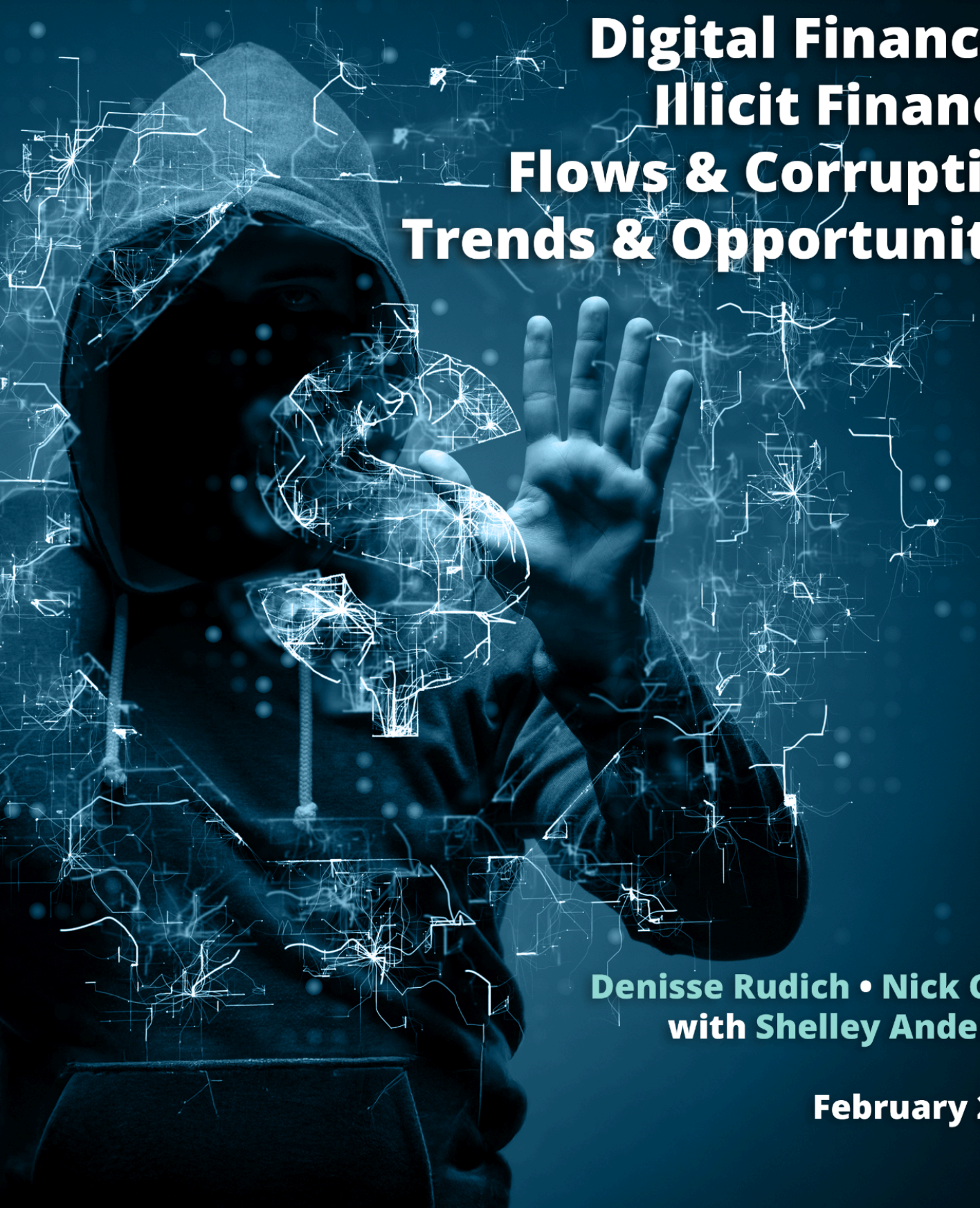
Alliance for Innovative Regulation



Digital Finance & Illicit Financial Flows & Corruption: Trends & Opportunities

Denisse Rudich • Nick Cook
with Shelley Anderson

February 2026

TABLE OF CONTENTS

INTRODUCTION 3

DIGITAL FINANCE 6

- Mobile Money 6
- Open Banking 10
- Crypto Assets 12
- Stablecoins 15

DIGITAL FINANCE TRENDS AND VULNERABILITIES 18

- Point of Sale (POS) / “Human ATMs” 18
- Agentic AI Payments and Stablecoins 18
- Deepfakes and Synthetic Identities 19
- Adaptive Digital Finance in Conflict Zones 19

RECOMMENDATIONS 22

- Apply Proportionate, Risk-Based AML/CFT Regulation Across Digital Finance 22
- Strengthen Digital Financial Literacy and Consumer Protection 22
- Accelerate Trusted, Interoperable Digital Identity Systems 23
- Improve Cross-Sector and Cross-Border Information Sharing 23
- Expand Access to Affordable Fraud Detection and Analytics 23
- Integrate Gender Dimensions into Risk Management and Consumer Protection 24
- Prepare Supervisory Frameworks for AI-Driven Finance and Automated Payments 24
- Embed Illicit Finance Controls into Stablecoin and Digital Trade Infrastructure 24

ABOUT THE PAPER 25

- Methodology 25
- About AIR 25
- Funded by GIZ 25
- With Special Thanks 25

1

INTRODUCTION

"Innovation has enormous potential to make finance more fair and inclusive, to make the financial system more competitive and healthy, and to make financial regulation more effective and efficient. At the same time, it carries great downside risk." – Jo Ann Barefoot[1]

Innovation in digital finance offers significant benefits for financial inclusion, economic growth and resilience, but it also creates new channels for laundering the proceeds of crime and for targeting previously unbanked and vulnerable communities. Enabled by mobile phones, internet connectivity and digital devices, digital finance is providing underserved populations with access to mobile bank accounts, financial services and digital wallets. This makes it easier to receive, store, and transfer value domestically and across borders.

In 2024, 79% of adults globally had either a bank account or mobile money account.[2] This expansion in account ownership has been substantially facilitated by rising smartphone adoption, which continues to lower barriers to accessing digital financial services. With more than 60% of the world's population now online, the opportunities for inclusive growth are substantial.[3] However, 1.4 billion people still lack access to formal financial services,[4] and even where access has improved, significant risks and vulnerabilities remain.

A growing set of vulnerabilities is emerging across the digital finance ecosystem. These include the deployment of new technologies by non-financial firms, extensive use of agent networks and outsourcing arrangements, limited regulation of new financial products, and weak or inaccessible redress mechanisms. Many consumers – particularly first-time users – remain inexperienced, financially illiterate and vulnerable. Privacy and security issues are also increasing as new forms of data are collected, shared and monetized.[5] Meanwhile, digital business models allow value to be created

---

[1] Jo Ann Barefoot, "Digital Technology Risks for Finance: Dangers Embedded in Fintech and Regtech" *Harvard Kennedy School: M-RCBG Associate Working Paper Series No. 151* (June 2020), available at: https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/AWP_151_final.pdf

[2] World Bank, *The Global Findex Database 2025*, (2025), available at: https://openknowledge.worldbank.org/entities/publication/8b9002b6-d8dd-426c-aa7c-6d7d16902cd7

[3] UNODC, "John Brandolino: Making our digital and physical worlds safer," (2025) available at: https://www.unodc.org/unodc/frontpage/2025/October/john-brandolino_-making-our-digital-and-physical-worlds-safer.html

[4] Gates Foundation, "Why focus on inclusive financial systems?" available at: https://www.gatesfoundation.org/our-work/programs/global-growth-and-opportunity/inclusive-financial-systems. (accessed November 2025)

[5] World Bank, "Digital Financial Inclusion," (October 2014), available at: https://www.worldbank.org/en/topic/financialinclusion/publication/digital-financial-inclusion

and transferred without physical presence, drawing on speed, automation, pseudonymity and the increasingly borderless nature of digital payments.[6]

These characteristics are being actively exploited by criminals. Fraud, money laundering, misappropriation of funds, market abuse and tax evasion are all being facilitated by digital channels. Criminal groups are "weaponizing" digital technologies to steal money, data and identities, while also scaling traditional illicit markets – including corruption, drug trafficking, human trafficking, arms tracking and wildlife crime – "at a greater scale and speed than ever before."[7]

Although precise estimates are challenging, it is widely believed that 2-5% of global GDP is laundered each year.[8] The United Nations has noted that Africa alone could gain USD 89 billion each year by addressing illicit financial flows - equivalent to 3.7% of the continent's GDP.[9] One recurring finding is that women, who are already "disproportionately excluded from beneficial financial systems" may be particularly vulnerable to related illicit finance risks.[10,11]

This paper examines the nexus between the rapid expansion of digital finance – particularly as a tool for financial inclusion – and the growing risks of illicit financial flows, including corruption. It considers the digital finance landscape across mobile money, open banking, stablecoins and crypto assets, highlighting the specific vulnerabilities each introduces. The paper also provides an overview of emerging trends such as point-of-sale "human ATMs," human independent financial flows driven by agentic AI payments and stablecoins, and the rise of deepfakes and synthetic identities generated and deployed by generative AI.

