

AFRICA GAMING REGULATORY INSIGHT

Follow the Money

Why African gambling regulators must connect betting surveillance, mobile money and AML intelligence

A new FATF report shows how illegal gambling proceeds can move through professional laundering networks that combine informal value transfer, mobile money, payment providers, mule accounts and virtual assets. The policy response must be integrated - and proportionate.

Nkopane Tshehla

Managing Director, Larocure Advisory

7 September 2026

The most revealing part of the Financial Action Task Force's new report is not that gambling appears in a money-laundering document. Regulators have long understood that casinos, betting accounts and lottery products can be misused. More significant is the wider financial architecture described by FATF: informal transfer networks, mobile wallets, payment service providers, mule accounts, virtual assets, encrypted communications, and cross-border settlement arrangements operating as parts of the same value chain.

For African gambling authorities, this shifts the regulatory question. The challenge is no longer only whether an operator is licensed, a website is blocked, or a betting outlet is inspected. It is also whether authorities can identify who is collecting the money, which payment rails are being used, how customer funds are aggregated, where value is settled and which regulated or unregulated intermediaries make the activity possible.

The core policy implication: gambling supervision, financial intelligence and payment oversight can no longer operate as separate regulatory conversations.

What the FATF report establishes

Published on 3 September 2026, Investigating Professional Money Laundering, Underground Banking, and the Use of Hawala and Other Similar Service Providers is a typologies and good-practice report. It is not a new gambling statute or regulation, and it does not itself impose a new effective date on operators. Its importance lies in the evidence base it gives to governments, financial intelligence units, law-enforcement agencies, supervisors and regulated businesses.

FATF describes professional money laundering as an infrastructure serving a broad range of criminal economies. Illegal gaming and gambling are expressly included alongside fraud, cyber-enabled crime, corruption, tax evasion and organised crime. The report also shows how modern laundering arrangements increasingly combine informal value-transfer mechanisms with formal financial infrastructure. Bank accounts, fintech platforms, payment service providers, prepaid products, and virtual-asset wallets can become entry and exit points in a wider laundering cycle.

The gambling connection is practical, not theoretical. FATF records the use of casino and junket-related value transfer to introduce cash into the formal system or move value through gambling arrangements. It also includes an official case study in which an illegal online-gambling platform separated its customer-facing operation from its financial flows through panel operators, digital wallets, online banking, mule accounts and accounts opened with stolen identities. Part of the proceeds was converted to cash, moved across borders through underground channels and later presented as foreign investment.

The specific case occurred outside Africa, but the operating model is highly relevant to African markets: a gambling interface may be visible in one place while the people, accounts and settlement arrangements supporting it are distributed across institutions and jurisdictions.

Why the African payment context matters

Africa's mobile-money success has expanded financial access, reduced transaction costs and enabled commerce for millions of people. That achievement must be protected. FATF is careful to state that informal transfer systems and similar services are not inherently criminal and may serve legitimate remittance and value-transfer needs. A sound regulatory response must therefore distinguish the criminal exploitation of a channel from its legitimate use.

At the same time, the report finds that mobile-money wallets are increasingly being incorporated into hybrid informal-transfer arrangements. Customer payments can enter through a wallet or agent network, be recorded and coordinated digitally, and then be settled elsewhere through cash, trade, bank accounts, virtual assets or another informal network. The result is a value chain in which one segment is visible to a regulated institution while another remains concealed.

Four sub-regional patterns

East Africa: FATF highlights cross-border remittance corridors, including routes connected to Somali diaspora flows, where mobile-money rails, cash agents, and informal exchangers may interact.

West Africa: The report identifies Lagos, Accra, Cotonou and Abidjan as nexus points where cash-based informal transfer activity may connect with mobile-money transfers and, in some cases, bank accounts.

North Africa: Currency controls and conflict dynamics can stimulate informal value-transfer activity, with mobile money emerging as an additional settlement layer in some markets.

Southern Africa: Integration is described as less pronounced but growing along migrant-remittance routes, particularly between Zimbabwe and South Africa and between Mozambique and South Africa.

These are regional risk observations, not findings that every transaction, agent or corridor is illicit. Their strategic value is that they direct authorities towards the points where gambling activity, payments, remittances and informal settlement can intersect.

The regulatory blind spot is the space between mandates.

A gambling regulator usually sees licence status, product approvals, technical systems, advertising, player accounts and operator reporting. A financial intelligence unit sees suspicious-transaction reports and financial patterns. A central bank or payment regulator sees payment institutions, wallets and transaction flows. A tax authority sees declared turnover and tax payments. Telecommunications authorities and mobile-network operators see subscriber and device relationships. Law enforcement sees criminal networks and evidential requirements.

Each institution may therefore hold a legitimate but incomplete view of the same illegal market. Professional laundering networks benefit when those views are not connected. They can move activity across institutional boundaries: from a gambling platform to a payment intermediary, from a wallet to an agent, from an agent to cash, and from cash into trade or cross-border settlement.

This is why enforcement based only on blocking a domain, closing a shop or arresting a low-level collector rarely removes the economic infrastructure. The public-facing channel may disappear while the payment accounts, customer lists, agents, settlement partners and controlling interests remain available for the next brand or platform.

What an integrated African response should look like

1. Connect gambling intelligence to financial intelligence

Gambling authorities and financial intelligence units should establish formal, lawful information-sharing arrangements with defined purposes, escalation criteria and safeguards. Intelligence on unlicensed operators, suspicious payment references, repeated beneficiary accounts, merchant identities, and associated domains should be comparable with suspicious-transaction reporting and other authorised financial data.

