

Enhanced Due Diligence in Prepaid and Cross-Border Payment Platforms: A Risk-Typology Framework for Cardholder Account Monitoring

Adaora Kalu^{1*}, Samuel Fadero², Omotayo Pedro³, Oluwatobiloba Mide-Ibrahim⁴

¹Independent Researcher, GA, USA, adaorakalu@gmail.com

²SanlamAllianz Life Insurance Ltd, Lagos Nigeria, femfad20@gmail.com

³Citco Group Limited, Vilnius, Lithuania, tayopedro@yahoo.com

⁴FinServe Pro, USA, tobbymide@gmail.com

*Corresponding Author: Adaora Kalu, adaorakalu@gmail.com

Abstract

This review examines how enhanced due diligence can be strengthened in prepaid and cross-border payment environments through a risk-typology approach to cardholder account monitoring. It adopts a structured narrative review method, synthesising interdisciplinary evidence from anti-money-laundering research, payment systems, financial regulation, transaction analytics, risk management, digital finance, and monitoring technologies. The analysis evaluates the expansion of prepaid ecosystems, cross-border exposure, financial-crime typologies, cardholder profiling, alert logic, investigative frameworks, regulatory governance, and technological innovation.

The findings show that effective monitoring depends on integrating customer identity, product characteristics, funding patterns, transaction velocity, geographic exposure, counterparties, devices, and historical behaviour within a dynamic risk architecture. Static onboarding classifications and isolated transaction thresholds are insufficient for detecting complex patterns such as rapid pass-through activity, mule-account behaviour, unusual cross-border corridors, account takeover, and linked transactional networks. The review further demonstrates that enhanced due diligence is most effective when embedded within a continuous investigative cycle that connects alert triage, contextual verification, source-of-funds assessment, relationship analysis, documented judgement, escalation, and feedback into future risk calibration. Cross-border compliance also requires consistent governance, secure information exchange, proportionate reporting, and coordination across jurisdictions.

The review concludes that resilient monitoring systems should combine behavioural baselines, typology-driven indicators, explainable analytics, and human oversight. It recommends continuous validation of alert scenarios, periodic recalibration of risk scores, stronger data governance, investment in investigator expertise, and careful integration of machine learning. Future research should test these frameworks on realistic multi-jurisdictional datasets while

preserving privacy, proportionality, transparency, and financial inclusion. Particular attention should be given to model drift, emerging typologies, interoperability constraints, and jurisdiction-specific behavioural variation.

Keywords: Enhanced due diligence; Prepaid payments; Cross-border transactions; Risk typologies; Cardholder monitoring; Financial crime

DOI: 10.21590/ijtmh.09.04.434

1. Introduction

1.1 Expansion of Prepaid Payment Ecosystems

The prepaid payment ecosystem has evolved from a narrow set of stored-value instruments into infrastructure connecting network-branded cards, digital wallets, mobile-money accounts, payroll products and other electronic payment channels. General-purpose reloadable cards were significant because they combined prefunded value with payment-network functionality, permitting purchases, cash withdrawals and recurring use without requiring a conventional deposit account. Their adoption also revealed that transaction intensity, funding method, merchant category and user characteristics shape usage patterns and exposure to fraud, demonstrating that prepaid instruments became persistent transactional accounts rather than simple cash substitutes requiring systematic oversight (Hayashi & Cuddy, 2014).

The inclusionary appeal of prepaid products rests on their capacity to provide electronic-payment functionality to people who may lack traditional bank accounts. Yet expansion has not automatically eliminated barriers to formal finance. Evidence from the United States shows that prepaid cards can facilitate shopping, wage receipt, bill payment and person-to-person transfers, while adoption among unbanked households remains uneven and constrained by liquidity, privacy and access considerations. Consequently, ecosystem growth has produced a heterogeneous cardholder population whose transaction behaviour cannot be interpreted through a single customer model (Toh, 2021).

