

Suspicious Gambling Activity as an Emerging Money Laundering Typology: Behavioral Indicators in Multi-Jurisdictional Retail Banking Accounts

Adaora Kalu^{1*}, Omotayo Pedro², Samuel Fadero³, Oluwatobiloba Mide-Ibrahim⁴

¹Independent Researcher, GA, USA

²Gwinnet Technical College, GA, USA

³SanlamAllianz Life Insurance Ltd, Lagos Nigeria

⁴FinServe Pro, USA

ABSTRACT

This review examines suspicious gambling-related activity as an increasingly complex financial-crime risk within multi-jurisdictional retail banking, focusing on the behavioral, transactional, regulatory, and technological factors that shape detection and control. The study adopts a structured narrative review approach, synthesizing peer-reviewed scholarship, regulatory perspectives, banking-risk research, and emerging analytical frameworks concerning gambling transactions, anti-money-laundering controls, customer profiling, cross-border exposure, and digital monitoring. The findings show that gambling activity becomes materially significant for financial-crime assessment not through isolated transactions, but through combinations of behavioral and transactional anomalies, including abrupt deviations from established account patterns, rapid fund movement, unusual account turnover, repeated cross-border transfers, opaque counterparties, unexplained sources of funds, and recurring links across multiple jurisdictions. The review further identifies regulatory fragmentation, uneven supervisory capacity, information-sharing constraints, weak data quality, and excessive reliance on static monitoring rules as important barriers to effective detection. Advanced methods, including machine learning, graph analytics, adaptive behavioral baselines, and real-time monitoring, offer substantial potential, but their effectiveness depends on explainability, governance, secure data architecture, analyst competence, and proportionate human oversight. Particular attention is given to avoiding the conflation of lawful gambling intensity with criminality, thereby preserving proportionality, fairness, and evidential rigor in compliance. The study concludes that defensible detection requires an integrated, evidence-led framework combining customer context, transaction history, network relationships, jurisdictional risk, and investigative judgment. It recommends stronger behavioral profiling, improved cross-border intelligence sharing, continuous model validation, interoperable reporting standards, and enhanced analyst training. Future research should prioritize longitudinal validation of red-flag combinations, AI-supported investigation quality, virtual-asset exposure, and the evolving interaction between digital gambling ecosystems and retail banking surveillance.

Keywords: Anti-money laundering; gambling transactions; behavioral indicators; retail banking; cross-border finance; transaction monitoring

International Journal of Technology, Management and Humanities (2025)

DOI: 10.21590/ijtmh.11.4.441

INTRODUCTION

Gambling-Linked Financial Crime in Retail Banking

Gambling-linked financial crime has become a significant concern for retail banks because gambling expenditure now intersects with ordinary payment accounts, digital channels, cross-border transfers and changing customer behaviour. The compliance problem is not that gambling activity is inherently illicit, but that legitimate gambling-related payments can coexist with financial flows generated

by fraud, corruption, theft or other predicate offences. Retail institutions must therefore distinguish lawful recreational expenditure from transactions whose scale, frequency, counterparties or economic purpose depart materially from the customer's expected profile. Research on regulated online gambling in Great Britain demonstrates that anti-money-laundering controls depend on close interaction between gambling operators and financial institutions, particularly where internet-based activity is funded through bank accounts and formal payment channels (Brooks, 2012).

The vulnerability arises partly from the financial characteristics of gambling itself. Funds may move repeatedly

between personal accounts and gambling-related payment environments, creating transaction volumes that are difficult to interpret without contextual information. Electronic gambling also reduces the analytical value of traditional distinctions between cash-intensive venues and account-based activity because customer funds can traverse interconnected digital systems. Buchanan's examination of electronic gaming devices emphasizes that technology changes both laundering exposure and the regulatory responsibilities attached to gambling businesses, reinforcing the need for coordinated controls rather than isolated institutional responses (Buchanan, 2018).

For retail banks, the challenge is acute because monitoring systems observe payments rather than the full behavioral context in which gambling occurs. A customer may exhibit legitimate but intensive betting expenditure, while another account may show modest gambling-related transactions embedded within suspicious financial behavior. Nigerian evidence indicates that gambling, including online forms, has expanded within an environment where regulatory and enforcement limitations remain material concerns. This makes contextual risk assessment especially important in markets where formal financial inclusion, digital payments and gambling participation overlap (Aguocha & George, 2021).

The African experience also demonstrates that gambling-related financial activity cannot be separated from national AML architecture. South Africa's regulatory model brought banking, gambling and other sectors within a structured compliance framework emphasizing customer identification, record keeping and suspicious transaction reporting. Such integration is significant for retail banking because the financial institution often becomes the point at which funds entering or leaving gambling environments can be assessed against account behavior, customer information and regulatory expectations (de Koker, 2003).

Multi-jurisdictional exposure further complicates this assessment. Digital gambling networks can operate across borders, involve several payment channels and interact with criminal ecosystems beyond the jurisdiction in which a bank account is maintained. Research from Southeast Asia illustrates how online gambling networks may intersect with transnational criminal activity, demonstrating why banks should interpret gambling-linked flows within geographical, counterparty and network contexts rather than treating them as a self-contained transaction category (Kamalludin, 2025).

Nevertheless, risk classification must avoid equating unusual gambling expenditure with criminality. AML assessment involves uncertainty, and professional judgments can be affected by overconfidence, false-positive preferences and other cognitive biases. A probabilistic approach is therefore valuable because it encourages analysts to consider combinations of evidence and competing explanations instead of treating an isolated indicator as determinative. This is relevant when gambling behavior is volatile or inconsistent

with conventional expenditure patterns (Ogbeide et al., 2023).

Technological analytics can strengthen this process when deployed as decision support rather than as a substitute for investigation. Machine-learning research in banking shows that improved client-risk classification can reduce inefficient false positives and direct investigative resources toward genuinely suspicious activity. For gambling-linked transactions, this suggests that customer baselines, transactional changes and risk attributes should be evaluated collectively, with human review retained for interpretation and escalation (Reite et al., 2025).

Gambling-linked financial crime must be understood within the macro-financial environments in which retail accounts operate. Differences in monetary conditions, institutional structures and economic pressures shape transaction behavior across jurisdictions and may affect how account activity is interpreted. Comparative analysis of middle-income emerging economies underscores the importance of local economic conditions when evaluating financial patterns, supporting a contextual rather than mechanically uniform approach to cross-border retail banking surveillance (Agwuna, Irrshad & Mazorodze, 2022).

Cross-Border Exposure and Detection Challenges

Cross-border exposure materially intensifies the detection problem surrounding gambling-linked financial crime because retail banks observe only fragments of activity that may span several institutions, payment infrastructures and regulatory jurisdictions. A customer's domestic account may appear routine when assessed in isolation, yet its risk profile can change when connected activity involves foreign gambling operators, payment intermediaries, digital wallets or counterparties located in jurisdictions with different supervisory expectations. Regional economic integration further increases legitimate cross-border financial mobility, making geographical movement alone an insufficient indicator of illicit conduct and requiring banks to interpret transactional context carefully (Enaifoghe, Dlamini & Agwuna, 2020). This distinction is especially important where lawful international payments resemble patterns generated by concealment.

Jurisdictional variation creates a second challenge. Differences in customer due diligence standards, reporting thresholds, supervisory capacity and enforcement practices can produce uneven visibility across the transaction chain. For Nigerian institutions, the effectiveness of anti-money-laundering controls therefore depends not only on statutory prohibitions but also on the quality of regulatory supervision and the coordination of responsible institutions. Weaknesses within supervisory arrangements can reduce the consistency with which suspicious cross-border patterns are identified and escalated (Ige, 2022).

Comparable difficulties arise elsewhere in Africa. Examination of Kenya's anti-money-laundering regime



demonstrates that formal detection mechanisms can be undermined by legislative omissions, implementation weaknesses and vulnerabilities associated with financial channels operating beyond conventional banking structures. For multi-jurisdictional retail accounts, such disparities mean that an institution may receive incomplete contextual information about transactions initiated, routed or settled through another jurisdiction, complicating judgments about whether gambling-related activity represents legitimate expenditure or a broader financial-crime concern (Gikonyo, 2018).