The analysis presented in this paper highlights several cross-cutting findings relevant to the governance of digital finance and the management of illicit financial flow (IFF) risks.

First, the rapid expansion of digital finance has materially altered the speed, scale and geographic reach of value transfer, particularly in low- and middle-income countries. Mobile mobile, open banking, crypto assets and stablecoins increasingly function as core financial infrastructure rather than peripheral innovations. While these systems have expanded access to payments, savings, and

---

[6] UNCTAD, *Tackling Illicit Financial Flows for Sustainable Development in Africa,* (2020), available at: https://unctad.org/system/files/official-document/aldcafrica2020_en.pdf

[7] UNODC, "John Brandolino: Making our digital and physical worlds safer," (2025) available at: https://www.unodc.org/unodc/frontpage/2025/October/john-brandolino_-making-our-digital-and-physical-worlds-safer.html

[8] UNODC, "Money Laundering," available at: https://www.unodc.org/unodc/en/money-laundering/overview.html (accessed 17 November 2025)

[9] UNCTAD, *Tackling Illicit Financial Flows for Sustainable Development in Africa,* (2020), available at: https://unctad.org/system/files/official-document/aldcafrica2020_en.pdf

[10] Gates Foundation, "Why focus on inclusive financial systems?" available at: https://www.gatesfoundation.org/our-work/programs/global-growth-and-opportunity/inclusive-financial-systems. (accessed November 2025)

[11] Transparency International and U4 Anti-Corruption Resource Centre, "The gendered dimensions of illicit financial flows," (3 June 2019), available at: https://www.u4.no/api/publications/the-gendered-dimensions-of-illicit-financial-flows/pdf

cross-border transfers, they have simultaneously reduced transaction friction in ways that can be exploited for illicit purposes.

Second, many digital finance systems exhibit dual-use characteristics, supporting both legitimate economic activity and illicit finance. Features such as real-time settlement, extensive agent networks, pseudonymity, interoperability and automation improve efficiency and inclusion but also lower the barriers for fraud, money laundering, corruption-related capital flight and other predicate offences. In several cases, criminal exploitation does not require technical sophistication, but rather leverages behavioural vulnerabilities, weak identity controls or regulatory gaps.

Third, the paper finds that risk exposure is unevenly distributed. First-time users, low-income populations, migrants and women are often more exposed to fraud and exploitation due to limited financial literacy, constrained control over devices or identity documentation, and restricted access to effective redress mechanisms. In these contexts, financial inclusion initiatives can unintentionally increase exposure to harm if safeguards do not evolve in parallel.

Fourth, existing regulatory and supervisory frameworks often struggle to keep pace with platform-based and cross-sector digital finance models. Fragmentation across telecoms, banking, fintech, crypto and technology sectors complicates oversight, while cross-border digital services frequently operate beyond the effective reach of national regulators. Inconsistent implementation of international standards further contributes to regulatory arbitrage and uneven risk mitigation.

Fifth, while digital finance increases IFF risks, it also generates new opportunities for detection and enforcement. Transaction traceability, data analytics and blockchain monitoring can strengthen financial intelligence and asset recovery when supported by appropriate legal frameworks, technical capacity and cross-border cooperation. The effectiveness of these tools, however, depends on timely access to data, interoperable systems and trust between public and private actors.

Taken together, these findings indicate that addressing IFF risks in digital finance is not solely a technical or compliance challenge. It requires coordinated governance across sectors and borders, sustained investment in supervisory capacity and consumer protection, and a deliberate effort to ensure that financial integrity objectives are pursued alongside, rather than at the expense of, a sustained commitment to financial inclusion.

2

DIGITAL FINANCE

Mobile Money

Mobile money has become one of the primary drivers of access to financial services, enabled by the mass adoption of mobile phones, particularly smartphones. Mobile technologies and services contributed an estimated USD 6.5 trillion to global GDP in 2024 and are projected to reach USD 11 trillion by 2030.[12] With financial access now literally in the palm of one's hand, and supported by expanding 4G and 5G networks, firms and entrepreneurs are offering a wide range of products via mobile channels. These include mobile lending, banking and payments; peer-to-peer transfers; crowdfunding and P2P lending; business-to-business payments; online trading; insure-tech; foreign exchange; international remittances; gamified investments; personal investment tools; and online procurement.[13] All of these services rely on mobile money payments infrastructure.

Mobile money accounts allow users to store value digitally and transfer funds safely. They are generally low cost, easy to set up and accessible through cash deposits, agent networks or third-party intermediaries. Mobile money has also become a major channel for remittances to and from diaspora communities. While this expansion has brought substantial benefits, it has simultaneously created a broader attack surface for criminals and fraudsters, particularly in emerging markets.

Globally, there were 2 billion mobile money accounts in 2024, with almost USD 1.7 trillion flowing through these systems – equivalent to USD 3.2 million in transactions per minute and USD 4.6 billion per day. A network of 28 million registered mobile money agents facilitates cash deposits, transactions and customer support.[14] Sub-Saharan Africa has emerged as the global "epicentre" of mobile money with 1.1 billion registered accounts and USD 1.1 trillion in transaction value in 2024.[15] This represents around 40% of adults in the region and contributes approximately USD 190 billion to regional GDP.[16]

---

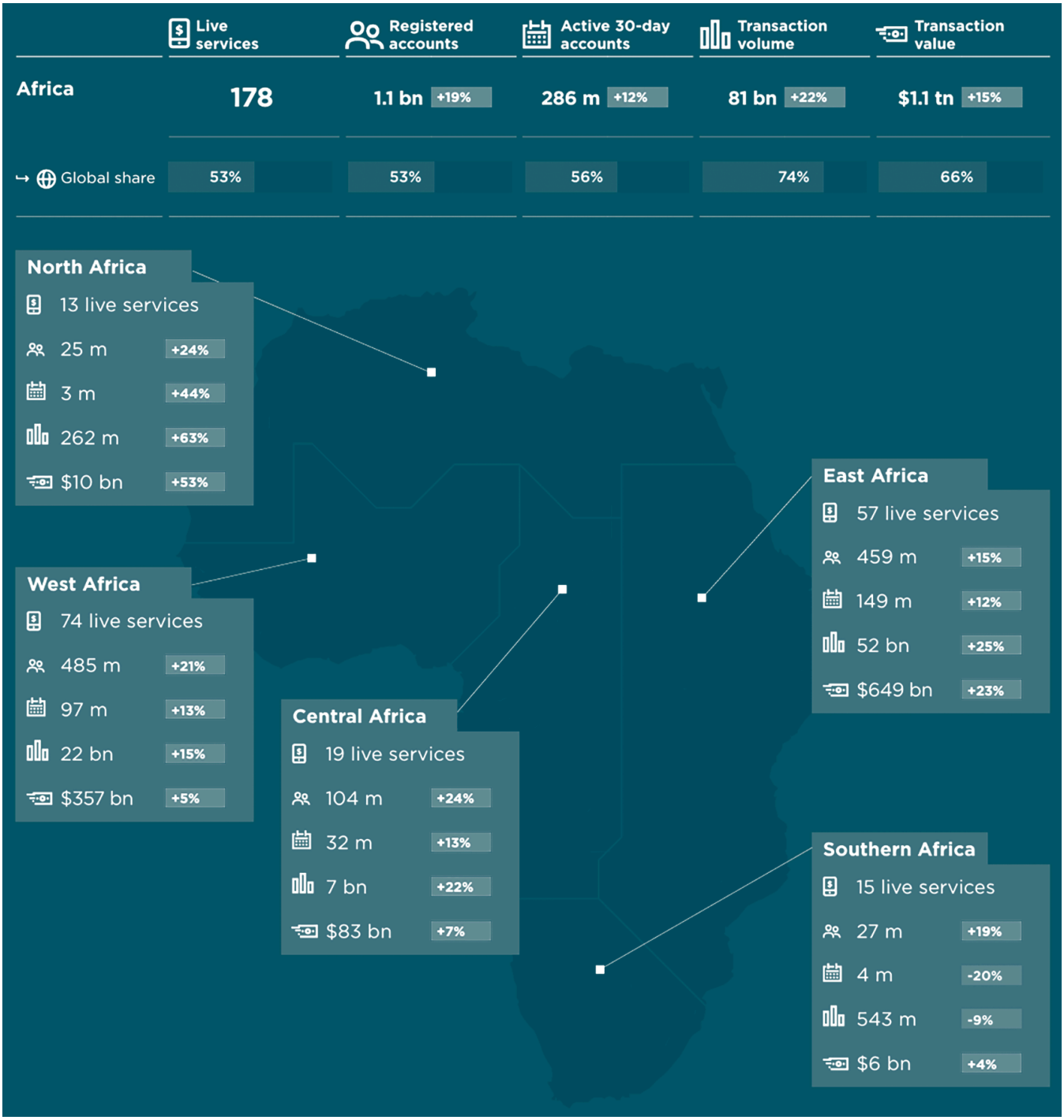
[12] GSMA, *The Mobile Economy,* (2025), available at: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2025/04/030325-The-Mobile-Economy-2025.pdf