This broadening of stored-value finance is visible where prepaid functionality converges with mobile-money platforms. Mobile money has transformed retail finance by allowing users to store monetary value, initiate transfers and access financial services through telecommunications infrastructure rather than exclusively through bank branches. Across African markets, this model has widened the institutional field to include telecommunications firms, banks, agents, technology providers and regulators, creating interconnected payment ecosystems in which value

moves across multiple technological and organisational interfaces (Ahmad, Green & Jiang, 2020).

Kenya illustrates how such platforms can progress from transactional convenience to embedded financial infrastructure. The widespread diffusion of M-PESA enabled households to store and transfer value through mobile accounts and was associated with improvements in consumption resilience and poverty reduction. Its scale demonstrates that prepaid or prefunded payment mechanisms can become routine components of household financial management, increasing transaction volumes, network effects and customer relationships requiring effective identification and behavioural monitoring (Suri & Jack, 2016).

Nigeria provides a contrasting but equally important trajectory. Although the country combines a large consumer base with numerous mobile-money operators, adoption initially lagged expectations despite licensing and policy support. Research attributes part of this outcome to weaknesses in business-model design, customer segmentation and scale, underscoring that ecosystem expansion depends not only on technological availability but also on sustainable delivery arrangements capable of generating recurrent usage and trusted customer relationships (David-West, Iheanachor & Umukoro, 2020).

Infrastructure further conditions how prepaid ecosystems develop. Evidence across Sub-Saharan Africa indicates that physical-service constraints can increase reliance on mobile channels for financial transactions, where conventional financial infrastructure is limited. This relationship helps explain why agent networks, mobile interfaces and prefunded accounts have become important gateways into formal payment systems, while also producing geographically dispersed transaction patterns that complicate branch-based approaches to customer oversight (Mothobi & Grzybowski, 2017).

The expansion is not confined to Africa. Evidence from low- and middle-income Asian economies indicates that mobile-payment development can strengthen financial inclusion when supported by cooperation among governments, financial institutions and technology companies. Such findings highlight a global shift from institution-centred payment delivery toward platform-centred ecosystems in which customer access, stored value, payment initiation and ancillary financial services operate through interoperable digital channels (Lee, Chen & Chu, 2023).

However, wider access alters the integrity responsibilities of payment providers. Greater formalisation can improve transaction visibility, yet financial inclusion and anti-money-laundering objectives do not align automatically where privacy concerns, cash preferences or informal economic activity discourage use of monitored services. The expansion of prepaid and mobile channels therefore creates a dual regulatory imperative: preserve low-friction access while ensuring that growing transaction networks remain sufficiently transparent for

proportionate customer due diligence and suspicious-activity detection (de Koker & Jentzsch, 2013).

Finally, the economic significance of these ecosystems extends beyond payments as transactional infrastructure can support entrepreneurial liquidity, business continuity and financial stability. In African economies, the relationship between entrepreneurship and financial stability reinforces the importance of payment systems that can support routine commercial exchange without unmanaged fragility. As prepaid and cross-border platforms become embedded in everyday commerce, their expansion strengthens the case for enhanced due diligence frameworks that distinguish legitimate high-frequency usage from patterns requiring escalated scrutiny (Agwuna, 2022).

1.2 Cross-Border Transaction Risk Exposure

Cross-border payment exposure arises not merely from transaction volume but from the interaction of multiple jurisdictions, currencies, intermediaries, and regulatory regimes. Digital remittance rails increasingly connect consumers and businesses to international networks, reducing transfer frictions while expanding the number of actors that may participate in a single payment chain. This infrastructural complexity can obscure the origin, destination, and economic purpose of transactions when customer, merchant, agent, and intermediary data are fragmented across platforms or countries (Rodima-Taylor & Grimes, 2019).

For prepaid and card-based platforms, risk is intensified when value moves through correspondent relationships or technology-enabled remittance channels that separate the customer-facing provider from institutions responsible for settlement. Such layered arrangements may improve speed and access, yet they also create dependencies on data interoperability, identity resolution and information sharing. De-risking within correspondent banking further demonstrates how financial institutions respond when cross-border relationships are perceived as costly or difficult to monitor, potentially concentrating flows in fewer channels or shifting activity toward alternative infrastructures (Rella, 2019).

