NEWS ON SOCIAL MEDIA IN GHANA

The digital revolution has transformed how information is produced, distributed, and consumed. Social media platforms have effectively become the modern public square where political discourse unfolds, reputations are built or destroyed, and public opinion is shaped in real time.

Yet this unprecedented democratization of communication has also introduced a dangerous new reality. Falsehoods can now travel faster, appear more convincing, and reach millions before the truth even begins to surface.

In recent years, the emergence of artificial intelligence tools capable of generating highly realistic images, videos, and audio has added a new dimension to the problem of misinformation. These AI-generated manipulations, commonly referred to as deepfakes, can make it appear that individuals said or did things they never actually said or did. When such fabricated content circulates widely on social media, it can mislead citizens, damage reputations, influence elections, and erode trust in institutions.

Ghana has not been immune to this phenomenon. As internet penetration increases and social media platforms become the primary source of news for many citizens, the spread of misinformation, fake news, and manipulated digital content has become an increasingly serious concern.

In light of the above, this article seeks to examines the growing threat posed by deepfakes, disinformation, and fake news in Ghana's social media ecosystem. It explores how these technologies are reshaping the information landscape, the risks they pose to democratic governance and public trust, the current legal and regulatory framework in Ghana, and the practical steps that can be taken to curb the spread of digitally manufactured falsehoods.

THE NEW INFORMATION BATTLEFIELD

For much of Ghana's post-independence history, the flow of information was largely dominated by traditional media institutions such as radio, television, and newspapers. These institutions operated within editorial structures that required some level of verification, professional judgment, and accountability.The emergence of digital platforms such as Facebook, WhatsApp, X, and TikTok has fundamentally changed this landscape.

Today, anyone with a smartphone can create content and distribute it instantly to thousands or even millions of people. While this development has democratized communication and empowered citizen journalism, it has also removed many of the traditional safeguards that once filtered inaccurate or misleading information.

As a result, misinformation can spread at extraordinary speed, especially through private messaging platforms where forwarded content is rarely verified before it is shared. Researchers studying misinformation trends on social media have consistently found that visual formats such as images and videos are significantly more persuasive than plain text, particularly when they appear authentic. This is precisely where deepfake technology has become especially powerful.

UNDERSTANDING THE LANGUAGE OF DIGITAL FALSEHOODS

Before examining the scale of the problem, it is important to understand the terminology that is frequently used when discussing online information disorders. The terms misinformation, disinformation, fake news, and deepfakes are often used interchangeably in public discourse, yet they refer to distinct concepts.

a. Misinformation

Misinformation refers to false or inaccurate information that is shared without the intent to deceive. In many cases, individuals who circulate misinformation genuinely believe that the content they are sharing is true.

For example, a social media user may forward a message on WhatsApp claiming that a particular herbal remedy cures a disease or that a certain government policy has been announced, even though no such announcement exists. The user may not intend to mislead others but may simply be passing along information they assume to be correct.

Because misinformation often spreads through trusted social networks such as family groups or community forums, it can be particularly difficult to correct once it begins circulating.

b. Disinformation

Disinformation, by contrast, refers to false information that is deliberately created and distributed with the intention of misleading people. Disinformation campaigns are often strategic and coordinated. They may involve the deliberate manipulation of images, videos, or narratives to influence public opinion, damage reputations, or create political advantage.

Globally, disinformation has been used to interfere with elections, manipulate financial markets, and fuel political polarization.

The key distinction between misinformation and disinformation therefore lies in intent. While misinformation may be shared unknowingly, disinformation is intentional-

ly designed to deceive.

c. Fake News

The term fake news gained widespread prominence during the last decade and generally refers to fabricated or misleading content that is presented in the format of legitimate news reporting.

Fake news articles are often designed to resemble credible news reports but contain entirely false or misleading information. In many cases, such stories are circulated online to attract website traffic, generate advertising revenue, or advance political narratives.