[13] Fintechnews Middle East, "Fintech in Kenya: An Overview," February 16, 2020, available at: https://fintechnews.ae/5330/fintech/fintech-in-kenya-an-overview/

[14] GSMA, *State of the Industry Report on Mobile Money 2025,* (2025), available at: https://www.gsma.com/sotir/wp-content/uploads/2025/04/The-State-of-the-Industry-Report-2025_English.pdf

[15] GSMA, *State of the Industry Report on Mobile Money 2025,* (2025), available at: https://www.gsma.com/sotir/wp-content/uploads/2025/04/The-State-of-the-Industry-Report-2025_English.pdf

[16] GSMA, *State of the Industry Report on Mobile Money 2025,* (2025), available at: https://www.gsma.com/sotir/wp-content/uploads/2025/04/The-State-of-the-Industry-Report-2025_English.pdf



(Image: overview of mobile money activity across Africa, +/- percentages relate to year-on-year changes vs 2023 data.)[17]

Despite rapid growth, mobile money users remain exposed to significant security vulnerabilities. Device passwords – often the first line of defence against handset theft – are used by only 60% of

[17] Image Source: GSMA, *State of the Industry Report on Mobile Money 2025,* (2025), available at: https://www.gsma.com/sotir/wp-content/uploads/2025/04/The-State-of-the-Industry-Report-2025_English.pdf

mobile phone owners globally. Women are ten percentage points less likely than men to password-protect their phones, partly because they are more likely to rely on hand-me-down devices or phones initially set up by someone else. The situation is even more acute in Sub-Saharan Africa, where only 48% of phones are password-protected, reflecting the widespread use of basic phones that lack biometric features. Notably, only half of mobile money account owners in the region have secured their devices. Although mobile money wallets typically require PINs, insecure phones still leave users vulnerable to theft, SIM-swap attacks and other forms of mobile-based cybercrime.[18]

Around 30% of unbanked individuals also lack the documentation needed to open mobile money accounts, limiting their ability to access safer, regulated services. Transaction data shows that mobile money is used predominantly for merchant payments, followed closely by peer-to-peer transfers and cash-in/cash-out activity – with 38% of all mobile money transactions involving cash conversion. International mobile money remittances, one of the most vulnerable channels for illicit finance, reached USD 54 billion in Sub-Saharan Africa alone.

GSMA's *State of the Industry Report on Mobile Money 2025*[19] documents a wave of service innovation that has steadily expanded the reach, interoperability and functionality of mobile money systems since the emergence of M-Pesa in Kenya, widely regarded as the catalyst for the global mobile money industry. In 2024, MTN MoMo became the first non-bank to offer an interbank digital payment service from South Africa's PayShap system. In Ghana, Google Play now accepts payments through Telecel Cash's mobile money service. Togocom and Orabank launched PASS TMONEY to enable offline money transfers between TMoney and Orabank. In Sierra Leone, Afrimoney partnered with PYYPL to launch a Visa card linked directly to mobile money accounts. MTM MoMo Liberia and FinTech BnB expanded remittance corridors to Côte D'Ivoire, Ghana, Guinea, Mali, Rwanda, Senegal, Sierra Leone and Uganda. M-Pesa has also enabled Ethiopian diaspora communities to send funds directly to domestic mobile wallets, while in Nigeria, PalmPay introduced a USSD-based service[20] allowing users without smartphones to access its agent network.

Despite these advances, low levels of financial literacy continue to expose users to fraud, scams and other illicit financial flows, particularly among first-time users and vulnerable populations.

Interpol has raised the alarm that Africa's multi-billion-dollar mobile money industry is being increasingly exploited by organized crime groups, a trend it expects to intensify.[21] The United Nations Conference on Trade and Development (UNCTAD) has similarly warned that online non-bank payment services, many of which rely on mobile money, are particularly vulnerable to illicit financial flows

[18] VoxDev, "Understanding mobile phone and internet use across the world," (7 November 2025), available at: https://voxdev.org/topic/understanding-mobile-phone-and-internet-use-across-world
[19] GSMA, *State of the Industry Report on Mobile Money 2025,* (2025), available at: https://www.gsma.com/sotir/wp-content/uploads/2025/04/The-State-of-the-Industry-Report-2025_English.pdf
[20] USSD (Unstructured Supplementary Service Data) is a protocol used on GSM cellular phones that enables interactive text-based communication between mobile users and service providers.
[21] Interpol, *Mobile money and organized crime in Africa,* (June 2020), available at: https://www.interpol.int/en/content/download/15457/file/2020%2007%2015%20PUBLIC%20VERSION%20-%20Strategic%20Analysis%20Report%20-Mobile%20Money%20in%20Africa%202020.pdf

because they are "fast, cheap" and can offer "anonymous means to make payments and international transfers."[22] Interpol has linked mobile money to a wide range of criminal activities, including fraud (such as agent-based transaction splitting to inflate commissions, investment scams, and the proliferation of SIM farms), as well as the trafficking of drugs (including cocaine, heroin, methamphetamines, khat, synthetic drugs, and illegal pharmaceuticals), human trafficking and migrant smuggling, the trade in small arms and wildlife, other environmental crimes, and corruption. Interpol has further identified human trafficking as a key form of criminality enabled by mobile money services.[23]

Kenya's long coastline and the port of Mombasa have been identified by Interpol as key transit points within the global drug trade, with proceeds estimated in the billions of dollars and mobile money services increasingly used to launder associated funds. The illicit trade in small arms has contributed to conflicts across countries such as the Democratic Republic of Congo, Libya, Liberia, Côte d'Ivoire and Sierra Leone.[24] Mobile money reportedly served as a primary payment channel for transactions involving the estimated 30 million illicit firearms circulating in Africa.[25] This trade has been linked to up to 70% of conflict-related deaths across the continent.[26]

Corruption further compounds these risks. An estimated 75 million people across Africa pay bribes each year.[27] A survey by the African Union indicates that 63% of young people have paid bribes to access essential services such as healthcare and education; transactions that are increasingly facilitated through mobile money.[28] In Kenya, mobile money has also been linked to kidnap-for-ransom payments, extortion and terrorist financing. Following the 2019 DusitD2 hotel attack in Nairobi, Kenya's Anti-Terrorism Police Unit identified mobile money transfers across 47 SIM cards connected to terror suspects, including linkages extending into South Africa.[29]

Increased cross-border interoperability, weak identity verification, the use of fake and synthetic IDs, and uneven regulatory enforcement further expose mobile money ecosystems to exploitation. At the

---

[22] UNCTAD, *Tackling Illicit Financial Flows for Sustainable Development in Africa,* (2020), available at: https://unctad.org/system/files/official-document/aldcafrica2020_en.pdf

[23] UNCTAD, *Tackling Illicit Financial Flows for Sustainable Development in Africa,* (2020), available at: https://unctad.org/system/files/official-document/aldcafrica2020_en.pdf