Exposure also varies with macroeconomic conditions. Exchange-rate movements, monetary-policy divergence and inflation dynamics can materially alter the value, direction and frequency of international transfers, particularly across emerging markets. Evidence from Brazil, Chile, Mexico, South Africa and Turkey demonstrates that policy rates and exchange-rate conditions are interrelated, reinforcing the need to interpret unusual transaction values within their jurisdictional and economic context rather than treating nominal thresholds as universally comparable risk signals (Agwuna, Kaseeram & Mazorodze, 2022).

In Nigeria, the challenge is compounded by the need to balance financial openness with safeguards against misuse of formal institutions. Nigerian AML scholarship has long emphasised risk-based suspicious-transaction reporting, stronger institutional coordination and adequate compliance capability. For prepaid and cross-border platforms, these concerns support monitoring models that evaluate customer identity, funding sources, geographic corridors, transaction velocity and counterparties collectively instead of relying solely on single triggers (Ajayi & Abdulkareem, 2010).

The regulatory problem is equally evident in mobile-money environments. Comparative evidence from Kenya and the Philippines shows that international AML standards must be adapted to technologically mediated payment systems so that risk controls do not undermine financial inclusion. A proportionate risk-based model is essential where cross-border prepaid products serve legitimate remittance needs but may also permit rapid, remote and repeated transfers (Vlcek, 2011).

African regulatory experience further demonstrates that exposure is shaped by differences in supervisory effectiveness. Comparative analysis of Mauritius and South Africa identifies risk-based regulation as central to AML frameworks while also highlighting the need for legal adaptation as financial crime evolves. For platform operators, jurisdictional differences can therefore create uneven control environments across connected payment chains (Beebejaun & Dulloo, 2023).

Finally, cross-border laundering presents an enforcement problem because transactional conduct may span territories while investigative authority remains jurisdictionally bounded. The development of extraterritorial and long-arm approaches reflects attempts to address this mismatch between internationally mobile activity and territorially organised law enforcement. Effective cardholder monitoring must consequently preserve granular transactional and customer information to support escalation, information exchange and investigation where suspicious activity traverses national boundaries (Amrani & Ali, 2022).

1.3 Risk-Typology Approaches to Account Monitoring

Risk-typology approaches translate known or emerging financial-crime behaviours into observable indicators that can be monitored across cardholder accounts. Rather than treating every unusual transaction as equivalent, typology-based monitoring groups activity into recognizable behavioural configurations, such as rapid movement of funds, repeated threshold-adjacent transactions, abrupt geographic shifts, circular transfers, or unexpected relationships among accounts. This approach is particularly relevant to prepaid and cross-border platforms, where high transaction velocity and distributed payment channels can make isolated events appear legitimate while the wider pattern is anomalous. Nigerian research on machine-learning applications similarly emphasizes the limitations of fragmented, legacy rule systems and the

value of integrated techniques capable of examining parties, accounts, and transactions together (Mohammed et al., 2022).

A robust typology framework should therefore combine customer context with transactional behaviour. Risk indicators become more informative when interpreted against expected account purpose, funding sources, transaction frequency, counterparties, and geographic exposure. South African risk-based AML scholarship reinforces the need for ongoing assessment across differing risk scenarios rather than static compliance at onboarding, supporting continuous recalibration of monitoring intensity as account behaviour changes (Henning & Hauman, 2017).

Graph-based methods strengthen this logic by representing accounts as nodes and transactions as relationships. Such models can identify unusual structures, repeated paths, dense clusters, or anomalous subgraphs that may be difficult to detect through transaction-level rules alone. Empirical work on bank-transaction graphs demonstrates that anomaly detection can distinguish suspicious behavioural patterns by analysing both account characteristics and network structure (Dumitrescu, Băltoiu & Budulan, 2022). For prepaid environments, this relational perspective is especially valuable because several cards, devices, beneficiaries, funding sources, or merchants may form a connected pattern whose aggregate significance is not visible from any single event.