Although the term has sometimes been used loosely to dismiss unfavorable reporting, at its core fake news refers to fabricated stories presented as legitimate journalism.

d. Deepfakes

Deepfakes represent the newest and perhaps most technologically sophisticated form of digital deception.

The term deepfake originates from "deep learning," a branch of artificial intelligence that uses neural networks to analyze large datasets and generate synthetic media. Using these tools, it is possible to create highly convincing images, audio recordings, and videos of individuals saying or doing things they never actually said or did.

Unlike traditional forms of fake content that rely on edited photographs or misleading text, deepfakes can simulate facial movements, voice patterns, and body language with remarkable accuracy.

This ability to fabricate realistic visual evidence poses a profound challenge for societies that traditionally rely on video recordings as proof of events.

DEEPFAKE INCIDENTS IN GHANA AND AROUND THE WORLD

The risks posed by deepfakes are no longer theoretical or speculative. Several incidents in Ghana and internationally illustrate how artificial intelligence is already being used to create misleading or deceptive digital content.In Ghana, one widely circulated manipulated video in 2025 appeared to show former President Nana Addo Dankwa Akufo-Addo sitting beside social media personality Serwaa Broni on a private jet. Investigations later revealed that the video had been generated using artificial intelligence to animate an altered image that had originally circulated several years earlier. The clip quickly spread across social media platforms, demonstrating how modern technology can revive old political controversies in new and more convincing forms.

In recent years, the emergence of artificial intelligence tools capable of generating highly realistic images, videos, and audio has added a new dimension to the problem of misinformation.

Similarly, a manipulated video circulated online falsely depicting Ghana's Minister of Education Haruna Iddrisu promoting what appeared to be a government-backed investment platform promising unrealistic financial returns. Authorities later clarified that the video was entirely fabricated and intended to deceive members of the public. Beyond Ghana, several high-profile global incidents have demonstrated the extraordinary power of deepfake technology.

Perhaps one of the most widely discussed deepfake incidents occurred in 2024 when sexually explicit AI-generated images of global music star Taylor Swift spread rapidly across social media platforms, attracting millions of views before they were eventually removed. The incident sparked widespread debate about the dangers of AI-generated sexual deepfakes and the urgent need for stronger digital protections. Taken together, these incidents demonstrate that deepfakes are not merely a technological novelty. They represent a rapidly evolving tool that can

be used for political manipulation, financial fraud, reputational harm, and online harassment.

GHANA'S LEGAL AND REGULATORY EFFORTS TO COMBAT FAKE NEWS, MISINFORMATION AND DISINFORMATION

The rapid spread of misinformation, disinformation, and manipulated digital content has forced governments around the world to reconsider how legal frameworks should address emerging digital threats. Ghana is no exception. While the country does not yet have legislation specifically dedicated to regulating deepfakes or artificial intelligence-generated media, several existing laws provide a foundation for addressing harmful online content.

One of the most important pieces of legislation in this regard is the Cybersecurity Act, 2020 (Act 1038). The Act establishes the Cyber Security Authority as the national body responsible for protecting Ghana's cyberspace, responding to cyber threats, and coordinating cybersecurity policy.

Under this legal framework, the Authority has the power to monitor cyber threats, promote digital safety awareness, and coordinate national responses to emerging digital risks including online fraud, digital impersonation, and cyber-enabled misinformation. Another important legal instrument is the Electronic Communications Act, 2008 (Act 775), which regulates electronic communications networks and services in Ghana. The Act gives regulatory authority to the National Communications Authority to oversee telecommunications and broadcasting operations in the country.

While the Act was enacted long before the emergence of generative artificial intelligence, its provisions relating to the misuse of electronic communications infrastructure can still be relevant in cases involving the deliberate distribution of harmful digital content.

In addition, criminal law provisions may apply where manipulated digital content causes reputational damage or financial harm. The Criminal Offences Act, 1960 (Act 29) contains provisions relating to fraud, false pretenses, and the publication of false statements capable of causing public harm.

Although these laws were not originally designed with deepfakes in mind, they may still provide a legal basis for prosecuting individuals who create or distribute harmful digital fabrications.