Information fragmentation is particularly consequential when suspicious activity extends across national borders. Financial intelligence units depend on timely access to banking information and effective mechanisms for exchanging intelligence with counterpart agencies. However, differences in legal authority, data-access arrangements and privacy safeguards can slow or constrain cross-border financial investigations, leaving individual institutions with only partial representations of wider transaction networks (Pavlidis, 2020).

Institutional heterogeneity also limits uniform detection. Comparative analysis shows that financial intelligence units differ considerably in organizational form, operational orientation and relationships with supervisory and law-enforcement bodies. Consequently, identical transactional indicators may generate different investigative responses across jurisdictions, reducing consistency in the interpretation of cross-border retail banking activity (McNaughton, 2023).

At bank level, scale compounds these structural problems. High transaction volumes, evolving laundering techniques and rigid rules-based monitoring can produce substantial false-positive burdens, particularly where cross-border behavior is heterogeneous. More adaptive approaches using anomaly detection, graph analysis and machine-learning support may improve prioritization, but their effectiveness still depends on explainability, data quality and regulatory acceptability. For gambling-linked accounts, detection is therefore strongest when automated monitoring is combined with customer context, jurisdictional risk intelligence and expert review rather than relying on single transactional triggers (Oztas et al., 2024).

Review Scope, Objectives, and Analytical Focus

This review examines suspicious gambling activity as an emerging money-laundering typology within multi-jurisdictional retail banking, with particular attention to the behavioral and transactional indicators that may distinguish legitimate gambling expenditure from activity warranting enhanced financial-crime scrutiny. Its scope centers on retail customer accounts because these accounts frequently serve as the interface between individuals, gambling operators, payment intermediaries, digital wallets, and cross-border financial networks. The review therefore considers how apparently routine deposits, withdrawals, transfers, card payments, and gambling-related credits can acquire different

risk meanings when assessed collectively, longitudinally, and across jurisdictions.

The primary objective is to identify recurring behavioral characteristics that can strengthen risk-based detection without treating gambling participation itself as evidence of criminal conduct. Particular emphasis is placed on transaction velocity, rapid movement of funds, repeated cycling between gambling platforms and bank accounts, unusual account turnover, inconsistent source-of-funds patterns, geographic dispersion, abrupt deviations from established customer behavior, and relationships among multiple counterparties. The analysis also examines how these indicators may interact rather than function independently, recognizing that suspiciousness often emerges from combinations of behaviors, timing, value, frequency, and contextual inconsistency.

Analytically, the review adopts a multi-layered perspective integrating customer behavior, transaction monitoring, jurisdictional exposure, institutional controls, and investigative judgment. It evaluates the limitations of static thresholds and isolated red flags while considering the value of behavioral baselines, network analysis, anomaly detection, and contextual risk assessment. Particular attention is given to false positives, fragmented cross-border information, inconsistent regulatory environments, and the need for explainable monitoring approaches. The review ultimately frames detection as a proportional, evidence-led process designed to improve prioritization, escalation, and defensible investigation within contemporary retail banking across increasingly complex digital and cross-border gambling ecosystems.

CONCEPTUALIZING GAMBLING-RELATED MONEY LAUNDERING RISKS

Gambling Transactions Within Laundering Cycles

Gambling transactions occupy a distinctive position within money-laundering cycles because they can connect legitimate consumer expenditure with financial flows whose underlying provenance is difficult to establish. In retail banking, the analytical problem is not the presence of gambling payments itself, but whether the surrounding movement of funds is economically coherent with the customer's profile, income, account history and purpose. Conventional descriptions of laundering as placement, layering and integration remain useful, yet modern payment systems often compress or overlap these stages. Nigerian scholarship has long emphasized that financial institutions require a risk-based, technologically informed capacity to detect suspicious movements rather than relying exclusively on prohibitions (Ajayi, 2010).

Within gambling-linked activity, the laundering cycle may be obscured by the legitimate appearance of payments entering and leaving regulated gambling environments.

The relevant risk arises when gambling-related transactions form part of a broader pattern that separates funds from their original source, complicates their transactional history, or allows subsequent credits to appear disconnected from predicate conduct. Comparative work on casino regulation in Macao and the United States demonstrates that jurisdictions differ in reporting expectations, documentation practices and indicators of suspicious activity, creating variation in how gambling-related financial flows are interpreted (Siu Lam & Greenlees, 2017).

Digital gambling further complicates this relationship because transactions may occur remotely and across financial infrastructures that are not coterminous with the customer's physical location. Regulatory research on internet gambling shows that extraterritorial activity can weaken jurisdictional boundaries and heighten dependence on financial intermediaries for oversight, particularly where operators, customers and payment processes are distributed across different legal environments (Morse, 2007).

The increasing digitization of gambling payments also creates an important traceability question. Payment architectures capable of producing consistent, auditable records may strengthen oversight, whereas fragmented systems can impede reconstruction of transaction histories. Research examining blockchain-supported processing of online gambling payments in Germany illustrates how transparency, payment supervision and law-enforcement accessibility can be incorporated into regulatory design, highlighting the importance of transaction visibility in disrupting laundering risks (Steinmetz & Fiedler, 2019).

Evidence from Australia reinforces the need to understand gambling-related laundering as part of wider financial and criminal networks rather than as an isolated casino problem. Investigations of Australian casinos have demonstrated how weak governance, opaque financial relationships and transnational intermediaries can create conditions in which illicit financial flows become difficult to distinguish from legitimate high-value gambling activity. For retail banks, this underscores the importance of assessing connected parties, account purpose and cross-border context rather than interpreting gambling credits or debits individually (Langdale, 2023).

African regulatory experience similarly demonstrates that the integrity of the laundering-control cycle depends on sustained due diligence and institutional coordination. South Africa's AML framework emphasizes customer identification, ongoing due diligence and risk-sensitive controls across financial markets, principles that are directly relevant when retail banks evaluate customers whose gambling-linked activity changes materially over time or intersects with higher-risk transactional environments (Chitimira, 2021).

The Nigerian retail-banking context also benefits from governance models that connect compliance responsibilities with operational quality. A governance-oriented approach encourages institutions to treat suspicious gambling activity

as a control problem requiring defined accountability, consistent escalation, documentation and oversight across the customer lifecycle rather than as a narrow transaction-screening exercise (Akin-Oluyomi & Akhigbe, 2022).

At enterprise level, this perspective is strengthened when operational analytics are incorporated into broader risk-management structures. Integrating analytical signals with human oversight can help institutions distinguish isolated anomalies from sustained patterns of concern, while ensuring that financial-crime decisions remain connected to governance, personnel capability and institutional risk appetite (Falemi, Akhigbe & Akin-Oluyomi, 2024).

Cashless gambling developments illustrate why this integrated perspective is increasingly important. Digital payment records can potentially improve traceability, but technological change does not eliminate governance weaknesses or guarantee effective monitoring. The design of cashless systems, data accessibility and oversight arrangements determine whether transaction records meaningfully strengthen AML controls. Accordingly, retail banks should evaluate gambling-linked activity within a continuous behavioral and transactional narrative, recognizing that suspiciousness arises from converging indicators rather than from gambling participation alone (Blaszczynski, Shaffer & Ladouceur, 2025).

Behavioral Indicators of Suspicious Account Activity

Behavioral indicators are central to identifying suspicious account activity because money laundering rarely presents as a single transaction that is intrinsically unlawful. In retail banking, concern arises when the pattern, timing, frequency, value, counterparties, or geographical characteristics of transactions diverge from the customer's established profile. This distinction is important for gambling-linked activity, where legitimate expenditure may generate irregular-looking debits and credits. Effective surveillance depends on interpreting behavioral change against historical account use rather than treating gambling transactions as inherently suspicious (Jullum et al., 2020).

Customer-level monitoring is strengthened when real-time operational information is combined with behavioral data. Such integration permits institutions to identify deviations, clusters, and emerging patterns that may be obscured when individual events are reviewed separately. Although developed for customer-experience management, the principle of linking behavior with contemporaneous operational signals supports a contextual interpretation of account activity and escalation decisions (Akhigbe, Falemi & Akin-Oluyomi, 2023).