[24] Interpol, *Mobile money and organized crime in Africa,* (June 2020), available at: https://www.interpol.int/en/content/download/15457/file/2020%2007%2015%20PUBLIC%20VERSION%20-%20Strategic%20Analysis%20Report%20-Mobile%20Money%20in%20Africa%202020.pdf

[25] Interpol, *Mobile money and organized crime in Africa,* (June 2020), available at: https://www.interpol.int/en/content/download/15457/file/2020%2007%2015%20PUBLIC%20VERSION%20-%20Strategic%20Analysis%20Report%20-Mobile%20Money%20in%20Africa%202020.pdf

[26] Interpol, *Mobile money and organized crime in Africa,* (June 2020), available at: https://www.interpol.int/en/content/download/15457/file/2020%2007%2015%20PUBLIC%20VERSION%20-%20Strategic%20Analysis%20Report%20-Mobile%20Money%20in%20Africa%202020.pdf

[27] UNCTAD, *Tackling Illicit Financial Flows for Sustainable Development in Africa,* (2020), available at: https://unctad.org/system/files/official-document/aldcafrica2020_en.pdf

[28] UNCTAD, *Tackling Illicit Financial Flows for Sustainable Development in Africa,* (2020), available at: https://unctad.org/system/files/official-document/aldcafrica2020_en.pdf

[29] Xinhua, "News Analysis: Mobile Money on Spot as Kenya Links Service to Terrorism Funding," Xinhuanet, January 30, 2019, available at: http://www.xinhuanet.com/english/africa/2019-01/30/c_137787614.htm

same time, recent regulatory reforms have improved licensing regimes, consumer protection, interoperability and know your customer (KYC) frameworks in several markets.

What This Means for Illicit Financial Flows (IFFs)

Mobile money systems combine high transaction volumes, rapid settlement, extensive agent networks and uneven digital identity controls—creating conditions that are highly attractive for illicit financial activity. Key IFF risks include the use of agent-assisted structuring to avoid reporting thresholds, the exploitation of SIM farms and synthetic identities to create multiple accounts, the laundering of proceeds through cash-in/cash-out cycles, and the growing integration of mobile money with cross-border remittances, crypto assets and stablecoins. Weak handset security and low financial literacy further increase exposure to fraud, extortion, kidnap-for-ransom payments, corruption and terrorism financing. At the same time, mobile money's digital traceability presents important opportunities for law enforcement and regulators when effective transaction monitoring, reporting and inter-agency cooperation frameworks are in place.

Open Banking

Open Banking continues to transform financial services through the use of application programming interfaces (APIs) that enable the real-time sharing of data between customers, financial institutions and licensed third-party providers, with the user's consent.[30] This portability is empowering individuals to gain a consolidated, real-time view of their finances across multiple accounts, supporting more informed financial decision-making. Open Banking has also driven new competition by introducing data-driven market entrants and enabling the development of innovative products such as personal finance management tools, budgeting and savings applications, alternative credit scoring models, digital lending, insurance and investment platforms.

The Open Banking ecosystem brings together banks, clearing and settlement mechanisms, and API platforms that together streamline payment initiation, reduce friction and enable seamless movement between service providers.[31] While some Open Banking models focus solely on data-sharing, others enable API-initiated payments, allowing customer funds to be transferred directly from a payer's bank to a beneficiary's bank without the use of cards.[32] As Open Banking scales globally, including through initiatives to support cross-border real-time payments, the ability to access and mobilise an individual's full financial footprint through APIs, combined with near instant settlement, creates new exposure to cyber-enabled fraud and illicit financial activity.

---

[30] ComplyAdvantage, *The State of Financial Crime 2024,* (January 2024), available at: https://get.complyadvantage.com/insights/the-state-of-financial-crime-2024-download

[31] OECD, *Open Finance and Open Banking in Sub-Saharan Africa*, (2024), available at: https://www.oecd.org/content/dam/oecd/en/topics/policy-sub-issues/digital-finance/Open-Finance-in-Africa-and-Open%20Banking-in-sub-Saharan-Africa.pdf

[32] European Banking Authority, "Response to consultation on draft Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and ML/TF risk factors," available at: https://www.eba.europa.eu/eba-response/13830 (accessed November 2025)

The Open Banking market is projected to reach USD 136 billion, with the number of instant payments expected to exceed 235 billion globally by 2027. [33,34] More than 69 countries have introduced instant payment systems, using a range of models based on either centralized or decentralized APIs, with varying regulatory approaches.[35] In India, the Unified Payments Interface (UPI) is expected to process up to 90% of all retail digital payments by 2027 and already handles nearly 19 billion transactions per month.[36,37] On the African continent, countries at the forefront of Open Banking adoption include South Africa, Nigeria, Kenya, Ghana, and Rwanda.[38] South Africa leads the region, with more than 200 FinTechs operating across account aggregation, financial management, alternative insurance, lending and payment solutions.[39] Nigeria issued its Open Banking guidelines in 2021. Kenya broadly follows the European Payment Services Directive 2 (PSD2) model, although a fully standardised, industry-wide API framework is not yet in place. Rwanda has incorporated Open Banking into its Five-Year Economic Strategy.

From a money laundering perspective, risks in Open Banking are driven primarily by customer behaviour, transaction patterns and delivery channels, rather than by the act of data-sharing itself.[40] Typologies of suspicious activity include: multiple transfers to the same beneficiary within short timeframes; a single payee receiving transfers from multiple unrelated accounts; repeated transactions just below reporting thresholds; unusually large or irregular value movements; regular incoming funds unrelated to wages followed by rapid outward transfers (a common indicator of money mule activity); and payments to or from high-risk jurisdictions, including countries subject to FATF countermeasures or comprehensive sanctions.

A key structural challenge is the limited ability to stop API-initiated payments once triggered, particularly where Open Banking providers do not apply real-time friction or risk-scoring controls. As a result, phishing and social engineering, impersonation fraud, authorised push payment

[33] FinTech Magazine, ",Open Banking is poised to drive innovation" (7 May 2021), available at: https://fintechmagazine.com/banking/open-banking-poised-drive-innovation
[34] FinTech Global, "Volume of instant payments to exceed 235 billion by 2027," (7 March 2023), available at: https://fintech.global/2023/03/07/volume-of-instant-payments-to-exceed-235-billion-by-2027/.
[35] HPS Worldwide, "Open Banking and Open Finance: Global Update 2024," (30 October 2024,)available at: https://www.hps-worldwide.com/blog/open-banking-and-open-finance-global-update-2024.
[36] India Ministry of External Affairs, "UPI to comprise 90% of all retail digital transactions in the next five years: RBI," (26 June 2023), available at: https://indbiz.gov.in/upi-to-comprise-90-of-all-retail-digital-transactions-in-the-next-five-years-rbi/
[37] Press Information Bureau of India, "UPI: India's Digital Revolution Goes Global," (17 September 2025), available at: https://www.pib.gov.in/FeaturesDeatils.aspx?id=155224&NoteId=155224&ModuleId=2
[38] Business Day, "Here are five African countries with open banking guidelines," (3 April 2025), available at: https://businessday.ng/technology/article/here-are-five-african-countries-with-open-banking-guidelines/?amp
[39] OECD, Open Finance and Open Banking in Sub-Saharan Africa, (2024), available at: https://www.oecd.org/content/dam/oecd/en/topics/policy-sub-issues/digital-finance/Open-Finance-in-Africa-and-Open%20Banking-in-sub-Saharan-Africa.pdf
[40] European Banking Authority, *The ML/TF Risk Factors Guidelines,* (1 March 2021), available at: https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf

scams, advanced fee fraud, counterfeit third party applications, and coordinated money mule networks have emerged as major areas of concern.

What This Means for Illicit Financial Flows (IFFs)

Open Banking introduces new IFF risks by combining real-time data access with near-instant, API-initiated payments. Once initiated, fraudulent payments are often difficult to interrupt or reverse, increasing the effectiveness of scams, impersonation attacks and authorised push payment fraud. Open Banking infrastructure is also increasingly exploited by organised money mule networks, which rapidly distribute illicit proceeds across multiple accounts to evade detection. Cross-border instant payment initiatives further amplify these risks by compressing the time available for transaction monitoring and supervisory intervention.