However, Ghana is also taking steps to introduce more targeted legislation to address the growing threat of misinformation and disinformation in the digital space. In July 2025, the Minister for Communication, Digital Technology and Innovations, Samuel Nartey George, announced that the government was advancing a proposed National Misinformation and Disinformation, Hate Speech And Publication Of Other Information Bill aimed at strengthening legal safeguards against the deliberate creation and spread of harmful digital content.

The proposed legislation is expected to provide a clearer enforcement framework for regulatory authorities while maintaining constitutional protections for freedom of expression. Once presented

to Parliament and subsequently enacted and assented into law, the Bill is anticipated to form a key part of Ghana's broader efforts to protect the integrity of the country's digital ecosystem, promote responsible online discourse, and enhance digital literacy. Beyond legislation, several institutions play an important role in safeguarding the integrity of Ghana's information environment.

The Cyber Security Authority has become increasingly active in monitoring emerging cyber threats, including digital impersonation and AI-enabled scams. Similarly, the National Communications Authority regulates telecommunications networks and has the authority to address misuse of digital communication infrastructure.

The National Media Commission also plays a crucial role in safeguarding responsible journalism and maintaining ethical standards within the media industry. In addition to these regulatory bodies, several civil society organizations and digital rights groups in Ghana have taken on the role of fact-checking online content and exposing misinformation campaigns. These organizations have become an essential part of the country's digital accountability ecosystem.

THE EMERGING CHALLENGE OF ARTIFICIAL INTELLIGENCE GOVERNANCE

Notwithstanding all the above, it is also important to note that the rise of generative artificial intelligence has introduced new regulatory challenges that many countries are still struggling to address.

Unlike traditional misinformation, which often relies on edited images or misleading text, deepfakes can produce highly convincing audio-visual material that may be extremely difficult for ordinary citizens to detect.

The challenge is further complicated by the global nature of social media platforms. Many of the companies that operate major digital platforms are headquartered outside Ghana, making national enforcement efforts more complex.

In addition, generative AI tools are increasingly accessible to the public. Individuals with little technical knowledge can now generate synthetic videos or voice recordings using freely available software.

This means that the threat of digital manipulation is no longer limited to sophisticated state actors or organized disinformation networks. In many cases, a single individual can create content capable of misleading thousands of people.

RECOMMENDATIONS FOR THE WAY FORWARD

Addressing the growing threat of deepfakes and digital disinformation will require a comprehensive approach that combines legal reform, technological solutions, and public education.

Several policy measures could significantly strengthen Ghana's ability to respond to this emerging challenge.

First, Ghana should begin developing a comprehensive legal framework for artificial intelligence governance. Such legislation should clearly define synthetic media, establish liability for malicious deepfake creation, and impose penalties for the deliberate use of AI-generated content to commit fraud, defamation, or election interference.

Second, regulators should strengthen cooperation with social media platforms to ensure the rapid detection and removal of manipulated digital content. Platforms must take greater responsibility for identifying AI-generated media and preventing its misuse.

Third, investment in digital literacy education is essential. Citizens must be equipped with the skills necessary to critically evaluate online information and identify potential misinformation.

Fourth, Ghana should encourage the development of AI detection technologies capable of identifying manipulated audio and video content. These tools are becoming increasingly important as deepfake technology becomes more sophisticated.

Finally, stronger collaboration between government agencies, media organizations, civil society groups, and academic institutions will be essential in building a resilient information ecosys-

tem capable of resisting disinformation campaigns.

CONCLUSION

The digital age has brought extraordinary opportunities for communication, innovation, and democratic participation. Yet it has also introduced new vulnerabilities that societies must confront. Deepfakes, misinformation, disinformation, and fake news represent one of the most significant challenges facing modern information ecosystems. As artificial intelligence continues to evolve, the ability to fabricate convincing digital content will only become more sophisticated. For Ghana, the task ahead is clear. Protecting the integrity of the country's information environment will require a careful balance between technological innovation, legal reform, responsible media practices, and an informed citizenry.