Behavioral assessment must nevertheless distinguish anomalous financial conduct from assumptions about individual character. Research on moral disengagement in Nigeria demonstrates that behavior is shaped by psychosocial influences and contextual conditions, reinforcing the



importance of avoiding deterministic interpretations of observed actions. Within retail banking, this supports an evidential approach in which unusual gambling-related activity is assessed alongside account history, source-of-funds information, transaction velocity, counterparties, and changes from established customer baselines (Sabbah, 2021).

Evidence from South Africa similarly shows why customer due diligence should remain responsive to changing risk. Even financial products regarded as low risk may be exposed to criminal misuse, meaning that simplified classifications cannot substitute for continuing attention to unusual transactional behavior. Behavioral indicators acquire greater significance when several deviations occur together or when activity contradicts information held about the customer's expected financial circumstances (de Koker, 2009).

Automation can improve detection of such combinations, but sophisticated monitoring also introduces governance concerns. Artificial intelligence can process transactional and behavioral information, yet opaque models, weak data quality, and insufficient explainability may undermine defensible decision-making. Suspicious-account detection should therefore combine automated pattern recognition with meaningful human review, ensuring that alerts are evaluated proportionately and that legitimate gambling behavior is not conflated with financial crime merely because it appears statistically unusual (Turksen, Benson & Adamyk, 2024).

Jurisdictional Differences in Regulatory Risk

Jurisdictional differences shape the regulatory risk associated with gambling-linked financial activity because global anti-money-laundering standards are implemented through national legal systems with unequal supervisory capacity, enforcement intensity and institutional coordination. Retail banks operating across borders therefore confront inconsistent definitions of reportable conduct, different customer-due-diligence expectations and varying thresholds for regulatory intervention. Nigerian analysis has shown that global AML standards can generate implementation difficulties when domestic conditions do not align with international expectations, creating gaps between compliance and practical effectiveness (Sotande, 2018).

These divergences are visible in gambling regulation. Across Sub-Saharan Africa, gambling markets have expanded while national regulatory arrangements remain heterogeneous, with differences in dedicated regulators, reporting transparency and approaches to online products. Such unevenness creates risk environments for banks processing gambling-related payments across jurisdictions because identical transaction patterns may arise under substantially different licensing, oversight and reporting conditions (Sichali et al., 2023).

Regulatory uncertainty becomes pronounced where gambling intersects with digital channels. Evidence from Bangladesh demonstrates that unclear legal status,

limited regulatory understanding and passive supervisory approaches can impede application of risk-based AML requirements to casinos and technologically mediated financial activity. For retail banks, these conditions complicate assessments of counterparties and payment destinations because formal legality does not necessarily indicate equivalent control effectiveness across jurisdictions (Haq et al., 2022).

Regional harmonization can reduce disparities, but common standards do not automatically produce uniform implementation. Research on Asian AML governance shows that transnational regulatory frameworks depend heavily on domestic agencies, political arrangements and administrative capacities. Consequently, compliance quality may differ even among jurisdictions committed to the same international standards, requiring banks to consider implementation effectiveness rather than nominal regulatory membership (Hameiri & Jones, 2015).

Cross-country evidence further indicates that money-laundering exposure is influenced by the interaction between auditing standards and national governance quality. Strong formal rules are most effective when supported by credible institutions, transparent reporting and enforceable oversight. In multi-jurisdictional retail banking, jurisdictional risk should therefore be integrated with customer behavior, transaction characteristics, gambling-sector controls and counterparty information rather than treated as a country label. This approach supports proportionate detection while reducing under-detection in weakly supervised environments and excessive suspicion toward legitimate cross-border gambling-related transactions (Baccouri, Talbi & Hakimi, 2024).

Retail Banking Vulnerabilities and Control Gaps

Retail banks occupy an exposed position in anti-money-laundering systems because they combine transaction volumes, payment execution, customer profiles and digital channels. In gambling-linked activity, these characteristics can obscure the distinction between ordinary payments and movements of funds warranting enhanced scrutiny. Vulnerability is intensified when institutions rely on fragmented customer information, static rules or commercially driven processes that privilege transaction speed over contextual assessment. Research on banking-sector exposure shows that competitive pressures, incentive structures and weaknesses in gatekeeping can undermine compliance architectures (Yeoh, 2020).

The Nigerian banking experience illustrates how institutional incentives may create control weaknesses. Babajide et al. (2020) show that deposit mobilisation pressures can encourage practices that dilute accountability and weaken scrutiny of problematic funds, particularly where profitability objectives are poorly balanced against compliance obligations. For retail accounts displaying repeated gambling-related inflows and outflows, inadequate

challenge of unusual source-of-funds patterns can allow suspicious activity to remain embedded within legitimate banking relationships.

Control gaps are also visible where digital payment ecosystems interact with banking. Akomea-Frimpong et al. (2019) identify weaknesses associated with authentication, supervision, agent conduct and customer awareness in Ghanaian mobile-money services, demonstrating how vulnerabilities outside banks can migrate into banking channels through interconnected payment systems. This matters for gambling-linked transactions because banks may receive funds whose preceding digital pathway is only partially visible within internal monitoring systems.

Effective mitigation requires governance structures connecting transparency, accountability and operational oversight. Enterprise governance models emphasizing auditable decision pathways, compliance analytics and assigned responsibility provide a basis for strengthening escalation, case ownership and management challenge when suspicious account behavior is identified. Such arrangements reduce the risk that alerts are generated technologically but remain weakly investigated institutionally (Akhigbe, Falemi & Akin-Oluyomi, 2025).

Human capability constitutes an additional control layer. Monitoring systems depend on analysts and frontline personnel who must interpret alerts, recognize contextual anomalies and document escalation decisions consistently. Frameworks linking workforce systems with operational performance metrics demonstrate the value of integrating human-resource capacity, workload indicators and measurable outcomes. Applied to financial-crime controls, this supports staffing, targeted training and quality assurance so that high alert volumes, including gambling-related activity, do not produce superficial reviews or inconsistent investigative outcomes (Falemi, Akhigbe & Akin-Oluyomi, 2023).

Transaction Patterns Across Multi-Jurisdictional Accounts

Multi-jurisdictional retail accounts create a distinctive monitoring problem because transaction risk emerges from sequences, relationships and geographic dispersion rather than from payment value alone. Gambling-linked activity may involve frequent credits and debits whose legitimacy cannot be inferred from direction or amount in isolation. The relevant analytical question is whether transaction behaviour remains coherent with the customer's established profile when account history, counterparties, timing, jurisdiction and source-of-funds information are considered together. Nigerian scholarship on anti-money-laundering enforcement stresses that cross-border financial crime requires coordinated legal and institutional responses because domestic controls can be weakened when transactions interact with external financial systems and differing enforcement environments (Olujobi & Yebisi, 2023).

Within account-level analysis, temporal structure is particularly important. Rapid changes in transaction frequency, repeated movement among related accounts, abrupt shifts in geographic destination, or recurring transfers involving the same network of counterparties may warrant closer examination when they diverge from established behaviour. Brazilian evidence from bank records used in criminal investigations shows that social network analysis can reveal relationships and transaction structures that conventional line-by-line review may overlook, particularly where multiple accounts participate in a connected financial pattern (Lima et al., 2022).

Cross-border complexity also arises because laundering networks adapt to regulatory change. Empirical European evidence indicates that tighter anti-money-laundering policies can alter network composition, including greater internationalisation and changing relationships among natural and legal persons. For retail banks, this means that jurisdictional diversity should be treated as contextual information within a broader behavioural model rather than as an automatic indicator of suspicion (Gerbrands et al., 2022).

Network-based detection provides a useful response to this complexity. Flow-oriented graph analysis can reconstruct relationships among accounts and identify suspicious structures that are difficult to detect when transactions are evaluated independently. Such methods are valuable where funds traverse several accounts or institutions because they preserve the relational structure of financial movement while supporting investigator prioritisation (Li et al., 2020).

Research using Italian financial data similarly demonstrates that network position, transaction frequency, geographic exposure and relationships among economic actors can improve risk assessment when incorporated alongside conventional customer information. This is especially relevant to multi-jurisdictional gambling-linked accounts, where apparently ordinary payments may acquire analytical significance only when viewed in relation to connected entities, repeated cross-border exposure or unusual changes in customer behaviour (Fronzetti Colladon & Remondi, 2017).