Without strong real-time risk scoring, behavioural analytics and coordinated interbank response mechanisms, Open Banking can substantially accelerate the speed, scale and complexity of illicit financial flows. At the same time, Open Banking supports source of funds checks. In certain countries, for customers assessed as being very low risk, a source of funds check from an account held at a regulated financial institution by the same individual may meet simplified due diligence requirements, streamlining KYC checks.

Crypto Assets

Crypto assets have moved from the fringes of the financial system into the mainstream, driven by strong political support in some jurisdictions, rising institutional interest, and expanding regulatory frameworks. As a result, global crypto market capitalisation reached approximately USD 4 trillion in 2025,[41] despite continuing high volatility. Crypto assets initially gained traction as a means of transferring value rapidly and at low cost without reliance on traditional financial intermediaries, supporting both legitimate economic activity and illicit use. The perception of pseudonymity has further contributed to their attractiveness for a wide range of users.

Sub-Saharan Africa has emerged as the third fastest-growing crypto region globally, driven primarily by retail participation. The region received over USD 205 billion in on-chain value, with most transactions ranging between USD 1,000 to USD 10,000.[42] This figure does not capture outgoing flows, over-the-counter transactions, peer-to-peer activity or transfers conducted via unhosted wallets. Crypto assets have increasingly been framed as a potential tool for financial inclusion in the region.[43] At the same time, significant business-to-business crypto activity now supports cross-border payments in Africa's two largest markets – Nigeria and South Africa – creating additional exposure to illicit financial

[41] Reuters, "Crypto sector breaches $4 trillion in market value during pivotal week," (18 July 2025), available at: https://www.reuters.com/business/crypto-sector-breaches-4-trillion-market-value-during-pivotal-week-2025-07-18/.
[42] Chainalysis, "The 2025 Geography of Crypto Report," (2025) available at: https://www.chainalysis.com/wp-content/uploads/2025/10/the-2025-geography-of-crypto-report-release.pdf
[43] Chainalysis, "The 2025 Geography of Crypto Report," (2025) available at: https://www.chainalysis.com/wp-content/uploads/2025/10/the-2025-geography-of-crypto-report-release.pdf

flows.[44] In Nigeria, Bitcoin is used widely as a hedge against currency risk and as an alternative savings mechanism.[45]

While regulatory frameworks have expanded to bring centralized crypto exchanges and certain virtual asset service providers (VASPs) within the scope of AML/CFT rules, a large proportion of crypto activity remains outside effective regulation. Many unregulated exchanges operating across borders face no legal obligation to comply with customer due diligence, capital adequacy, governance or transaction reporting obligations. This creates opportunities for misuse by criminal actors. Peer-to-peer markets supported by unhosted wallets and informal crypto hawala services facilitate direct transfers between individuals without identity verification. In such environments, users may unknowingly transact with counterparties seeking to launder criminal proceeds. These marketplaces may be susceptible to scams, including price manipulation, fake escrow services and malware distribution through messaging platforms. Uneven global implementation of FATF standards for virtual assets continues to exacerbate these risks

Crypto assets have been linked to nearly every major predicate offense for money laundering, including ransomware extortion, trade-based money laundering, kidnap-for-ransom, tax evasion, large-scale fraud (particularly investment and romance scams) and capital flight.[46] In at least one African country, billions of dollars are suspected to have been lost through balance-of-payments leakages linked to corrupt public officials using crypto to purchase foreign real estate.[47]

The Central African Republic (CAR) provides an interesting example: after briefly adopting Bitcoin as legal tender, the government reversed course following international pressure, before launching the SANGO project aimed at establishing the country as a "crypto oasis." This initiative included proposals for crypto-based citizenship, tokenised access to land and the tokenisation of mineral assets. More recently, CAR launched the $CAR meme Coin,[48] promoted by President Faustin-Archange Touadéra on his official X account. The token surged rapidly in value before collapsing amid concerns of fraud and the President's announcement being flagged by AI systems as a potential deepfake.[49,50] The

[44] Chainalysis, "The 2025 Geography of Crypto Report," (2025) available at: https://www.chainalysis.com/wp-content/uploads/2025/10/the-2025-geography-of-crypto-report-release.pdf
[45] Chainalysis, "The 2025 Geography of Crypto Report," (2025) available at: https://www.chainalysis.com/wp-content/uploads/2025/10/the-2025-geography-of-crypto-report-release.pdf
[46] African Business, "Africa's regulators urged to move faster as stablecoins gain ground," (3 November 2025), available at: https://african.business/2025/11/technology-information/africas-regulators-urged-to-move-faster-as-stablecoins-gain-ground
[47] Anonymous, 5 September 2024.
[48] BBC, "CAR leader launches meme-coin 'experiment'," (11 February 2025), available at: https://www.bbc.co.uk/news/articles/cly5x0vpen8o.
[49] Bitget Wallet, "What is $CAR Coin? How to Buy the Central African Republic's Meme Coin Experiment," (October 2025), available at: https://web3.bitget.com/en/academy/what-is-car-coin-how-to-buy-the-central-african-republic-meme-coin-experiment
[50] Investing.com "CAR memcoin plunges 96.7% amid launch skepticism," (12 February 2025), available at: https://uk.investing.com/news/cryptocurrency-news/car-memecoin-plunges-967-amid-launch-skepticism-93CH-3920162

government has since announced plans to tokenize 1,700 hectares of land through $CAR, potentially linked to natural resource development.[51]

In Ghana, DOBIBO has emerged as a fake AI crypto platform that uses social media apps such as Telegram and WhatsApp for users to recruit friends and family into investment scams, offering reimbursements and rewards for new recruits. DOBIBO has been identified by authorities in Italy and New Zealand as providing illegal services.[52,53] An anonymous source shared how the app works: "The app's interface fabricates massive profits, making the victim believe their money is growing… When victims attempt withdrawals, the account freezes. The operators then demand a final "verification fee" or "capital gains tax" (10-20% of balance) to unlock the funds. Once this fee is paid, the victim is blocked, and the platform disappears."[54]

Law-enforcement operations increasingly confirm the role of crypto assets in organised crime and terrorism financing. Interpol's Operation Catalyst identified the misuse of crypto to support terrorist financing linked to financial fraud, cyber-enabled scams, money laundering and kidnap-for-ransom across six African countries, with victims losing approximately USD 5 million. In Kenya, a VASP was identified as having links to terrorism financing, while law enforcement uncovered crypto wallets in Tanzania used to recruit and radicalize individuals from East and North Africa. In another case, a cross-border Ponzi scheme spanning Cameroon, Kenya and Nigeria was linked to high-value wallets suspected of supporting terrorist financing.[55]

At the same time, blockchain transparency has enabled some of the largest asset seizures in criminal history. In October 2025, authorities seized billions of dollars in Bitcoin linked to forced-labour crypto scam compounds in Cambodia, where victims trafficked from Burundi, Ethiopia, Ghana, Kenya, Nigeria, Tanzania, and Uganda were forced to operate scam centers.[56]

---

[51] Mariblock, "CAR to tokenize 1,700 hectares of land using meme coin," (7 June 2025), available at: https://www.mariblock.com/car-to-tokenize-1-700-hectares-of-land-using-meme-coin/

[52] Comissione Nazionale per le Societa' e la Borsa, *Warnings,* (10 October 2025), vailable: https://www.consob.it/web/consob-and-its-activities/-/consob-warning-of-2025-10-10-blackout-websites

[53] Financial Market Authority, "Txex - WhatsApp educational and investment platform scam," (20 August 2025) available at: https://www.fma.govt.nz/library/warnings-and-alerts/txex/.

[54] Anonymous, 18 December 2025

[55] Interpol, "83 arrests in landmark African operation against terrorism financing," (22 October 2025), available at: https://www.interpol.int/en/News-and-Events/News/2025/83-arrests-in-landmark-African-operation-against-terrorism-financing

[56] Office of Public Affairs | Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes | United States Department of Justice

What This Means for Illicit Financial Flows (IFFs)

Some crypto assets significantly expand the speed, reach and opacity of illicit financial flows by enabling near-instant, cross-border value transfer without reliance on traditional intermediaries. Key IFF risks arise from the widespread use of unhosted wallets, peer-to-peer marketplaces and unregulated cross-border exchanges, which operate outside effective customer due diligence and reporting frameworks. Criminal actors exploit these features for ransomware, large-scale fraud, kidnap-for-ransom payments, corruption-related capital flight, trade-based money laundering and terrorism financing.