The battle for truth in the digital age is no longer fought only in newsrooms or courtrooms. It is increasingly fought on the screens of smartphones, in social media feeds, and in the algorithms that shape what billions of people see every day. Ensuring that truth continues to prevail in that environment is one of the defining challenges of our time.

08

INDUSTRY PLAYERS' SPOTLIGHT

FIDO: EXPANDING FINANCIAL ACCESS THROUGH DIGITAL LENDING IN GHANA

FIDO Ghana is one of the notable players shaping Ghana's evolving fintech ecosystem. Operating as a digital lending and financial services platform, FIDO has positioned itself as a technology-driven company focused on improving access to credit and financial inclusion for underserved individuals and small businesses across Ghana.

Founded in 2015 and headquartered in Accra, FIDO operates as a licensed Tier 3 Microfinance Institution under the supervision of the Bank of Ghana. The company has become well known for offering instant mobile-based loans without the traditional barriers associated with conventional banking institutions.

What FIDO Does

FIDO primarily provides digital micro-loans through its mobile application. Its platform allows users to apply for loans directly from their smartphones and receive approval decisions within minutes. Unlike many traditional financial institutions, the company does not generally require collateral or guarantors before disbursing loans.

The company serves:
- Individuals with limited or no formal credit history
- Informal sector workers
- Small business owners and micro-entrepreneurs
- Salaried and self-employed professionals

FIDO uses artificial intelligence (AI) and machine learning systems to assess customer risk profiles and make lending decisions in real time. Instead of relying solely on traditional banking records, the platform analyses alternative data sources and user behavior to determine creditworthiness.

FIDO's Role in Ghana's Fintech Space

FIDO represents a broader shift within Ghana's fintech industry toward embedded finance, digital credit, and financial inclusion. Ghana has experienced significant growth in mobile money adoption over the past decade, creating opportunities for fintech companies to build financial products around mobile-first infrastructure.

Within this ecosystem, FIDO

has distinguished itself through:
- AI-powered credit scoring
- Fully digital loan processing
- Fast loan disbursement
- Focus on underserved and unbanked populations
- Expansion into broader financial services

The company has been described as part of the growing wave of African fintechs leveraging technology to close financing gaps for populations traditionally excluded from formal banking systems.

Financial Inclusion and Economic Impact

One of FIDO's strongest contributions to the Ghanaian market is its role in promoting financial inclusion.

By digitizing the lending process and reducing entry barriers, FIDO provides faster access to working capital and emergency funding for users who may otherwise remain financially excluded. According to investment and industry reports, millions of loans have been disbursed through the platform since its launch.

This approach has made digital lending platforms increasingly important for Ghana's SME and informal business sectors, where access to short-term capital can significantly affect business continuity and growth.
Technology and Innovation
FIDO's business model is heavily technology-driven. The company's automated systems use:
- Machine learning algorithms
- Real-time fraud detection
- Alternative credit scoring systems
- Mobile-first infrastructure

This technological foundation allows the platform to process large numbers of applications efficiently while reducing operational costs. The company has also invested in research and development operations in Accra to strengthen its engineering and product development capabilities.

Investment and Growth
FIDO has attracted significant international investor interest over the years, reflecting growing confidence in Ghana's fintech market and Africa's digital finance sector more broadly.
The company has secured multiple rounds of funding, including:
- A $30 million Series A funding round in 2022
- Additional debt and equity financing in subsequent years
- Strategic financing partnerships with institutions such as Stanbic Bank Ghana, FMO, and BlueOrchard

Challenges and Industry Considerations

Like many digital lenders operating across emerging markets, FIDO operates within a highly competitive and closely scrutinized fintech environment. Digital lending platforms often face conversations around:
- Customer service quality
- Interest rates and repayment structures
- Data protection and cybersecurity
- Responsible lending practices

Public discussions on online forums show mixed customer experiences, reflecting both the convenience of instant digital lending and broader concerns associated with loan repayment pressures in the fintech lending sector.