Machine learning further extends typology detection where predefined rules cannot anticipate every laundering strategy. However, unusual behaviour is not synonymous with criminal activity; limited labelled data means that algorithmic systems often identify anomalies rather than prove money laundering. Consequently, automated outputs should support, rather than replace, analyst judgement and contextual investigation (Canhoto, 2021).

Typologies must also evolve because criminal networks adapt to regulation. Evidence from dynamic network analysis shows that AML policy changes can alter network composition, international connections, and organisational behaviour, indicating that monitoring scenarios require periodic review rather than permanent thresholds (Gerbrands et al., 2022). Accordingly, effective account monitoring should integrate client risk profiling with suspicious-behaviour flagging, while maintaining interpretability and validation so alerts remain operationally useful and proportionate (Jensen & Iosifidis, 2023).

1.4 Review Scope, Objectives, and Approach

This review examines enhanced due diligence within prepaid and cross-border payment platforms, with particular emphasis on how risk typologies can strengthen cardholder account monitoring. Its scope encompasses prepaid cards, mobile-enabled stored-value products, digital payment accounts, remittance channels, and related cross-border transaction environments in which customer activity may traverse multiple institutions, jurisdictions, currencies, and technological interfaces. The review focuses on the interaction between customer risk,

transaction behaviour, geographic exposure, counterparties, funding patterns, and platform architecture, while recognising the need to balance financial inclusion, operational efficiency, and regulatory integrity.

The primary objective is to develop a coherent risk-typology framework that explains how observable account behaviours can be translated into meaningful monitoring indicators for enhanced due diligence. Specific objectives include identifying major sources of exposure within prepaid and cross-border ecosystems, examining recurring financial-crime typologies, assessing approaches to cardholder risk profiling and segmentation, evaluating alert-generation and account-monitoring logic, and considering governance, investigative, and technological mechanisms that support proportionate escalation.

Methodologically, the review adopts a structured narrative approach that synthesises interdisciplinary evidence from anti-money-laundering research, payment systems, financial regulation, transaction analytics, risk management, and digital finance. The analysis is organised thematically to compare established practices with emerging approaches, particularly those involving behavioural analytics, anomaly detection, network analysis, and adaptive monitoring. Rather than treating enhanced due diligence as a discrete post-alert procedure, the review positions it as part of a continuous risk-assessment cycle linking onboarding, transaction monitoring, investigation, escalation, and ongoing customer-risk recalibration. This framing supports consistent, evidence-informed monitoring across evolving international digital payment environments.

2. Prepaid and Cross-Border Risk Architecture

Prepaid and cross-border payment platforms operate as layered ecosystems in which financial-crime exposure emerges from product design, customer identity, funding methods, transaction channels, geography, intermediaries, and data infrastructure. Risk therefore cannot be located in a single transaction or component. Open-system prepaid instruments may be loaded through multiple channels, used at dispersed merchants, converted into cash, and transported across borders, creating portability and fungibility that complicate conventional controls. Analysis of cross-border prepaid cards shows that characteristics supporting remittances and convenience can also weaken visibility over the movement and beneficial control of stored value (Linn, 2008).

At the product layer, risk is shaped by reloadability, cash access, transaction limits, transferability, anonymity, and connectivity to international payment networks. These characteristics determine how easily value may enter, circulate through, and exit the platform. Prepaid products can be exploited through card mules, remote acquisition, international shipment, repeated loading, or rapid conversion of stored value where identification and transaction aggregation are weak. Risk architecture should therefore distinguish limited-purpose

instruments from higher-functionality products capable of cross-border withdrawal or repeated loading instead of assigning a uniform risk profile to all prepaid accounts (Choo, 2009).

Jurisdictional design forms another layer. Comparative evidence from Nigeria, the United Kingdom, the United States, and India demonstrates differences in licensing, agent oversight, thresholds, identification, and product restrictions. Such variation matters because controls applied at issuance may not correspond with those governing redemption, agent activity, or downstream transactions elsewhere. Platforms should therefore map each cardholder relationship to the regulatory status of issuers, programme managers, agents, processors, and jurisdictions while preserving proportionate safeguards against misuse (Esoimeme, 2018).