The use of mixers, tumblers, OTC brokers, chain-hopping and informal crypto hawala services further obscures transaction trails. At the same time, the traceability of blockchain transactions—when paired with effective analytics and international cooperation—offers powerful tools for asset tracing and seizure, making crypto both a major risk amplifier and a potential enforcement asset.

Stablecoins

Stablecoins have emerged as a major potential driver of growth in the digital payments ecosystem and are increasingly positioned as a tool for financial inclusion, particularly for cross-border transactions. Stablecoins are blockchain-based tokens designed to maintain a stable value in relation to a referenced asset.[57] They enable near-instant global transfers at costs typically ranging between 0.5-2% of transaction value.[58] In contrast, remittance payments can take 5+ days with a global average cost of 6.49% of the amount sent (8.78% in sub-Saharan Africa).[59] While opening a conventional bank account *can* take days or weeks (although many digital banks have now significantly reduced this timeframe), decentralized digital wallets capable of holding stablecoins can be created in minutes. These characteristics make stablecoins highly attractive for both legitimate economic activity and illicit use.

Stablecoin adoption has accelerated rapidly, with approximately USD 51 trillion in stablecoin transactions between November 2024 and November 2025. The most widely used stablecoins are USD Coin (USDC) and Tether (USDT), both pegged to the US dollar.[60] In environments characterised by limited access to banking, high inflation, exchange-rate volatility, and currency shortages, stablecoins have emerged as a potential alternative to traditional fiat, increasingly functioning as a parallel digital

[57] Bank for International Settlements, "Stablecoin growth – policy challenges and approaches," *BIS Bulletin No. 108,* (11 July 2025), available at: https://www.bis.org/publ/bisbull108.pdf
[58] BVNK, "Blockchain in cross-border payments: a complete 2025 guide," (17 October 2025), available at: https://bvnk.com/blog/blockchain-cross-border-payments.
[59] World Bank, "An Analysis of the Trends in Costs of Remittance Services: Remittance Prices Worldwide Quarterly," (March 2025), available at: https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q125_1_0.pdf
[60] In 2024, USDC monthly transfer volume between $3.21 billion to $1.54 trillion and USDT processed between $703 billion to $1.01 trillion per month.

dollar.[61] In Sub-Saharan Africa, stablecoins accounted for an estimated 43% of all crypto transactions in 2024, with Nigeria leading regional adoption.[62] Nigeria received approximately USD 92.1billion in stablecoin value, reflecting both its population scale and strong uptake among the digitally connected "tech-savvy youth" seeking to preserve value.[63] In early 2025, Nigeria launched the cNGN stablecoin on regulated exchanges, and established a cross-government working group to develop a national stablecoin regulatory framework.[64,65] South Africa, Ethiopia, Kenya, and Ghana are the next largest stablecoin markets in the region.

Stablecoins are also being actively integrated into trade and payments infrastructure. The pan-African Africa Digital Access and Public Infrastructure for Trade (ADAPT) initiative aims to use stablecoins to support cross-border trade by building trusted digital identity alongside national ID platforms (such as Kenya's eCitizen). This initiative will also enable secure cross-border data exchange and develop an interoperable finance layer linking mobile money, banking systems, digital currencies and stablecoins. Pilots are planned for Kenya and Ghana, with projected economic gains of USD 23.6 billion.[66] However, without strong trade-based money laundering controls and interoperable identity safeguards, such systems also risk amplifying illicit financial flows.

Stablecoins now dominate on-chain illicit activity. The Financial Action Task Force (FATF) has warned that "most on-chain illicit activity now involves stablecoins," noting that mass adoption could further amplify illicit finance risks.[67] The use of USDT on the TRON blockchain is regarded as particularly high-risk due to its low transaction costs and high throughput. When combined with mixers and tumblers (which blend the crypto assets of many users together) or cross-chain bridges or chain-hopping techniques (which enable transfer of stablecoins between different blockchains), the origin, destination and beneficial ownership of stablecoin transactions become increasingly difficult to trace.

The UN Office on Drugs and Crime (UNODC) has identified Tether as the "'preferred choice" for money laundering linked to sextortion, romance or "pig-butchering" scams, online gambling, human trafficking

[61] Lennox Yieke, *African Business,* "Africa's regulators urged to move faster as stablecoins gain ground," (3 November 2025), available at: https://african.business/2025/11/technology-information/africas-regulators-urged-to-move-faster-as-stablecoins-gain-ground

[62] Lennox Yieke, *African Business,* "Africa's regulators urged to move faster as stablecoins gain ground," (3 November 2025), available at: https://african.business/2025/11/technology-information/africas-regulators-urged-to-move-faster-as-stablecoins-gain-ground

[63] Chainalysis, *The 2025 Geography of Crypto Report*, (September 2025), available at: https://www.chainalysis.com/wp-content/uploads/2025/10/the-2025-geography-of-crypto-report-release.pdf

[64] IMF, "Regulating the Crypto Market in Nigeria," (July 2025), available at: file:///C:/Users/drudi/Downloads/2958-7875-018.2025.issue-096-en.pdf

[65] Ledger Insights, "Nigeria's central bank forms stablecoin working group," (23 October 2025), available at: https://www.ledgerinsights.com/nigerias-central-bank-forms-stablecoin-working-group/

[66] IOTA Foundation, "ADAPT: Building Africa's Digital Trade Future," (17 November 2025), available at: https://blog.iota.org/adapt-africa-digital-trade/

[67] FATF, "FATF urges stronger global action to address Illicit Finance Risks in Virtual Assets," (26 June 2025), available at: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html

and large-scale fraud.[68] Although the report focused on East and Southeast Asia, some commentators claim that this reflects the preference for USDT to retain the value of proceeds of crime by criminal groups around the world.

In Nigeria, stablecoins were also linked to alleged market manipulation activity that contributed to pressure on the naira through peer-to-peer markets and self-hosted wallets in early 2024. More broadly, the FATF has linked stablecoins to sanctions evasion, including activity associated with the Democratic People's Republic of Korea. The EU recently sanctioned Ruble-backed stablecoin A7A5, which was used to move more than USD 8 billion through blacklisted wallets.[69]

While stablecoins increase the speed and scale of cross-border financial flows, they can also strengthen law-enforcement capabilities when properly monitored. On-chain transparency allows for real-time tracing and seizure when regulatory frameworks, analytics capacity and international cooperation are in place. When combined with privacy-enhancing technologies, stablecoins also present future opportunities to balance transaction monitoring with data protection, provided robust governance frameworks are implemented.

What This Means for Illicit Financial Flows (IFFs)

Stablecoins represent one of the most significant accelerators of illicit financial flows in the digital finance ecosystem. Their ability to move large volumes of dollar-denominated value instantly across borders, outside the banking system and often beyond effective identity controls, makes them particularly attractive for money laundering, fraud, sanctions evasion, trade-based money laundering and terrorism financing. The dominance of USDT on low-cost, high-speed blockchains, combined with mixers, chain-hopping and self-hosted wallets, significantly reduces transaction traceability. At the same time, stablecoins can enhance enforcement when robust blockchain monitoring, exchange supervision and cross-border regulatory cooperation are in place - creating a dual-use environment that requires strong, coordinated governance.

[68] UNODC, *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat*, January 2024, available at: https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf

[69] Elliptic, "The A7 leaks: The role of crypto in Russian sanctions evasion and election interference," (26 September 2025), available at: https://www.elliptic.co/blog/the-a7-leaks-the-role-of-crypto-in-russian-sanctions-evasion-and-election-interference

3

DIGITAL FINANCE TRENDS AND VULNERABILITIES

Beyond today's mainstream digital finance channels, a new wave of technologies and business models is emerging that further blurs the boundary between innovation and illicit financial risk. These developments, ranging from informal POS-based cash access and automated AI-driven payments to deepfakes and synthetic identities, are already reshaping how value is moved, how financial services are accessed and how criminals exploit system vulnerabilities. While these trends promise efficiency and new forms of access, they also introduce complex regulatory, supervisory and enforcement challenges that are not yet fully addressed in many, if any, jurisdictions.

Point of Sale (POS) / "Human ATMs"

Across several African markets, point of sales (POS) devices are increasingly being used as informal cash-in and cash-out points, effectively transforming retail agents into "human ATMs". This model has grown rapidly in environments where banking infrastructure is limited or unreliable. Customers use debit cards or mobile-linked accounts to deposit or withdraw cash via POS agents, who execute the corresponding digital transfer through their own mobile or bank accounts. In Nigeria and Tanzania, banks have partnered with FinTechs such as Moniepoint and OPay to scale this POS ecosystem and extend last-mile access to financial services.