As regulation in Ghana's fintech ecosystem continues to evolve, companies like FIDO are expected to operate within increasingly robust compliance and consumer protection frameworks.

Conclusion

FIDO has become an important participant in Ghana's fintech ecosystem by leveraging technology to expand access to credit and digital financial services. Through AI-driven lending systems, mobile accessibility, and a focus on underserved populations, the company reflects the growing transformation of financial services in Ghana and across Africa.
Its growth also highlights larger trends shaping the fintech industry today, including financial inclusion, embedded finance, alternative credit scoring, and the digitization of banking services. As Ghana's fintech sector continues to mature, companies like FIDO are likely to remain central to conversations around innovation, access to finance, and the future of digital banking in Africa.

09

PAST AND UPCOMING INDUSTRY EVENTS

GHANA LAUNCHES NATIONAL AI STRATEGY TO POSITION COUNTRY AS AFRICA'S LEADING ARTIFICIAL INTELLIGENCE HUB

President John Dramani Mahama has officially launched Ghana's National Artificial Intelligence Strategy (2025–2035), marking what government officials and technology leaders describe as a major step towards positioning the country as a leading artificial intelligence hub on the African continent.

The strategy seeks to drive the responsible adoption of artificial intelligence across critical sectors of the economy while promoting innovation, digital inclusion, job creation, and long-term economic transformation.

The launch event brought together senior government officials, members of the judiciary, policymakers, academics, technology experts, and development partners, all united around a broader national vision of building an AI ecosystem rooted in ethics, accountability, and Ghanaian values.

Chairing the event, the Speaker of Parliament Alban Kingsford Sumana Bagbin described the launch as a defining moment in Ghana's development journey.

While acknowledging the transformative potential of artificial intelligence across governance, healthcare, education, and economic systems, the Speaker of Parliament cautioned against pursuing technological advancement without ethical responsibility.

According to him, technological progress must remain guided by human values and public interest considerations rather than existing solely for innovation's sake.

He further reaffirmed Parliament's commitment to supporting the development of legal and regulatory frameworks capable of protecting citizens while enabling innovation and responsible technological growth.

Minister for Communication, Digital Technology, and Innovations, Samuel Nartey George, also stressed that Ghana's AI future must remain inclusive and aligned with local realities.

He noted that artificial intelligence has the potential to

improve education delivery, healthcare systems, agricultural productivity, financial services, and broader public sector efficiency if implemented responsibly.

According to the Minister, government intends to integrate AI systems into public sector operations while also introducing an Emerging Technologies Bill to provide legal backing for responsible AI deployment within the country.

He added that institutions such as the Data Protection Commission and the Cyber Security Authority would be strengthened to ensure effective oversight, cybersecurity protection, and ethical governance of AI technologies.

A detailed presentation on the strategy was delivered by Prof. Jerry John Kponyo, Principal Investigator and Scientific Director of the Responsible AI Lab at Kwame Nkrumah University of Science and Technology.

Prof. Kponyo explained that the strategy emerged from extensive consultations involving entrepreneurs, engineers, policymakers, researchers, think tanks, and traditional authorities across the country.

According to him, the framework reflects Ghana's broader ambition to become Africa's leading AI hub by 2035 through investments in talent development, digital infrastructure, research, and public sector innovation.

The strategy is structured around several key pillars, including AI education and training, youth empowerment, digital infrastructure development, data governance, applied AI research, and accelerated AI adoption across strategic sectors of the economy.

Among the targets outlined is a plan to train one million young people and 10,000 AI researchers by 2035 through reskilling programmes, start-up support initiatives, and expanded technology education.

The strategy also proposes integrating coding, data science, and artificial intelligence education into school curricula from the foundational level upward, while ensuring inclusion for persons with disabilities and participants within the informal sector.

On infrastructure, government intends to support the development of innovation hubs beyond Accra, strengthen energy capacity, and establish advanced AI computing infrastructure within Ghana.

Prof. Kponyo, however, cautioned that the country must carefully manage risks associated with brain drain, digital inequality, job displacement, and excessive dependence on donor funding.