Customer identity is the architecture's principal attribution layer. Digital payment systems depend on reliable linkage between persons and the credentials, devices, accounts, and instruments through which activity occurs. Digital KYC can improve onboarding and access, but its effectiveness depends on registration quality, authoritative data, interoperability, cybersecurity, and cross-jurisdictional recognition. Identity should consequently be treated as continuously validated information rather than a static onboarding record, allowing changes in device use, account control, documentation, or geographic behaviour to modify cardholder risk (Arner et al., 2019).

Transaction risk intensifies when platform functionality combines with speed, distance, and limited face-to-face oversight. Mobile-money research identifies anonymity, rapidity, elusiveness, and insufficient oversight as material AML/CFT concerns. In prepaid and cross-border environments, these characteristics justify monitoring loading frequency, transfer velocity, withdrawal behaviour, merchant categories, counterparties, and geographic corridors rather than relying solely on transaction size. The appropriate unit of analysis is often the behavioural sequence, because individually ordinary transactions may collectively indicate pass-through activity, structuring, unexplained geographic dispersion, or activity inconsistent with account purpose (Whisker & Lokanan, 2019).

Agent and channel risk must also be incorporated. Evidence from Ghanaian mobile-money services shows that fraud exposure can arise across relationships involving operators, agents, partnering banks, regulators, and subscribers. Distributed payment systems therefore require controls beyond the issuer's internal environment. Agent authentication, transaction permissions, settlement patterns, unusual reversals, device associations, and concentrated activity should feed enterprise monitoring, enabling platforms to distinguish cardholder anomalies from agent-level or network-level irregularities (Akomea-Frimpong et al., 2019).

The architecture must simultaneously protect information required for enhanced due diligence. Remittance systems process identity, payment, location, and behavioural data, creating privacy and cybersecurity exposures alongside financial-crime risk. Country-level differences in data

protection can complicate international monitoring and information sharing. EDD architecture therefore requires lawful access, traceable processing, secure retention, and controls that keep risk intelligence available for investigation without unnecessarily exposing cardholder information (Akanfe, Valecha & Rao, 2020).

Access-control design becomes critical where actors require different visibility. Attribute-based encryption demonstrates how access policies can be tied to authorised characteristics, allowing sensitive information to remain protected while designated stakeholders perform defined functions. In payment monitoring, this principle supports differentiated access for investigators, compliance analysts, operations personnel, and external partners, reducing unnecessary disclosure while preserving information flows needed for escalation and case management (Shittu & Nabil, 2023).

Integrity across distributed data exchanges is equally important. Blockchain-assisted architectures illustrate how tamper-resistant records, auditability, non-repudiation, and controlled information sharing can strengthen trust where multiple organisations exchange operational data. Comparable principles can support reliable transaction histories, evidential continuity, and reconciliation across processors or jurisdictions, provided governance and interoperability limitations are addressed rather than assuming that distributed technology independently resolves compliance risk (Shittu et al., 2022).

Decentralised transaction models further show that transparency, participant authentication, programmable rules, and secure recordkeeping can be embedded within multi-party exchanges. These characteristics are relevant because prepaid risk frequently spans several actors rather than remaining within one account. A mature architecture should connect customer identity, product characteristics, agents, devices, funding sources, transaction networks, geography, and investigative outcomes within a unified risk view. Such integration allows enhanced due diligence to operate dynamically, with new activity recalibrating risk and directing proportionate scrutiny toward combinations of indicators that materially depart from expected cardholder behaviour (Shittu et al., 2021).

3. Financial Crime Typologies in Payment Platforms

Financial crime within prepaid and cross-border payment platforms rarely manifests through a single, universally identifiable transaction. It is more accurately understood through typologies: recurring combinations of actors, behaviours, transaction sequences, channels and contextual indicators associated with fraud, laundering or account misuse. Typology-based analysis is therefore concerned with identifying patterns rather than merely testing transactions against isolated thresholds. Electronic payment fraud is especially challenging because legitimate and illicit transactions frequently coexist within high-volume data streams, while criminal techniques

evolve in response to existing controls, producing concept drift and continuously changing fraud signatures (Abdallah, Maarof & Zainal, 2016).