Investigative systems can also benefit from integrating bank statements with external relational information. Work on money-laundering detection using social network algorithms shows that combining transactional data with information about associated entities can help analysts identify connections and roles that are not immediately visible from isolated payments. The value of such systems lies in supporting, rather than replacing, professional interpretation of suspicious patterns (Dreżewski, Sepielak & Filipkowski, 2015).

For African banks, these analytical capabilities operate within legal and institutional constraints. Kenyan research demonstrates that banks simultaneously face obligations to detect suspicious transactions and duties arising from the banker-customer relationship. Cross-border gambling-linked monitoring must therefore be evidence-based,



proportionate and sufficiently documented to justify escalation without treating lawful international activity as inherently problematic (Gikonyo, 2021).

Data integration is equally important. Analytics frameworks designed for complex distributed operations demonstrate how heterogeneous data can be consolidated, analysed and translated into decision-support signals. Applied cautiously to financial-crime monitoring, this principle supports combining account history, customer characteristics, transaction timing and jurisdictional information into a coherent analytical view rather than maintaining fragmented surveillance processes (Akin-Oluyomi & Akhigbe, 2023b).

A multi-site performance perspective further reinforces the need for consistent indicators across geographically dispersed environments. Standardised metrics, centralised data integration and comparative monitoring can help institutions identify deviations that would otherwise remain hidden within separate business units or national systems. In retail banking, this supports consistent evaluation of cross-border gambling-linked activity while allowing legitimate jurisdictional differences to be interpreted contextually rather than mechanically (Akin-Oluyomi & Akhigbe, 2023a).

Accordingly, meaningful pattern assessment requires banks to distinguish correlation from inference. A recurring international transfer, gambling-related credit, or sudden change in account velocity should trigger contextual review only when combined with other relevant indicators. Table 1 therefore organizes the principal observable patterns by analytical significance and monitoring response, emphasizing proportional escalation, corroboration and customer-specific baselines rather than deterministic classification.

Behavioral Red Flags and Customer Profiling

Behavioral red flags are most informative when they are interpreted as deviations from an established customer

profile rather than as standalone evidence of financial crime. In retail banking, the relevant profile should integrate expected income, occupation, geographic footprint, transaction frequency, normal counterparties, product use and historical gambling-related expenditure. South African evidence on customer due diligence demonstrates that effective risk profiling depends on validated customer information, ongoing monitoring and the capacity to update risk assessments as digital behavior changes (Gaviyau & Sibindi, 2023).

For gambling-linked accounts, temporal changes can be particularly revealing. Large-scale UK retail-banking data show that gambling expenditure can be persistent and strongly heterogeneous across customers, with heavier gambling associated with materially different financial outcomes. The implication for profiling is not that high expenditure is intrinsically suspicious, but that analysts should compare gambling activity with disposable income, savings behavior, debt exposure and the broader financial pattern of the account before escalating concern (Muggleton et al., 2021).

Behavioral-tracking research further shows that frequency, intensity, variability and upward changes in wagering can distinguish materially different gambling profiles over time. These dimensions are useful for banking analytics because they encourage attention to trajectory rather than isolated transactions; abrupt acceleration in gambling-linked payments may therefore warrant contextual review when it is inconsistent with prior account use or declared financial circumstances (Braverman & Shaffer, 2012).

Cross-game evidence similarly indicates that combinations of active days, number of activities, transaction variability and changing expenditure patterns provide richer behavioral signals than any single measure. For retail banks, this supports multivariate monitoring in which changes in payment frequency, funding behavior and account turnover are

Table 1: Illustrative Transaction-Pattern Assessment Matrix

<i>Observable account pattern</i>	<i>Analytical significance</i>	<i>Appropriate monitoring lens</i>
Sudden increase in cross-border activity	Possible departure from established account baseline	Compare with customer history and economic profile
Repeated movement among connected accounts	May indicate a wider relational transaction structure	Assess counterparties and network relationships
Geographic activity inconsistent with profile	May increase contextual jurisdictional risk	Examine location, purpose and expected account use
Multiple recurring common counterparties	May reveal relationships invisible transaction-by-transaction	Apply network and entity-link analysis
Gambling-linked inflows and outflows change sharply	May represent legitimate behavioral change or elevated risk	Compare timing, frequency and customer circumstances
Similar patterns across several jurisdictions	May indicate fragmented activity requiring consolidated review	Integrate data across relevant banking systems
High transaction frequency without clear profile alignment	May generate risk when combined with additional anomalies	Use behavioral baselines and proportionate escalation

assessed together instead of being converted mechanically into suspicion (Braverman et al., 2013).

More recent account-based research demonstrates that machine-learning models can identify distinct behavioral patterns from deposits, losses, session frequency and account depletion. In an AML setting, comparable analytical logic can help prioritize cases for human review, provided that models remain explainable and do not equate gambling-related intensity with criminal conduct (Auer & Griffiths, 2023).

Cluster-based approaches also illustrate the value of grouping behavior across several measurable dimensions. Empirical work applying gambling-disorder criteria to account-based data shows that heterogeneous customers can display different combinations of activity, reinforcing the need for dynamic rather than one-dimensional profiling (Catania & Griffiths, 2022).

Behavioral interpretation must also account for broader psychosocial context. Nigerian evidence demonstrates that observable conduct can be associated with interacting socioeconomic and social influences, cautioning against simplistic assumptions that one behavioral characteristic explains an individual's underlying motivation (Balogun & Sabboh, 2021). Related evidence on peer approval, socioeconomic status and locus of control further supports a multidimensional understanding of behavior, which is relevant when analysts distinguish unexplained account deviations from legitimate changes in personal circumstances (Sabbah & Ojo, 2023).

Crucially, a defensible red-flag framework should distinguish behavioral change from criminal inference. Sudden increases in gambling-related transfers, repeated funding cycles, unexplained cross-border movements or sharp departures from historical activity become analytically meaningful only when corroborated by other customer and transaction information. This preserves proportionality while directing investigative attention toward patterns that are unusual, persistent and insufficiently explained over time.

From a control perspective, behavioral red flags are useful only when institutions can investigate and document them consistently. Nigerian AML scholarship emphasizes the role of internal audit, staff capability, monitoring effectiveness and information sharing in strengthening financial-crime controls. Customer profiling should therefore operate within a governed escalation process that tests unusual gambling-linked activity against source-of-funds information, customer history, jurisdictional exposure and corroborating transaction evidence. This reduces both false positives and the risk that meaningful behavioral changes are overlooked within high-volume retail banking environments (Akinteye et al., 2023).

Monitoring, Investigation, and Reporting Frameworks

Monitoring, investigation, and reporting frameworks determine whether unusual gambling-linked transactions are converted from alerts into defensible financial intelligence. In

multi-jurisdictional retail banking, monitoring should begin with risk-sensitive scenarios combining customer profile, transaction history, geographic exposure, counterparties, and deviations from established behavior. Rule sets alone are insufficient where transaction patterns evolve or legitimate gambling activity produces superficially unusual flows. Predictive models can improve prioritization by identifying combinations of attributes associated with reportable activity, provided outputs remain subject to human validation and documented model governance (Hayble-Gomes, 2023).

Data quality is foundational. Poor transaction coding, inconsistent customer classifications, incomplete counterparty information, or inaccurate event dates can distort model training and weaken alert quality. This is consequential for gambling-linked accounts because rapid credits, debits, reversals, and cross-border payments may be misinterpreted when contextual fields are missing. Evidence from machine-learning applications in AML demonstrates that deficiencies in event definition and historical case data can degrade model performance, increasing both false positives and missed risk (Gupta et al., 2022).

Once an alert is generated, investigation should reconstruct the customer's financial narrative rather than merely confirm that a threshold was breached. Analysts should examine source-of-funds information, historical account use, linked parties, geographic patterns, prior alerts, and plausible explanations for changes in gambling-related activity. Research drawing on financial intelligence units shows that suspicious activity reports are most valuable when they contain developed transactional narratives and relevant contextual information to support intelligence analysis (Naheem, 2018).