According to him, Ghana's AI ecosystem must ultimately become self-sustaining if the strategy is to achieve long-term success.

The event also featured remarks from Paul Baffoe-Bonnie, who examined artificial intelligence from the perspective of justice delivery and the rule of law.

The Chief Justice acknowledged the growing potential for AI to support areas such as legal research and case management but stressed that human judgment and accountability must remain central to judicial decision-making.

He warned that issues relating to transparency, bias, and accountability within AI systems could not be ignored, particularly in sensitive areas involving justice administration and constitutional rights.

Launching the strategy officially, President Mahama stated that Ghana intends to become an active participant in the global AI ecosystem rather than merely a consumer of foreign technologies.

According to the President, the country's AI agenda will prioritise inclusion, skills development, employment creation, and human-centred innovation.

To support implementation, government announced plans to invest approximately US$250 million towards the establishment of a world-class AI computing centre, alongside an additional US$20 million earmarked for the short- to medium-term rollout of the strategy.

The launch of the National AI Strategy is being viewed by many within Ghana's technology ecosystem as one of the country's most ambitious digital transformation initiatives in recent years.

Stakeholders at the event broadly agreed that while the strategy establishes an important framework for Ghana's AI future, its ultimate success will depend heavily on implementation, institutional coordination, sustainable funding, and the ability to translate policy ambitions into practical outcomes across the economy and public sector.

GHANA FINTECH AWARDS 2026 HIGHLIGHTS INDUSTRY'S RAPID EVOLUTION AND GROWING FOCUS ON INCLUSION, PARTNERSHIPS, AND DIGITAL INFRASTRUCTURE

Ghana's fintech ecosystem gathered in Accra last week for the fifth edition of the Ghana FinTech Awards, an event that not only celebrated innovation within the industry but also revealed how quickly the country's digital finance landscape is evolving.

Held on Saturday, 28 March 2026, the awards ceremony brought together fintech founders, financial institutions, regulators, payment service providers, technology companies, investors, and ecosystem stakeholders to recognize outstanding performance across the financial technology sector.

A total of 23 awards were presented across categories covering digital banking, financial inclusion, cybersecurity, agritech, edutech, remittances, payments infrastructure, and emerging technologies.

The event was organized by Arkel Limited in partnership with the Ghana Fintech and Payments Association, KPMG Ghana, and Fintech Management Solutions.

Beyond the awards themselves, the event reflected the broader maturity of Ghana's fintech ecosystem, particularly as digital finance continues to expand beyond basic payments into lending, infrastructure, partnerships, agriculture, education, and embedded financial services.

Organisers indicated that winners were selected through a four-stage evaluation process involving public nominations, independent product assessments, public voting, and final jury deliberations focused on measurable innovation and market impact during the year under review.

One of the standout names of the night was Fido, which emerged as the dominant winner across multiple categories.

The company secured four major awards, including Fintech Company of the Year, Fintech for Financial Inclusion Firm of the Year, Fintech & Bank Partnership of the Year for its EasySave collaboration with Access Bank Ghana, and Fintech & Non-Bank Partnership of the Year for its FidoBiz Entrepre-

neur Loans partnership with Bolt.

In addition, Philip Twum of Fido was named Young Fintech Leader of the Year.
Industry observers noted that the recognition reflected growing market attention towards fintech companies capable of combining innovation with practical financial inclusion outcomes and strategic partnerships.

On the institutional side, GCB Bank recorded a strong showing, winning Best Commercial Bank with Digital Innovation as well as Mobile Banking App of the Year.
Patrick George Quantson of GCB Bank was also recognised as Fintech CTO/CIO of the Year.

The bank's performance was viewed by many as evidence that traditional financial institutions are increasingly adapting to the competitive realities of digital finance and innovation-led banking.
Another notable winner was Payaza Africa, which secured both IT/Tech Firm of the Year and Fintech Platform of the Year for its Give Platform.