2. Attribute the operator behind the interface

A website or app is only the visible layer. Authorities need to identify the controlling persons, beneficial owners, payment beneficiaries, agents, affiliates, technology suppliers and settlement counterparties connected to the activity. Persistent attribution is more valuable than a list of URLs because operators can replace domains and brands far faster than they can replace every financial and operational dependency.

3. Make payment intelligence a core supervisory capability

Payment methods should not be treated as a footnote in licensing or enforcement. Regulators need structured data on deposit and withdrawal channels, payment service providers, merchant arrangements, wallets, agent networks, chargeback patterns and customer-fund flows. For legal operators, this improves assurance over customer protection, segregation of funds and AML controls. For illegal operators, it creates additional points for detection and disruption.

4. Build risk indicators around behaviour, not technology

A mobile wallet, cash agent, or virtual asset is not proof of criminality on its own. Risk indicators should focus on combinations of behaviour: rapid movement through multiple accounts, repeated low-value deposits into common beneficiaries, unexplained third-party payments, high transaction velocity, unusual geographic dispersion, shared devices or identity attributes, mismatches between declared activity and payment volumes, and links to known illegal-gambling infrastructure.

5. Create domestic coordination cells and cross-border channels

FATF emphasises dedicated domestic coordination and deeper international cooperation. In the gambling context, this points to standing mechanisms that connect gambling regulators, financial intelligence units, central banks, payment supervisors, revenue authorities, telecommunications bodies, police and prosecutors. Where activity crosses borders, the same model should extend through regional AML bodies, regulator-to-regulator cooperation and established legal channels for evidence and asset tracing.

6. Move from case-by-case action to system-wide disruption

Authorities should measure success not only by the number of websites blocked or outlets closed, but by whether the underlying network has lost access to payment accounts, agents, merchant facilities, technology, customer acquisition channels and settlement partners. The strategic objective is to increase the cost and reduce the resilience of the illegal operation.

Implications for licensed operators and payment providers

The report also carries a clear message for compliant businesses. Licensed gambling operators should expect closer attention to the full payment chain, including third-party processors, wallet providers, agents and outsourced technology. Risk-based customer due diligence, source-of-funds enquiries where justified, transaction monitoring, account-linkage analysis and timely suspicious-transaction reporting will become more important as authorities focus on hybrid financial models.

Payment providers and mobile-money businesses should not be expected to become gambling regulators. They should, however, have reliable ways to identify licensed merchants, detect unauthorised gambling use of their services, preserve relevant data and respond lawfully to regulator or FIU requests. Clear official safelists, standardised notices and feedback loops would reduce uncertainty and help legitimate providers distinguish a licensed operator from an illegal one.

The strongest public-private partnerships will share useful indicators without exposing sensitive investigative detail or creating indiscriminate exclusion. FATF's warning about financial inclusion is especially important in Africa: overbroad de-risking can push legitimate customers and remittance providers away from supervised channels, reducing transparency rather than improving it.

A continental regulatory opportunity

Africa does not need to copy another region's enforcement model without adaptation. The continent's high use of mobile money, fragmented gambling laws, varied institutional capacity and extensive cross-border trade require an African regulatory architecture. That architecture should connect licensing data, digital-gambling surveillance, payment intelligence, beneficial-ownership information, tax data and cross-border cooperation while remaining consistent with privacy, due process and financial-inclusion obligations.

For many authorities, the immediate priority is not an expensive new platform. It is agreement on the questions that existing data must answer: Which operator controls the activity? Which accounts receive the money? Which providers enable deposits and withdrawals? Which agents or intermediaries recur across cases? Where is the value ultimately settled? Which part of the network can be lawfully disrupted with the greatest effect?

Once institutions share those questions, technology can support a more durable regulatory capability. Without that institutional alignment, even sophisticated monitoring tools risk producing alerts that remain trapped inside separate mandates.

Conclusion: follow the network, not only the website

The FATF report should be read as an early warning for African gambling policy. Illegal gambling is not simply a licensing violation occurring on a screen or at an outlet. At scale, it can form part of a wider financial ecosystem that uses regulated and unregulated channels together, crosses borders and survives by exploiting gaps between institutions.

The answer is not to treat every remittance, wallet or informal transfer as suspicious. It is to connect gambling intelligence with payment and AML intelligence, apply risk-based indicators, protect legitimate financial access and target the people and infrastructure that repeatedly enable illegal activity.

African regulators that develop this capability will be better placed to protect consumers, preserve the integrity of licensed markets, recover public revenue and disrupt criminal value chains. The strategic principle is straightforward: if illegal gambling is organised as a network, regulation and enforcement must respond as a network too.

Source note

Primary official source: Financial Action Task Force, [Investigating Professional Money Laundering, Underground Banking, and the Use of Hawala and Other Similar Service Providers](#), published 3 September 2026.

This article is policy analysis for general information and does not constitute legal advice.

Website publishing details

Suggested URL slug: follow-the-money-african-gambling-regulators-aml-intelligence

Meta description: FATF links illegal gambling to professional laundering networks. Africa needs connected gambling, payment and AML intelligence without undermining inclusion.

Suggested categories: Regulatory Intelligence; AML and Financial Crime; Digital Gambling; Africa