Reporting effectiveness also depends on proportionality. Excessive reporting can overwhelm banks and financial intelligence units, while under-reporting can conceal meaningful risk. Empirical evidence from Italy indicates that suspicious transaction reporting can support AML effectiveness, but congestion effects arise when reporting volumes exceed analytical capacity. Banks should therefore calibrate escalation criteria toward quality, materiality, and evidential coherence rather than equating a large number of reports with stronger compliance (dalla Pellegrina et al., 2020).

The institutional feedback loop is equally important. Financial intelligence units receive, analyse, and disseminate reports, but reporting entities benefit when typologies, deficiencies, and investigative outcomes are communicated back into monitoring design. Evidence from Pakistan identifies delays, limited feedback, staffing constraints, and weak international cooperation as factors reducing the operational value of financial intelligence. For gambling-linked cross-border activity, feedback can improve scenario calibration and help institutions distinguish emerging typologies from legitimate customer behavior (Sultan & Mohamed, 2023).



Table 2: Illustrative Monitoring, Investigation, and Reporting Framework

<i>Framework stage</i>	<i>Primary analytical function</i>	<i>Key governance requirement</i>	<i>Expected output</i>
Customer baseline	Establish expected account behavior	Reliable KYC and profile data	Dynamic behavioral benchmark
Transaction monitoring	Identify material deviations	Validated scenarios and models	Prioritized alerts
Alert triage	Separate noise from credible concerns	Risk-based prioritization	Investigation queue
Case investigation	Reconstruct transactional context	Documented evidence and analyst review	Reasoned case assessment
Escalation review	Test evidential sufficiency	Independent challenge and quality assurance	Escalation or closure decision
Regulatory reporting	Communicate substantiated suspicion	Accurate, timely and coherent narrative	STR/SAR submission
Secure information exchange	Preserve controlled case information	Access controls, auditability and data integrity	Defensible information trail
FIU feedback integration	Translate intelligence into controls	Governance ownership and model recalibration	Improved monitoring scenarios
Continuous validation	Test effectiveness over time	Performance metrics and periodic review	Adaptive detection framework

Artificial intelligence can enhance this framework by ranking alerts, detecting nonlinear patterns, and identifying cases whose combined features are difficult to capture through static scenarios. Analysis of large suspicious-activity-report datasets demonstrates that machine-learning techniques can improve predictive discrimination and support focused compliance review. However, model performance should not substitute for investigative reasoning; automated results require explainability, validation, and documented challenge before influencing escalation or reporting decisions (Lokanan, 2025).

In Nigeria, AML effectiveness within commercial banking depends on how international standards are translated into operational processes. Research on Nigerian commercial banks identifies implementation limitations associated with institutional capacity, regulatory application, and the practical effectiveness of domestic AML measures. These concerns reinforce the need for monitoring architectures integrating customer due diligence, alert investigation, record keeping, governance, and escalation rather than treating suspicious transaction reporting as an isolated compliance endpoint (Ahiauzu, 2023).

A wider African perspective similarly underscores investigative capacity. Evidence from Ghana indicates that financial investigation systems can be formally established yet still require stronger practical effectiveness in tracing and responding to complex money-laundering activity. For multi-jurisdictional gambling-linked accounts, this supports coordination between bank investigations, reporting, and financial-intelligence analysis, particularly when transactions

involve multiple legal entities, countries, or payment channels (Ofori & Appiah, 2025).

Secure information governance is necessary throughout the monitoring lifecycle. Access-control research demonstrates how attribute-based encryption can restrict sensitive information to authorized users while preserving controlled data sharing. Applied conceptually to AML case management, this principle supports role-based access to customer records, investigative notes, and intelligence outputs, reducing unnecessary exposure while maintaining information availability for multidisciplinary review and escalation (Shittu & Nabil, 2023).

Integrity of inter-system data exchange is equally important when monitoring draws from multiple platforms. Blockchain-assisted secure data-exchange architectures illustrate how tamper resistance, auditability, and verifiable information flows can strengthen trust in distributed data environments. Within retail banking, comparable design principles can support reliable transfer of case information between transaction-monitoring systems, investigative teams, and controlled reporting channels, where cross-border activity requires traceable data lineage and defensible records (Shittu et al., 2022).

Finally, effective monitoring requires continuous recalibration rather than static deployment. Digital-twin research demonstrates the broader value of comparing observed system behavior against dynamic expected states to detect emerging anomalies in real time. Translated cautiously into AML surveillance, this concept supports behavioral baselines that evolve with legitimate customer

activity while highlighting material deviations for review. Such adaptive monitoring is particularly relevant to gambling-linked accounts, where transaction intensity can change rapidly and investigators must distinguish normal variation from persistent, unexplained patterns requiring escalation (Shittu et al., 2023).

Table 2 is an analytical synthesis developed for this review.

Emerging Risks and Research Priorities

Emerging risk in gambling-linked financial crime is increasingly shaped by the convergence of digital gambling, virtual assets, artificial intelligence, cross-border payments, and customer behaviour. For retail banks, these developments weaken static typologies because transactional relationships can evolve faster than conventional rules. Nigerian research on virtual assets demonstrates that regulatory change may lag technological adoption, creating periods in which financial products interact with existing bank accounts before controls mature. This makes crypto-linked gambling flows, pseudonymous transfers, and changing payment channels important areas for scrutiny rather than assumptions based solely on transaction value (Adaramola, 2025).

Virtual assets also introduce jurisdictional asymmetry. Comparative evidence from South Africa, Mauritius, Namibia, and the United Kingdom shows differences in licensing, customer due diligence, recordkeeping, and suspicious transaction reporting for virtual-asset service providers. For multi-jurisdictional retail banking, these differences can produce uneven visibility when gambling-related funds pass between conventional accounts and digital-asset environments. Future research should examine how jurisdiction-specific virtual-asset controls affect banks' ability to reconstruct customer behaviour, identify beneficial ownership, and distinguish legitimate digital gambling expenditure from unexplained financial activity (Van Staden, Kilian & McIntyre, 2025).

Artificial intelligence represents a parallel opportunity and risk. AI-enabled monitoring can process larger transaction volumes, identify nonlinear relationships, and prioritize complex alerts, yet it raises concerns about explainability, confidentiality, discrimination, model drift, and regulatory accountability. European analysis emphasizes that technological capability must be reconciled with legal requirements governing trustworthy and transparent financial monitoring. Research should move beyond accuracy comparisons and test whether AI-supported AML models remain interpretable, auditable, and stable when applied to heterogeneous gambling-linked retail accounts across jurisdictions (Horobets et al., 2025).

Technology adoption itself should be treated as a socio-technical research problem. Advanced analytical tools will not strengthen detection if analysts lack confidence, training, or authority to challenge automated recommendations. Organizational research indicates that readiness depends on strategic alignment, capability development, feedback,

and adaptive reinforcement. In retail banking AML, future studies should test how employee preparedness affects model adoption, alert disposition, escalation quality, and interpretation of unfamiliar gambling-related patterns rather than assuming technological deployment produces operational effectiveness (Akhigbe, Falemi & Akin-Oluyomi, 2024).

Institutional readiness extends beyond individual users. Evidence on generative-AI adoption highlights the importance of data governance, cybersecurity, management capability, ethical accountability, and organizational coherence before advanced systems are embedded into decision-making. These considerations are transferable to AML innovation because gambling-related monitoring depends on integrating transactional data, customer information, external intelligence, and automated analytical outputs. Research should examine whether differences in institutional maturity between advanced and resource-constrained banking environments affect detection quality and model governance (Ayinde, Ojukwu & Ohunyon, 2025).

Human factors also require closer attention. Complex alert environments can impose cognitive demands on analysts who must interpret model outputs, reconcile contradictory information, and make defensible escalation decisions under time pressure. Multimodal workload research demonstrates the value of combining behavioral, physiological, and subjective indicators when evaluating human-machine interaction. Future AML studies could investigate analyst workload, automation reliance, alert fatigue, and decision consistency to determine how monitoring systems can support professional judgment without creating excessive cognitive dependence or superficial review (Adamolekun et al., 2025).