One important typology involves compromised payment credentials and subsequent unauthorised card usage. In digital environments, stolen card details may be exploited remotely without possession of the physical card, while transaction behaviour can shift rapidly across merchants, amounts, locations and time periods. Research on credit-card fraud demonstrates the importance of analysing historical cardholder behaviour and transaction aggregation because fraudulent activity is more reliably identified through deviation from established spending patterns than by transaction value alone (Dornadula & Geetha, 2019). For prepaid platforms, this implies that sudden changes in merchant categories, transaction frequency, international use or cash-out behaviour may become meaningful when assessed relative to the account's established history.

Temporal and geographic irregularities constitute a related typology. Fraudulent activity can exhibit unusual concentrations of transactions within short periods, abrupt changes in transaction location, or atypical combinations of spatial and temporal characteristics. Advanced fraud-detection research demonstrates that integrating these dimensions can reveal patterns that conventional feature-by-feature analysis may overlook. Such evidence is particularly pertinent to cross-border prepaid accounts, where geographic mobility is legitimate but rapid or improbable changes in location can nevertheless strengthen an existing risk signal when combined with other anomalies (Cheng et al., 2020).

Mobile-enabled payment platforms create additional typologies involving identity compromise, SIM-related manipulation and social engineering. Kenya's experience illustrates how mobile financial ecosystems can be exploited when weaknesses arise in subscriber identification, registration, authentication and forensic traceability. These vulnerabilities reinforce the importance of linking account monitoring to device, SIM, identity and transaction information rather than viewing the payment account as an isolated financial record (Wanjohi, 2017).

Money-mule activity represents another significant typology because apparently legitimate cardholders or account holders can become intermediaries for illicit funds. Mules may knowingly or unknowingly receive criminal proceeds before forwarding, withdrawing, or redistributing them, thereby separating underlying crime from final fund movement. Systematic evidence indicates that recruitment can occur through employment propositions, social relationships, online communications and other forms of inducement, creating heterogeneous mule profiles that complicate reliance on conventional customer categories (Abdul Rani, Syed Mustapha Nazri & Zolkafli, 2023).

Operationally, mule behaviour may appear as incoming funds inconsistent with prior account activity followed by rapid onward transfers, withdrawals or conversion into another form of

value. Geographic origin and destination, transaction timing and sudden increases in activity may therefore provide stronger evidence when assessed collectively. Importantly, previously low-risk customers can become conduits after onboarding, demonstrating why risk classification cannot remain static throughout the customer relationship (Esoimeme, 2020).

Laundering typologies in digital payment systems can also involve fragmentation and layering across multiple accounts or channels. Instead of moving illicit value directly between two points, actors may distribute transactions across instruments, counterparties and jurisdictions to weaken the apparent connection between source and destination. African scholarship on ICT-enabled financial systems emphasises that technological development simultaneously creates opportunities for financial inclusion and new avenues for laundering, requiring regulatory controls and analytical technologies capable of identifying suspicious digital patterns at scale (Couchoro, Sodokin & Koriko, 2021).

Adaptive analysis is especially important because criminals may deliberately modify transaction characteristics after controls become predictable. Aggregating transaction histories can expose sequences and relationships that would remain inconspicuous when events are assessed independently. Research applying transaction aggregation and representation-learning techniques to card fraud illustrates how behavioural context can improve recognition of changing fraud patterns without assuming that every anomalous transaction is inherently illicit (Yeşilkanat et al., 2020).

Typology development should nevertheless avoid simplistic behavioural profiling. Behavioural research demonstrates that problematic conduct can reflect interacting psychosocial influences rather than a single predictor, supporting analytical frameworks that consider combinations of indicators instead of deterministic associations between one characteristic and misconduct (Sabboh, 2021). Similarly, evidence examining socio-behavioural determinants shows that contextual and interpersonal conditions may influence behaviour in different ways, reinforcing the methodological value of multifactor assessment rather than categorical assumptions about particular individuals or groups (Balogun & Sabboh, 2021).