The awards highlighted the growing importance of payment infrastructure providers within Africa's fintech ecosystem, particularly as digital transactions and interoperable payment systems continue to expand across the continent.

The event also reflected increasing recognition of diversity and inclusion within the fintech space.

EMTECH was awarded Female-Led Fintech Company of the Year, while Gillian Darko of Yellow Card received Fintech Personality of the Year (Female).

Their recognition reinforced the growing visibility of women within leadership positions across Africa's digital finance and emerging technology sectors.

Outside traditional banking and payments, the awards also demonstrated how fintech innovation is increasingly intersecting with agriculture and education.

GrowForMe won both Agritech of the Year and Emerging Technology of the Year for its Micro Aggregator product, reflecting the expanding role of digital finance solutions within agricultural value chains and rural financing systems.

Meanwhile, eCampus received Edutech of the Year, highlighting the continued convergence between financial technology, digital learning, and education accessibility.

Cybersecurity also emerged as an increasingly important theme throughout the awards.

Innovare Limited was named Cybersecurity Company of the Year, a category many analysts viewed as particularly significant given rising concerns around fraud, data protection, cyber resilience, and infrastructure security across digital financial ecosystems.

The prominence of partnership-focused awards also reflected a broader industry trend.

Two dedicated categories recognised fintech-bank and fintech-non-bank collaborations, reinforcing the growing understanding that the future of financial services will likely depend less on isolated operators and more on interconnected digital ecosystems involving banks, fintech firms, telecommunications companies, retailers, and platform businesses.

Several observers noted that Ghana's fintech ecosystem appears to be entering a more mature phase where long-term sustainability, infrastructure resilience, interoperability, compliance, and strategic collaboration are becoming just as important as innovation itself.

The continued emphasis on financial inclusion was another defining feature of the awards.

Winning products and platforms across categories consistently reflected efforts to expand access to formal financial services, digital savings, lending, remittances, and payment systems for underserved populations and SMEs.

This aligns with broader trends across Africa, where fintech continues to play a central role in bridging financial access gaps and accelerating digital economic participation.
As Ghana's fintech sector continues to evolve, the 2026 Ghana FinTech Awards offered more than a celebration of industry achievements. They provided a snapshot of where the ecosystem itself is heading.
Increasingly, the future of fintech in Ghana appears to be centred not only on payments and digital transactions, but also on ecosystem partnerships, embedded finance, infrastructure security, financial inclusion, and sector-wide digital transformation.

3I AFRICA SUMMIT 2026 POSITIONS GHANA AT THE CENTRE OF AFRICA'S DIGITAL FINANCE FUTURE

The 2026 edition of the 3i Africa Summit concluded in Accra after three days of high-level discussions focused on fintech innovation, digital infrastructure, cross-border payments, financial inclusion, and the future of Africa's digital economy.

Held from 6 to 8 May 2026 at the Destiny Arena in Accra, the summit brought together policymakers, regulators, central bankers, fintech founders, investors, telecommunications operators, development finance institutions, and technology leaders from across Africa and beyond.

The summit, which has increasingly established itself as one of Africa's major fintech and digital economy gatherings, was organised under the theme "The Next Frontier: Shaping Africa's Integrated FinTech Future." Discussions throughout the event reflected a broader continental push towards building more interconnected, inclusive, and resilient digital financial ecosystems.

This year's summit was co-organised by the Bank of Ghana and Development Bank Ghana in collaboration with Elevandi, a subsidiary of the Monetary Authority of Singapore, and the Global Finance and Technology Network. Organisers indicated that the summit attracted thousands of delegates from more than 60 countries, including regulators, fintech operators, investors, and innovation-focused institutions.
One of the major highlights of the summit was Ghana's announcement of plans to collaborate with other African countries to pilot a continental digital trade corridor aimed at improving cross-border commerce and financial integration within Africa.

Speaking during the summit, Vice President Jane Naana Opoku-Agyemang stated that Ghana would work alongside countries including Rwanda and Zambia to test systems supporting seamless digital transactions across borders. The proposed initiative is expected to focus on mobile money interoperability, harmonised electronic invoicing systems, and mutual recognition of digital identity systems for cross-border KYC verification.