While many POS Agents operate legitimately, this model has also facilitated the rapid growth of money mule networks, whereby agents move funds on behalf of third parties using their own or pooled accounts. This allows criminal actors to layer and distribute illicit proceeds while minimising their own digital footprint. Weak onboarding controls, inadequate monitoring of agent behaviour and fragmented KYC enforcement have heightened these risks. In response to mounting concerns related to large-scale money laundering and mule activity, authorities in Nigeria temporarily restricted or scrutinised the operations of major POS-linked FinTech providers.[70]

Agentic AI Payments and Stablecoins

The emergence of agentic artificial intelligence, which can take autonomous decisions or actions, introduces a new layer of automation into digital finance, enabling software-driven agents to initiate payments, procure services and execute financial transactions autonomously.[71] When combined with stablecoins, this creates the potential for largely human-independent financial flows operating at

[70] News Central, "CBN Banks Major Players: OPay, Palmpay, Kuda Bank, Moniepoint in Crosshairs," (5 May 2024), available at: https://www.youtube.com/watch?v=ZGaMpMYSXl8

[71] AIR, "Shaping the Future of Stablecoin Oversight," (16 September 2025), available at: https://regulationinnovation.org/wp-content/uploads/2025/10/AIR-Stablecoins-US-Event-Recap-Report_092025.pdf

machine speed and global scale. While this could significantly enhance efficiency in areas such as supply chains, trade finance and digital commerce, it also creates new governance challenges.

In such environments, traditional "Know Your Customer" (KYC) frameworks alone will be insufficient. Regulators and financial institutions will increasingly need to implement "Know your Agent" protocols, ensuring that automated agents are verifiably authorised to act on behalf of identifiable legal persons.[72] Without such controls, agentic payment systems could be exploited for rapid, automated laundering, large-scale fraud and sanction evasion. A careful balance will be required between enabling innovation and preventing the emergence of fully automated criminal finance systems.

Deepfakes and Synthetic Identities

The rapid advancement of generative AI, which generates text, images or other content, is accelerating the creation and deployment of deepfakes and synthetic identities. This poses severe challenges to digital finance ecosystems that rely primarily on remote onboarding and non-face-to-face verification. AI-generated identity documents, biometric spoofing and real-time synthetic video impersonation increasingly undermine the reliability of conventional digital KYC processes. When combined with sophisticated social-engineering techniques, these tools can enable criminals to manipulate victims over extended periods, often with devastating financial and psychological consequences.

At the same time, crime-as-a-service and money laundering-as-a-service business models are dramatically lowering the cost per victim, making lower-income and first-time users of digital financial services more attractive targets. As digital inclusion expands, beneficiaries of mobile money, crypto and stablecoin adoption face heightened exposure to fraud, identity theft and financial exploitation. This requires identity verification systems, consumer protection frameworks and real-time fraud detection capabilities to be significantly strengthened.

Adaptive Digital Finance in Conflict Zones

Conflict-affected environments are increasingly emerging as fertile ground for the misuse of digital financial innovations. While digital finance platforms can expand access to banking-like services for civilians in fragile settings, these same tools may also be exploited to raise, transfer, or obscure funds that sustain armed conflict or facilitate large-scale fraud.

In many cases, evidence of such misuse is difficult to independently verify, relying heavily on investigative reporting, expert testimony, and anecdotal accounts rather than judicial findings or publicly available enforcement actions. The examples below are therefore intended to illustrate observed patterns of risk rather than to establish definition attribution or scale.

In Sudan, civilians and businesses reportedly continue to use *Bankak*, the Bank of Khartoum's mobile banking application, by connecting to the internet through illegally obtained Starlink satellite dishes

[72] AIR, "Shaping the Future of Stablecoin Oversight," (16 September 2025), available at: https://regulationinnovation.org/wp-content/uploads/2025/10/AIR-Stablecoins-US-Event-Recap-Report_092025.pdf

linked to the Starlink system operated by SpaceX.[73] Investigative reporting and expert commentary suggest that Sudanese paramilitary group, the Rapid Support Forces (RSF) may be charging commissions reportedly as high as 25% for access to Starlink connectivity used to facilitate mobile banking transactions. The RSF is also reported to use Bankak "to pay fighters and move looted funds, effectively integrating a de facto parallel financial layer 'into a formal banking application.[74] While these claims are difficult to independently verify, they highlight how digital financial tools can continue to function, and be repurposed, amid the collapse of conventional banking infrastructure.

In the Democratic Republic of Congo (DRC), the March 23 Movement (M23), a group subject to US sanctions[75], is reported to be leveraging mobile money agent networks as an informal revenue collection mechanism. Agents are purportedly permitted to continue operating only if they pay a so-called "protection tax" and facilitate payments linked to the illicit mineral trade.[76,77,78] Although direct transactional evidence remains limited, these reports underscore the vulnerability of agent-based payment systems to coercion by armed groups, particularly where state oversight and physical security are weak.

In Libya, investigative sources describe an informal network of brokers equipped with point-of-sale (POS) machines that disguise cash withdrawals as legitimate retail transactions, allowing funds to be laundered without triggering additional AML/CFT alerts.[79] In this model, individuals reportedly swipe payment cards with POS merchants and receive cash minus a substantial premium, often estimated at10-30%).[80] These practices illustrate how POS infrastructure can be repurposed in environments characterised by fragmented authority and parallel financial systems.

In Zimbabwe, the *Malaicha* system has evolved into a hybrid digital–physical value transfer mechanism linking Zimbabwe and South Africa[81]. Platforms such as *Malachai.com* reportedly allow users in South Africa to "purchase" goods in South African rand, which are then sourced in Zimbabwe or from bonded warehouses and delivered locally. By settling value off-platform and bypassing formal currency controls[82], the system functions in practice as a net-settlement swap, drawing comparisons to

[73] ArabNews, "Smuggled Starlink dishes throw lifeline to some in war-torn Sudan," (3 April 2024), available at: https://www.arabnews.com/node/2487506/amp
[74] Anonymous, 18 December 2025
[75] Office of Foreign Assets Control, *Sanctions List Search – M23,* available at: https://sanctionssearch.ofac.treas.gov/Details.aspx?id=15585 (accessed 18 December 2026)
[76] Anonymous, 18 December 2026
[77] Jamestown, "M23 Leverages Taxes and Minerals to Sustain DRC Operations," (12 April 2025), available at: https://jamestown.org/m23-leverages-taxes-and-minerals-to-sustain-drc-operations/
[78] CGTN Africa, "Banks, traders face challenges in rebel-controlled eastern DRC," (4 May 2025), available at: Banks, traders face challenges in rebel-controlled eastern DR Congo https://www.youtube.com/watch?v=HwWdPwZqZAs
[79] Anonymous, 18 December 2026
[80] Anonymous, 18 December 2026
[81] Reuters, "Zimbabweans in S.Africa use app to send food home after border restrictions," (19 May 2020), available at: https://www.reuters.com/article/world/zimbabweans-in-safrica-use-app-to-send-food-home-after-border-restrictions-idUSKBN22V1IV/
[82] BIZCommunity, "Hello Paisa launches Malaicha collection, delivery service app for Zimbabweans," (30 July 2019), available at: https://www.bizcommunity.co.zw/Article/238/394/193751.html

hawala-style[83] informal value transfer systems. While these services themselves may operate within regulatory grey areas rather than explicitly illegal frameworks, their broader economic function illustrates how digital commerce tools can replicate informal remittance rails at scale.

Taken together, these cases, while often difficult to conclusively verify, illustrate a recurring pattern: in environments marked by conflict, weak governance, or fragmented regulatory authority, innovative payment systems can be adapted or repurposed in ways that facilitate illicit finance.

Limited regulatory oversight and constrained supervisory capacity in such contexts heighten the risk that illicit funds are introduced into, or transit through, formal financial systems. This underscores the need for conflict-sensitive financial regulation, improved monitoring of emerging payment rails, and strengthened international cooperation to address the evolving intersection between digital finance, fragility, and illicit financial flows.

[83] Anonymous, 18 December 2025

4

RECOMMENDATIONS

Digital finance now operates as critical infrastructure for economic growth in many countries, and its governance will play a decisive role in shaping development outcomes. The recommendations below focus on strengthening the institutional, regulatory and technical foundations needed to manage illicit finance risks while supporting sustainable, inclusive growth.