Finally, research should exploit the analytical value of payment behaviour while maintaining a clear boundary between behavioral anomaly and criminal inference. Evidence from gambling-payment research shows that transaction timing, frequency, variability, and funding patterns can provide useful behavioral signals, but stakeholder consensus remains necessary regarding interpretation and ethical application. Longitudinal, cross-jurisdictional studies should test which combinations of gambling-linked payment indicators remain robust across customer groups, products, and regulatory environments, while measuring false positives and legitimate behavioral variation. Such research would strengthen risk-sensitive profiling without converting unusual gambling activity into presumptive evidence of laundering (Lakew, Jonsson & Lindner, 2024).

CONCLUSION

This review examined how suspicious gambling-related activity can function as an emerging money-laundering risk within multi-jurisdictional retail banking, with particular emphasis on behavioral indicators, transaction patterns, regulatory variation, monitoring architecture,



and investigative decision-making. The study's objectives were met by integrating these dimensions into a coherent analytical framework that distinguishes legitimate gambling expenditure from activity that becomes concerning because of its broader financial context.

The review shows that no single gambling transaction, payment value, jurisdiction, or behavioral change is sufficient to establish suspicion. Rather, risk emerges when multiple indicators converge, including abrupt deviations from established account behavior, rapid movement of funds, repeated cross-border transfers, unusual account turnover, unexplained sources of funds, recurring links to common counterparties, and patterns that are inconsistent with a customer's known financial profile. The analysis further demonstrates that jurisdictional differences in supervision, reporting obligations, financial-intelligence capacity, and digital-asset regulation can create uneven visibility across transaction chains, increasing the importance of contextual and network-based assessment.

A central finding is that effective detection depends on combining dynamic customer profiling with transaction monitoring, relational analysis, human investigation, and defensible escalation. Advanced analytics, machine learning, graph-based methods, and adaptive monitoring can strengthen prioritization, but only when supported by reliable data, explainable models, secure information governance, and appropriately trained analysts. Excessive reliance on static rules risks both false positives and missed threats.

Accordingly, retail banks should strengthen behavioral baselines, integrate cross-jurisdictional and counterparty intelligence, improve model validation, and maintain clear documentation of investigative reasoning. Regulators and financial intelligence units should promote interoperable reporting standards, timely feedback, and stronger information-sharing mechanisms. Future research should test indicator combinations longitudinally across jurisdictions, assess the effectiveness of AI-supported monitoring, and examine how virtual assets, digital gambling platforms, and evolving payment technologies alter laundering exposure. These priorities would support more proportionate, evidence-led, and operationally resilient financial-crime controls across increasingly interconnected retail markets.

REFERENCES

- [1] Adamolekun, A., Logah, F.X., Alabi, C., Baanye, J., Wilson, M., Ganiu, O., Seong, Y. and Yi, S. (2025) 'Toward a unified framework for multimodal cognitive workload assessment in human-machine interaction systems', *SSRN Electronic Journal*, SSRN 5235980. DOI: 10.2139/ssrn.5235980.
- [2] Adaramola, O. (2025) 'The dark arts of crypto laundering and the Nigerian financial ecosystem: Examining regulatory perspectives of virtual assets and virtual asset providers in mitigating money laundering risks in Nigeria', *Journal of Economic Criminology*, 7, Article 100117. DOI: 10.1016/j.jeconc.2024.100117.
- [3] Aguocha, C.M. and George, S. (2021) 'An overview of gambling in Nigeria', *BJPsych International*, 18(2), pp. 30–32. DOI: 10.1192/bji.2020.28. (PubMed)
- [4] Agwuna, L., Irrshad, K. and Mazorodze, B.T. (2022) 'Assessing monetary policy via the Taylor Rule in a selection of middle-income emerging market economies: Issues and evidence', *Management and Economics Research Journal*, 8(2), pp. 1–14, Article 9900060. DOI: 10.18639/MERJ.2022.9900060. (HATASO)
- [5] Ahiauzu, N. (2023) Assessing the effectiveness of international anti-money laundering measures: A study of commercial banks in Nigeria. Doctoral thesis. Guildford: University of Surrey. DOI: 10.15126/thesis.900807.
- [6] Ajayi, K. (2010) 'Insulating the vaults from the tide of dirty money: Are the floodgates secure?', *Journal of Money Laundering Control*, 13(1), pp. 33–44. DOI: 10.1108/13685201011010191. (DOI.org)
- [7] Akhigbe, R., Falemi, A. and Akin-Oluyomi, O.T. (2023) 'A conceptual model for improving customer experience using workforce behavior and real-time operational data', *International Journal of Multidisciplinary Research and Growth Evaluation*, 4(6), pp. 1322–1338. DOI: 10.54660/IJMRGE.2023.4.6.1322-1338.
- [8] Akhigbe, R., Falemi, A. and Akin-Oluyomi, O.T. (2024) 'An advanced framework for technology adoption that supports employee readiness in modern organizations', *International Journal of Advanced Multidisciplinary Research and Studies*, 4(1), pp. 1637–1659. DOI: 10.62225/2583049X.2024.4.1.5344.
- [9] Akhigbe, R., Falemi, A. and Akin-Oluyomi, O.T. (2025) 'An advanced governance model for improving transparency, accountability and strategic execution in complex enterprises', *International Journal of Advanced Multidisciplinary Research and Studies*, 5(6), pp. 1169–1188. DOI: 10.62225/2583049X.2025.5.6.5341.
- [10] Akin-Oluyomi, O.T. and Akhigbe, R. (2022) 'A supply chain governance model for enhancing compliance and operational quality across retail networks', *International Journal of Multidisciplinary Research and Growth Evaluation*, 3(6), pp. 860–878. DOI: 10.54660/IJMRGE.2022.3.6.860-878. (ResearchGate)
- [11] Akin-Oluyomi, O.T. and Akhigbe, R. (2023a) 'An advanced framework for improving multi-site operational efficiency using data-driven performance indicators', *International Journal of Advanced Multidisciplinary Research and Studies*, 3(1), pp. 1763–1781. DOI: 10.62225/2583049X.2023.3.1.5343.
- [12] Akin-Oluyomi, O.T. and Akhigbe, R. (2023b) 'A proposed supply chain analytics framework for improving forecasting accuracy and reducing bottlenecks', *International Journal of Advanced Multidisciplinary Research and Studies*, 3(1), pp. 1686–1703. DOI: 10.62225/2583049X.2023.3.1.5338.
- [13] Akinteye, S.A., Mokube, M., Ochei, D. and Vutumu, A. (2023) 'The impact of internal audit on improving anti-money laundering (AML) and counter terrorist financing (CTF) controls in Nigeria', *UMYU Journal of Accounting and Finance Research*, 5(1), pp. 11–27. DOI: 10.61143/umyu-jaf.5(1)2023.002.
- [14] Akomea-Frimpong, I., Andoh, C., Akomea-Frimpong, A. and Dwomoh-Okudzeto, Y. (2019) 'Control of fraud on mobile money services in Ghana: An exploratory study', *Journal of Money Laundering Control*, 22(2), pp. 300–317. DOI: 10.1108/JMLC-03-2018-0023.
- [15] Auer, M. and Griffiths, M.D. (2023) 'Using artificial intelligence algorithms to predict self-reported problem gambling with