4. Cardholder Risk Profiling and Segmentation

Cardholder risk profiling and segmentation are central to enhanced due diligence because they convert heterogeneous customer information into differentiated levels of monitoring intensity. In prepaid and cross-border environments, an effective profile should integrate verified identity, occupation or business purpose, expected account use, funding sources, product functionality, geographic exposure, delivery channel, transaction velocity, counterparty relationships and historical behaviour. The objective is not to assign immutable labels, but to establish an evidence-based expectation of legitimate activity against which emerging deviations can be evaluated. South African evidence on customer due diligence underscores the movement toward

risk-based dynamic profiling as digital banking expands the customer information available to compliance functions (Gaviyau & Sibindi, 2023).

The quality of segmentation depends first on the quality and relevance of customer data. Know-your-customer information can support granular risk classification when demographic, occupational, account and transactional characteristics are analysed collectively rather than through isolated indicators. Machine-learning analysis of bank KYC data demonstrates that customers, regions, products and services can be classified into differentiated risk profiles, suggesting that assessment can move beyond manually assigned categories where institutions possess structured information (Chen, 2020). For prepaid issuers, a low-value account at onboarding should not automatically remain low risk if later behaviour indicates international activity or unexplained funding changes.

Risk scoring should also recognise uncertainty. Customer characteristics rarely provide deterministic evidence of financial crime, and the same observable feature may carry different implications across markets or transaction corridors. Probabilistic approaches to anti-money-laundering assessment are valuable because they require consideration of conditional risk, evidence quality and expert judgement instead of treating compliance as a box-ticking exercise. This matters when enhanced due diligence depends on combinations of weak signals rather than one decisive indicator (Ogbeide et al., 2023).

Profiles must further evolve throughout the account lifecycle. Empirical banking evidence indicates that changes in transaction volume, bank usage, credit characteristics and firm-specific conditions can alter the probability that subsequent activity will be identified as suspicious. A cardholder segmentation model should consequently support migration between risk bands when behaviour changes materially rather than leaving outdated classifications intact (Reite et al., 2023). In cross-border prepaid platforms, such migration may be triggered by new jurisdictions, sharp increases in loads, frequent cash withdrawals, new beneficiaries or activity inconsistent with the stated relationship purpose.

Behavioural segmentation provides a practical means of structuring this continuous assessment. Research on credit-card users shows that recency, frequency and monetary measures can be combined with clustering and predictive classification to identify groups with distinct usage characteristics. For AML purposes, the same logic can be adapted cautiously: recency, frequency and value should be combined with geographic, device, merchant and counterparty variables to create monitoring cohorts whose expected patterns are coherent enough to make anomalies meaningful (Djurisic et al., 2020).

Clustering is particularly useful where a customer population is too heterogeneous for uniform thresholds. Two-stage analysis of retail-banking customers demonstrates that segmentation can reveal distinct behavioural patterns obscured in aggregate data. In prepaid platforms, clustering

can similarly distinguish occasional domestic users, payroll-linked cardholders, frequent travellers, remittance-oriented customers and commercially active users, allowing alert logic to reflect legitimate differences in account purpose (Kovács, Ko & Asemi, 2021).

Algorithmic profiling nevertheless requires careful validation because statistically visible differences can become inappropriate proxies for risk. Research applying machine learning to financial-service portfolios illustrates the capacity of data-driven methods to identify patterns across multidimensional datasets, while also highlighting uncertainty in variables underlying risk profiles. Segmentation models should therefore prioritise demonstrably risk-relevant features and test for stability, interpretability and bias before outputs are used to intensify scrutiny (Lozano-Medina, Hervert-Escobar & Hernandez-Gress, 2020).