Apply Proportionate, Risk-Based AML/CFT Regulation Across Digital Finance

Regulators should expand the scope of AML/CFT regulation across digital finance in a proportionate and risk-based manner, taking account of local market conditions, financial inclusion goals and supervisory capacity. Where possible, local regulators should seek to understand emerging technologies, and regulatory frameworks that support innovation and protect societies. Mobile money providers, agent networks, POS operators, Open Banking payment initiators, stablecoin issuers and virtual asset service providers should be brought within supervisory frameworks in ways that avoid unnecessary de-risking or exclusion.

Tiered licensing and supervision models can help align regulatory expectations with transaction volumes and systemic importance, while simplified customer due diligence might be applied to genuinely low-risk use cases. Higher-risk activities, particularly cross-border payments, stablecoins, crypto trading and agent aggregation, should trigger enhanced scrutiny. Regulators are encouraged to convene regular policy and technical working groups with industry, civil society, financial intelligence units and law enforcement to test how emerging technologies and business models should be regulated without suppressing responsible innovation. This should include exploration of novel solutions to support the ability of firms, agents and third party intermediaries to submit suspicious activity and transaction reports.

Strengthen Digital Financial Literacy and Consumer Protection

Digital financial inclusion must be matched with sustained investment in consumer protection and financial literacy. As first-time users enter digital ecosystems at scale, their exposure to fraud, scams and identity exploitation increases sharply. Governments and providers should prioritise national digital financial literacy strategies targeting youth, women, informal workers and migrant populations. Low-cost education tools, including SMS alerts, USSD prompts, WhatsApp chatbots and in-app security nudges, can play an important role in teaching users how to secure their devices, recognise scam typologies, verify payment requests and access redress. Trusted, well-publicised dispute-resolution

mechanisms across telecoms, banks, FinTechs and crypto service providers are essential to maintaining confidence in digital finance systems.

Accelerate Trusted, Interoperable Digital Identity Systems

Trusted, interoperable digital identity systems should be treated as foundational public infrastructure for secure digital finance. Governments and development partners should prioritise interoperability between civil registries, telecom operators, financial institutions and digital wallet providers, while supporting cross-border identity verification pilots within regional economic communities. Digital IDs must be universally accessible, portable across services and borders, and privacy-preserving by design. Emerging approaches, such as verifiable credentials, wallet-based identity and distributed ledger-enabled identity systems, offer promise, but only if embedded within strong governance, oversight and data-protection regimes.[84] Properly designed digital identity systems can simultaneously strengthen inclusion and enhance law-enforcement activity and asset tracing.

Improve Cross-Sector and Cross-Border Information Sharing

Effective disruption of modern illicit finance requires substantially stronger cross-sector and cross-border cooperation. Banks, mobile money providers, crypto platforms, telecom operators, social media companies and FIUs must be able to share risk information securely and in real time. Public-private financial crime coordination mechanisms should be formalised where they do not yet exist. Privacy-enhancing technologies, such as homomorphic encryption, zero knowledge proofs and differential privacy, should be piloted to enable secure typology sharing, collective risk detection and joint transaction analysis without violating data-protection laws. Legal, institutional and cultural barriers to information sharing, including data localisation and liability concerns, require explicit policy attention.

Expand Access to Affordable Fraud Detection and Analytics

Access to affordable fraud detection and analytics tools remains a major constraint in many low-capacity markets. Digital finance providers, particularly agent networks and smaller FinTechs, may lack effective transaction monitoring, mule-network detection and crypto tracing tools. Regulators and development partners should promote the use of open-source monitoring and blockchain analytics tools, alongside shared monitoring utilities for POS ecosystems and mobile money platforms. Training for regulators, FIUs, mobile money compliance teams and agent supervisors should focus on typologies such as agent-assisted structuring, SIM farms, mule networks, stablecoin layering and cross-platform fraud.

To develop suitable solutions for each different type of digital service provider, further work should be carried out to gain an in-depth understanding of key vulnerabilities and exposures of different types of digital finance service providers to illicit financial flows. An educated agent network, supported by

[84] AIR, "Advancing Digital Identity: Building Essential Infrastructure," (2024), available at: https://regulationinnovation.org/wp-content/uploads/2024/05/Advancing-Digital-Identity-Brief.pdf

automated red-flag transaction monitoring systems, can significantly reduce community-level exposure to illicit finance.

Integrate Gender Dimensions into Risk Management and Consumer Protection

Gender considerations must be explicitly integrated into digital finance risk management and consumer protection frameworks. Women often face barriers related to identity ownership, device control and access to recourse, while also being disproportionately targeted by scam typologies, sextortion and social engineering.[85] Systematic collection of gender-disaggregated data on fraud victimisation and KYC access barriers is essential to designing effective protections.[86] Consumer education initiatives, onboarding frameworks and digital ID systems must be designed to ensure that women are not inadvertently excluded or exposed to heightened exploitation risks.

Prepare Supervisory Frameworks for AI-Driven Finance and Automated Payments

As automation accelerates, supervisors and policymakers must prepare for the implications of AI-driven finance and agentic payment systems. Traditional "Know Your Customer" regimes will increasingly need to be complemented by "Know Your Agent" standards that ensure automated systems are verifiably authorised to initiate transactions on behalf of identifiable legal persons. Financial institutions should be required to maintain human override mechanisms, ensure auditability of AI-driven transaction decisions and apply real-time behavioural analytics to detect anomalous payment activity. Without these safeguards, fully automated laundering, fraud and sanctions evasion may scale faster than existing supervisory models can manage.

Embed Illicit Finance Controls into Stablecoin and Digital Trade Infrastructure

As stablecoins and digital payment rails become embedded within trade infrastructure and regional payment systems, illicit finance risks must be addressed at the design stage. Trade-based money laundering controls should be integrated directly into digital trade documentation, invoicing systems and cross-border payment workflows. Stablecoin ecosystems require clear reserve transparency, issuer supervision, wallet-level risk controls and interoperable sanctions screening. If financial crime controls are not embedded at the infrastructure layer, illicit finance will scale in parallel with digital trade.

---

[85] CGAP, "Break the Bias: Evidence Shows Digital Finance Risks Hit Women Hardest," (8 March 2022), available at: https://www.cgap.org/blog/break-bias-evidence-shows-digital-finance-risks-hit-women-hardest

[86] Alliance for Financial Inclusion, "Nine key actions to balance women's financial inclusion and financial integrity," (30 November 2025), available at: https://www.afi-global.org/opinion/nine-key-actions-to-balance-womens-financial-inclusion-and-financial-integrity/#_ftn3

ABOUT THE PAPER

Methodology

The paper was developed through a combination of desk-based research and targeted interviews to support the stocktaking exercise. The desk-based research drew on a wide range of sources, including reports from international organizations and civil society, law enforcement publications, court cases, academic research, and media reporting. It also involved the identification and analysis of available qualitative and quantitative data on digital finance – both to assess its contribution to financial inclusion and, where possible, to understand the scale, value and impact of illicit financial flows. Interview insights were cross-checked and validated before being incorporated into the paper.

About AIR

The Alliance for Innovative Regulation (AIR) is a nonprofit, non-membership organization working to make the financial system fully fair, inclusive and highly resilient through responsible use of new technology. By connecting regulation, finance, technology and society, AIR supports global innovation and collaboration to overcome the system's legacy shortcomings and prepare it for rapid technology change.

Financial regulation should be a potent force for good. It should operate as an invisible force in people's lives, ensuring that consumers are shielded from discrimination and abuse, that small businesses can access capital, that criminals cannot use the financial system to hide illicit activity, and that financial catastrophes are averted. AIR educates, connects, and supports the regulatory ecosystem to help realize these goals. Learn more about AIR at regulationinnovation.org.

Funded by GIZ

This research was funded by GIZ, a German federal enterprise in the field of international cooperation for sustainable development as part of the self-funded project "Governance of Digital Finance". The views expressed in this publication should not be attributed to the funder.

With Special Thanks

Special thanks are extended to the individuals who contributed their time and insights through interviews, including Sean Doyle (World Economic Forum), Rob Reeves (Lextego), Chukwunonso Arinze (Kaoshi), and Verengai Mabika (Expectation State). Their expertise significantly informed the development of this paper.