Observers at the summit described the proposal as an important step towards supporting broader continental integration efforts under the African Continental Free Trade Area framework, particularly as African economies continue to push for greater intra-African trade and digital connectivity.

Another key theme dominating discussions was the growing need for Africa-led digital infrastructure capable of supporting

the continent's long-term fintech and innovation ambitions.

At one of the summit sessions, Fidelity Bank Ghana called for stronger investment in African-owned digital infrastructure, arguing that the continent's digital transformation agenda must be supported by locally driven systems rather than excessive dependence on external technological frameworks.

Discussions also focused heavily on digital public infrastructure, cybersecurity resilience, digital identity systems, open banking, tokenisation, artificial intelligence, and inclusive instant payment systems.

Participants repeatedly stressed that while Africa has made significant progress in financial inclusion through mobile money and fintech innovation, major gaps still remain in interoperability, digital infrastructure coordination, and regulatory harmonisation across jurisdictions.
The role of telecommunications operators and mobile money providers was also prominent throughout the summit.

MobileMoney LTD and MTN Ghana played visible roles in several panel discussions and keynote sessions focused on consumer protection, digital credit expansion, and responsible financial innovation.

Chief Executive Officer of MobileMoney LTD, Shaibu Haruna, highlighted the importance of balancing rapid fintech growth with strong consumer safeguards, particularly as digital credit products and mobile banking services continue expanding across African markets.

Across multiple sessions, there was a noticeable shift in tone from broad discussions about fintech potential towards more implementation-focused conversations around infrastructure, policy coordination, investment readiness, and ecosystem resilience.

Several participants noted that Africa's fintech ecosystem is entering a more mature phase where attention is increasingly moving beyond startup growth alone towards long-term sustainability, regulatory architecture, interoperability, and continental-scale digital integration.

Artificial intelligence and digital public infrastructure also featured prominently during discussions, reflecting growing recognition that Africa's digital economy will depend heavily on reliable identity systems, interoperable payment rails, secure data governance frameworks, and scalable infrastructure capable of supporting future innovation.

The summit additionally hosted policy dialogues, innovation showcases, startup exhibitions, and investment discussions involving founders, venture capital firms, regulators, and development finance institutions.
Industry stakeholders broadly described the 2026 summit as evidence of Ghana's increasingly important role within Africa's fintech and digital transformation ecosystem.

Over the past few years, Ghana has steadily positioned itself as one of the continent's more active fintech and digital finance hubs through reforms in mobile money interoperability, payment systems regulation, digital banking, and financial inclusion initiatives.

The discussions at the Destiny Arena ultimately reflected a broader continental reality. Africa's digital economy is no longer centred solely on expanding access to digital payments. Increasingly, the focus is shifting towards building integrated digital ecosystems capable of supporting trade, investment, innovation, and economic growth at continental scale.

As the summit concluded, one message appeared consistently across discussions: Africa's next phase of fintech growth will likely depend less on isolated national systems and more on coordinated digital infrastructure capable of connecting markets, businesses, governments, and consumers across the continent.

Publisher's Notice or Disclaimer ©

The information provided in this document does not, and is not intended to, constitute legal advice; instead, all information, content, and materials are for general informational purposes only.

Readers should contact their lawyers to obtain advice with respect to any particular legal matter. No reader or user should act or refrain from acting on the basis of information in this document without first seeking legal advice from his or her lawyers.

The use of, and access to, this document or any other resources by the firm does not create an attorney-client relationship between the reader or user and the firm, key contacts, and contributors.

All liability with respect to actions taken or not taken based on the contents of this document is hereby expressly disclaimed. The content in this document is provided "as is;" no representations are made that the content is error-free or may be affected by subsequent changes in legislation on the subject matter.

For more information,

visit
www.sustineriattorneys.com

or follow us on **@SustineriAttorneys**

or call **+233302553892**