- account-based player data in an online casino setting', *Journal of Gambling Studies*, 39, pp. 1273–1294. DOI: 10.1007/s10899-022-10139-1.
- [16] Ayinde, M., Ojukwu, P.U. and Ohunyon, G. (2025) 'Organizational readiness for generative AI integration in healthcare operations: Comparative management capabilities between the U.S. and low- and middle-income countries', *International Journal of Advanced Multidisciplinary Research and Studies*, 5(6), pp. 2207–2222. DOI: 10.62225/2583049X.2025.5.6.6007.
- [17] Babajide, A.A., Lawal, A.I., Amodu, L.O., Asaleye, A.J., Ewetan, O.O., Olokoyo, F.O. and Matthew, O.A. (2020) 'Challenges of accountability in Nigeria: The role of deposit money bank', *Journal of Money Laundering Control*, 23(2), pp. 477–492. DOI: 10.1108/JMLC-10-2019-0082.
- [18] Baccouri, M., Talbi, D. and Hakimi, A. (2024) 'The effects of auditing and reporting standards and country-level governance on money laundering: A cross-country analysis', *Journal of Public Affairs*, 24(3), e2935. DOI: 10.1002/pa.2935.
- [19] Balogun, C.T. and Sabbah, G.M. (2021) 'Psycho-sociological factors as determinants of juvenile delinquency among adolescents in junior secondary schools in Patani Local Government Area of Delta State, Nigeria', *International Journal of Academic Management Science Research*, 5(10), pp. 34–40.
- [20] Blaszczyński, A., Shaffer, H.J. and Ladouceur, R. (2025) 'Cashless gambling: Potential money laundering and responsible gambling initiatives', *Journal of Gambling Business and Economics*, 17(1), pp. 99–116. DOI: 10.5750/jgbe.v17i1.2193. (DOI.org)
- [21] Braverman, J. and Shaffer, H.J. (2012) 'How do gamblers start gambling: Identifying behavioural markers for high-risk internet gambling', *European Journal of Public Health*, 22(2), pp. 273–278. DOI: 10.1093/eurpub/ckp232.
- [22] Braverman, J., LaPlante, D.A., Nelson, S.E. and Shaffer, H.J. (2013) 'Using cross-game behavioral markers for early identification of high-risk internet gamblers', *Psychology of Addictive Behaviors*, 27(3), pp. 868–877. DOI: 10.1037/a0032818.
- [23] Brooks, G. (2012) 'Online gambling and money laundering: "Views from the inside"', *Journal of Money Laundering Control*, 15(3), pp. 304–315. DOI: 10.1108/13685201211238052. (University of Portsmouth)
- [24] Buchanan, J. (2018) 'Money laundering through gambling devices', *Society and Business Review*, 13(2), pp. 217–237. DOI: 10.1108/SBR-08-2017-0057. (Macquarie University)
- [25] Catania, M. and Griffiths, M.D. (2022) 'Applying the DSM-5 criteria for gambling disorder to online gambling account-based tracking data: An empirical study utilizing cluster analysis', *Journal of Gambling Studies*, 38(4), pp. 1289–1306. DOI: 10.1007/s10899-021-10080-9.
- [26] Chitimira, H. (2021) 'An exploration of the current regulatory aspects of money laundering in South Africa', *Journal of Money Laundering Control*, 24(4), pp. 789–805. DOI: 10.1108/JMLC-10-2020-0120. (IDEAS/RePEc)
- [27] dalla Pellegrina, L., Di Maio, G., Masciandaro, D. and Saraceno, M. (2020) 'Organized crime, suspicious transaction reporting and anti-money laundering regulation', *Regional Studies*, 54(12), pp. 1761–1775. DOI: 10.1080/00343404.2020.1772963.
- [28] de Koker, L. (2003) 'Money laundering control: The South African model', *Journal of Money Laundering Control*, 6(2), pp. 166–181. DOI: 10.1108/13685200310809527. (vLex)
- [29] de Koker, L. (2009) 'The money laundering risk posed by low-risk financial products in South Africa: Findings and guidelines', *Journal of Money Laundering Control*, 12(4), pp. 323–339. DOI: 10.1108/13685200910996038.
- [30] Dreżewski, R., Sepielak, J. and Filipkowski, W. (2015) 'The application of social network analysis algorithms in a system supporting money laundering detection', *Information Sciences*, 295, pp. 18–32. DOI: 10.1016/j.ins.2014.10.015.
- [31] Enaifoghe, A., Dlamini, N.P. and Agwuna, L.U. (2020) 'African economic integration development in technological transformation: Assessing the importance of ethical leadership for policy implementation in SADC', *Journal of Economics and Behavioral Studies*, 12(6), pp. 11–20. DOI: 10.22610/jebbs.v12i6(J).3102.
- [32] Falemi, A., Akhigbe, R. and Akin-Oluyomi, O.T. (2023) 'A proposed framework for integrating employee retention systems with operational productivity metrics', *International Journal of Advanced Multidisciplinary Research and Studies*, 3(1), pp. 1704–1724. DOI: 10.62225/2583049X.2023.3.1.5339.
- [33] Falemi, A., Akhigbe, R. and Akin-Oluyomi, O.T. (2024) 'A conceptual enterprise risk management model that integrates HR strategy with operational analytics', *International Journal of Multidisciplinary Research and Growth Evaluation*, 5(6), pp. 1730–1753. DOI: 10.54660/IJMRGE.2024.5.6.1730-1753.
- [34] Fronzetti Colladon, A. and Remondi, E. (2017) 'Using social network analysis to prevent money laundering', *Expert Systems with Applications*, 67, pp. 49–58. DOI: 10.1016/j.eswa.2016.09.029.
- [35] Gaviyau, W. and Sibindi, A.B. (2023) 'Anti-money laundering and customer due diligence: Empirical evidence from South Africa', *Journal of Money Laundering Control*, 26(7), pp. 224–238. DOI: 10.1108/JMLC-06-2023-0103.
- [36] Gerbrands, P., Unger, B., Getzner, M. and Ferwerda, J. (2022) 'The effect of anti-money laundering policies: An empirical network analysis', *EPJ Data Science*, 11(1), Article 15. DOI: 10.1140/epjds/s13688-022-00328-8.
- [37] Gikonyo, C. (2018) 'Detection mechanisms under Kenya's anti-money laundering regime: Omissions and loopholes', *Journal of Money Laundering Control*, 21(1), pp. 59–70. DOI: 10.1108/JMLC-06-2017-0023.
- [38] Gikonyo, C. (2021) 'Banks in Kenya and anti-money laundering obligations: The conflicts of interests arising', *Journal of Money Laundering Control*, 24(2), pp. 427–439. DOI: 10.1108/JMLC-01-2020-0008.
- [39] Gupta, A., Dwivedi, D.N., Shah, J. and Jain, A. (2022) 'Data quality issues leading to sub optimal machine learning for money laundering models', *Journal of Money Laundering Control*, 25(3), pp. 551–555. DOI: 10.1108/JMLC-05-2021-0049.
- [40] Hameiri, S. and Jones, L. (2015) 'Regulatory regionalism and anti-money-laundering governance in Asia', *Australian Journal of International Affairs*, 69(2), pp. 144–163. DOI: 10.1080/10357718.2014.978737.
- [41] Haq, M.Z., Ayub, Z.A., Mohamed Yusoff, Z. and Khan, M.A.A. (2022) 'Factors influencing anti-money laundering regulatory approaches towards casinos and cryptocurrencies in Bangladesh', *Journal of Money Laundering Control*, 25(2), pp. 445–454. DOI: 10.1108/JMLC-04-2021-0034.
- [42] Hayble-Gomes, E. (2023) 'The use of predictive modeling to identify relevant features for suspicious activity reporting', *Journal of Money Laundering Control*, 26(4), pp. 806–830. DOI: 10.1108/JMLC-02-2022-0034.
- [43] Horobets, N., Reznik, O., Maliyk, V., Vyhivskiy, I. and Bobrishova, L. (2025) 'Artificial intelligence technologies in banking:



- Challenges and opportunities for anti-money laundering in the context of EU regulatory initiatives', *Journal of Money Laundering Control*, 28(4–5), pp. 593–608. DOI: 10.1108/JMLC-03-2025-0041.
- [44] Ige, A.A. (2022) 'Appraisal of the regulatory frameworks for combatting money laundering in Nigeria', *Journal of Money Laundering Control*, 25(2), pp. 345–357. DOI: 10.1108/JMLC-02-2021-0013.
- [45] Jullum, M., Løland, A., Huseby, R.B., Ånonsen, G. and Lorentzen, J. (2020) 'Detecting money laundering transactions with machine learning', *Journal of Money Laundering Control*, 23(1), pp. 173–186. DOI: 10.1108/JMLC-07-2019-0055.
- [46] Kamalludin, I. (2025) 'Money laundering, labor exploitation, and human trafficking within the online gambling network: An interdisciplinary approach to transnational crime in Southeast Asia', *AML/CFT Journal: The Journal of Anti Money Laundering and Countering the Financing of Terrorism*, 3(2), pp. 197–224. DOI: 10.59593/amlcft.2025.v3i2.230.
- [47] Lakew, N., Jonsson, J. and Lindner, P. (2024) 'Can payment behavior be used to signal harmful gambling? A Delphi study among different stakeholders on key indicators', *Gaming Law Review*, 28(8), pp. 264–278. DOI: 10.1089/glr.2024.0008.
- [48] Langdale, J. (2023) 'Money laundering in Australian casinos', *Journal of Money Laundering Control*, 26(7), pp. 99–109. DOI: 10.1108/JMLC-09-2022-0136. (DOI.org)
- [49] Li, X., Liu, S., Li, Z., Han, X., Shi, C., Hooi, B., Huang, H. and Cheng, X. (2020) 'FlowScope: Spotting money laundering based on graphs', *Proceedings of the AAAI Conference on Artificial Intelligence*, 34(4), pp. 4731–4738. DOI: 10.1609/aaai.v34i04.5906.
- [50] Lima, R.S., Serrano, A.L.M., Imoniana, J.O. and Cupertino, C.M. (2022) 'Identifying financial patterns of money laundering with social network analysis: A Brazilian case study', *Journal of Money Laundering Control*, 25(1), pp. 118–134. DOI: 10.1108/JMLC-12-2020-0139.
- [51] Lokanan, M.E. (2025) 'Enhancing AML compliance: A machine learning approach to suspicious activity detection through routine activity theory', *Journal of Money Laundering Control*, 28(4–5), pp. 680–698. DOI: 10.1108/JMLC-07-2024-0114.
- [52] McNaughton, K.J. (2023) 'The variability and clustering of Financial Intelligence Units (FIUs): A comparative analysis of national models of FIUs in selected western and eastern (post-Soviet) countries', *Journal of Economic Criminology*, 2, Article 100036. DOI: 10.1016/j.jeconc.2023.100036.
- [53] Morse, E.A. (2007) 'Extraterritorial internet gambling: Legal challenges and policy options', *International Journal of Intercultural Information Management*, 1(1), pp. 33–48. DOI: 10.1504/IJIM.2007.014369. (DOI.org)
- [54] Muggleton, N., Parpart, P., Newall, P., Leake, D., Gathergood, J. and Stewart, N. (2021) 'The association between gambling and financial, social and health outcomes in big financial data', *Nature Human Behaviour*, 5(3), pp. 319–326. DOI: 10.1038/s41562-020-01045-w.
- [55] Naheem, M.A. (2018) 'TBML suspicious activity reports – a financial intelligence unit perspective', *Journal of Financial Crime*, 25(3), pp. 721–733. DOI: 10.1108/JFC-10-2016-0064.
- [56] Ofori, E. and Appiah, M.O. (2025) 'Multinational tax evasion and money laundering: Examining the financial investigation system in Ghana', *Journal of Money Laundering Control*, 28(2), pp. 442–462. DOI: 10.1108/JMLC-09-2024-0150.
- [57] Ogbeide, H., Thomson, M.E., Gonul, M.S., Pollock, A.C., Bhowmick, S. and Bello, A.U. (2023) 'The anti-money laundering risk assessment: A probabilistic approach', *Journal of Business Research*, 162, Article 113820. DOI: 10.1016/j.jbusres.2023.113820. (ScienceDirect)
- [58] Olujobi, O.J. and Yebisi, E.T. (2023) 'Combating the crimes of money laundering and terrorism financing in Nigeria: A legal approach for combating the menace', *Journal of Money Laundering Control*, 26(2), pp. 268–289. DOI: 10.1108/JMLC-12-2021-0143.
- [59] Oztas, B., Cetinkaya, D., Adedoyin, F., Budka, M., Aksu, G. and Dogan, H. (2024) 'Transaction monitoring in anti-money laundering: A qualitative analysis and points of view from industry', *Future Generation Computer Systems*, 159, pp. 161–171. DOI: 10.1016/j.future.2024.05.027.
- [60] Pavlidis, G. (2020) 'Financial information in the context of anti-money laundering: Broadening the access of law enforcement and facilitating information exchanges', *Journal of Money Laundering Control*, 23(2), pp. 369–378. DOI: 10.1108/JMLC-10-2019-0081.
- [61] Reite, E.J., Karlsen, J. and Westgaard, E.G. (2025) 'Improving client risk classification with machine learning to increase anti-money laundering detection efficiency', *Journal of Money Laundering Control*, 28(1), pp. 93–107. DOI: 10.1108/JMLC-03-2024-0040. (DOI.org)
- [62] Sabbah, G.M. (2021) 'Psychosocial factors as predictors of moral disengagement among in-school adolescents in Ibadan Metropolis', *International Journal of Academic Information Systems Research*, 5(10), pp. 1–7.
- [63] Sabbah, G.M. and Ojo, Y. (2023) 'Influence of peer approval seeking, socio-economic status and locus of control on academic self-handicapping behaviour of undergraduates in Oyo State, Nigeria', *British Journal of Multidisciplinary and Advanced Studies: Education, Learning, Training & Development*, 4(4), pp. 98–112. DOI: 10.37745/bjmas.2022.0261.
- [64] Shittu, H. and Nabil, M. (2023) 'Smart supply chain management with attribute-based encryption access control', 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), pp. 198–204. DOI: 10.1109/CCWC57344.2023.10099268.
- [65] Shittu, M.A., Adeniji, I.O., Shittu, H. and Opara, I.S. (2022) 'Blockchain-assisted secure data exchange architectures for SCADA-controlled power systems', *Iconic Research and Engineering Journals*, 6(3), pp. 359–380. DOI: 10.64388/IREV6I3-1714041.
- [66] Shittu, M.A., Shittu, H., Adeleke, O.J. and Adedokun, O.J. (2023) 'Digital twin modeling for real time monitoring and fault detection in smart substations', *International Journal of Industrial Engineering Research and Development*, 14(2), pp. 25–44. DOI: 10.34218/IJIERD_14_02_003.
- [67] Sichali, J.M., Bunn, C., McGee, D., Marionneau, V.K., Yendork, J.S., Glozah, F., Udedi, M. and Reith, G. (2023) 'Regulation of gambling in Sub-Saharan Africa: Findings from a comparative policy analysis', *Public Health*, 214, pp. 140–145. DOI: 10.1016/j.puhe.2022.07.018.
- [68] Siu Lam, C. and Greenlees, M. (2017) 'Casino money laundering regulations – Macao and USA', *Journal of Money Laundering Control*, 20(1), pp. 52–69. DOI: 10.1108/JMLC-04-2016-0015. (Macao Polytechnic University)
- [69] Sotande, E. (2018) 'The regime against money laundering: A call for scientific modelling', *Journal of Money Laundering Control*, 21(4), pp. 584–593. DOI: 10.1108/JMLC-11-2017-0066.

- [70] Steinmetz, F. and Fiedler, I. (2019) 'A state-operated blockchain-based system for the transparent processing of online gambling payments in Germany', *Gaming Law Review*, 23(10), pp. 715–725. DOI: 10.1089/glr.2019.23108. (Sage Journals)
- [71] Sultan, N. and Mohamed, N. (2023) 'Financial intelligence unit of Pakistan: An evaluation of its performance and role in combating money laundering and terrorist financing', *Journal of Money Laundering Control*, 26(4), pp. 862–876. DOI: 10.1108/JMLC-04-2022-0060.
- [72] Turksen, U., Benson, V. and Adamyk, B. (2024) 'Legal implications of automated suspicious transaction monitoring: Enhancing integrity of AI', *Journal of Banking Regulation*, 25, pp. 359–377. DOI: 10.1057/s41261-024-00233-2.
- [73] Van Staden, N., Kilian, E. and McIntyre, J.-L. (2025) 'A comparative dive into virtual asset legislation in South Africa, Mauritius, Namibia and the UK', *Journal of Money Laundering Control*, 28(7), pp. 50–64. DOI: 10.1108/JMLC-10-2024-0170.
- [74] Yeoh, P. (2020) 'Banks' vulnerabilities to money laundering activities', *Journal of Money Laundering Control*, 23(1), pp. 122–135. DOI: 10.1108/JMLC-05-2019-0040.