Context matters when interpreting financial behaviour. Socio-economic conditions can influence income patterns and financial responsibilities, meaning that changes in inflows or expenditure should not automatically be treated as suspicious without plausible economic context. Evidence from Ibadan illustrates how economic pressures interact with psychosocial and household variables, reinforcing contextual interpretation when constructing behavioural expectations for cardholders (Ezeani & Sabboh, 2021).

Similarly, multivariate behavioural research demonstrates that outcomes are often associated with interacting personal and contextual factors rather than a single explanatory characteristic. Applied to account monitoring, this supports composite risk assessment in which transaction velocity, funding origin, geography, account tenure, counterparties and deviations from prior behaviour are considered jointly rather than allowing one attribute to determine a cardholder segment (Sabbah & Ojo, 2023).

Finally, the credibility of segmentation depends on measurement discipline. Risk categories, scoring scales and escalation thresholds should be defined clearly, tested, reviewed against observed outcomes and recalibrated when evidence shows weak discrimination. Principles of instrument development and validation provide a methodological foundation for ensuring that composite measures capture the construct they claim to assess rather than producing numerical labels (Sabbah, 2022). For enhanced due diligence, this requires documented feature selection, model governance, periodic validation, and clear pathways through which new transaction evidence can modify risk classification and monitoring intensity.

5. Account Monitoring Indicators and Alert Logic

Account monitoring in prepaid and cross-border payment platforms should operate through continuous signal collection, contextual comparison and proportionate escalation rather than isolated threshold tests. Relevant indicators include unusual transaction values, rapid loading and cash-out, abrupt geographic changes, repeated cross-border transfers, beneficiary turnover,

dormant-account reactivation and channel changes. The principle resembles sensor-based fault monitoring, where observations are assessed against expected operating conditions so deviations become meaningful when interpreted collectively rather than as standalone events (Sunday & Omoegun, 2022a).

This architecture requires a transition from reactive review toward predictive surveillance. Reactive systems identify risk only after a loss, complaint or regulatory event, whereas predictive monitoring seeks combinations of weak signals that precede misconduct. For cardholder accounts, historical behaviour can establish rolling baselines for transaction frequency, value, merchant categories, funding sources, countries and withdrawal patterns. Alerts should therefore arise not merely when an absolute limit is crossed, but when current activity departs materially from the customer's established risk-adjusted profile (Sunday et al., 2020).

Real-time monitoring becomes critical where prepaid balances can be loaded, transferred and withdrawn rapidly across jurisdictions. A digital-twin perspective illustrates the value of continuously reconciling observed conditions with an expected system state and updating the model as new data arrive. Applied to payment monitoring, this means maintaining a dynamic representation of the cardholder relationship in which new transactions alter behavioural baselines, cumulative risk scores and escalation priorities, allowing emerging anomalies to be identified before they become entrenched (Shittu et al., 2023).

Indicators should also be calibrated around condition-based deviation rather than arbitrary uniformity. Vibration-monitoring research demonstrates how baseline establishment and signal interpretation permit abnormal conditions to be distinguished from normal variation. In prepaid monitoring, the same logic supports peer-group and self-history comparisons: frequent international spending may be ordinary for one cardholder but anomalous for another. Alert logic should therefore assess magnitude, direction, duration and recurrence of deviation while considering travel, remittance purpose and established commercial activity (Omoegun et al., 2023).

Automation is necessary because payment environments generate more events than investigators can manually review. Automated process-control principles support rule execution, event capture, predefined responses and escalation when operating parameters move outside acceptable ranges. Within enhanced due diligence, rules can identify high-velocity loads, repeated cash withdrawals, prohibited geographies, unusual merchant combinations or rapid pass-through activity, while orchestration logic can aggregate related events into a single case rather than producing disconnected alerts for one behaviour (Sunday & Omoegun, 2022b).

Feature engineering determines whether monitoring systems recognise behavioural context. Credit-card fraud research shows that transaction aggregation and periodic features can improve

detection because current activity gains significance when related to prior transactions. For prepaid platforms, features may include rolling transaction count, load-to-spend ratios, time between funding and withdrawal, beneficiary concentration, cross-border frequency and deviations from normal timing. Well-designed features therefore transform raw transaction streams into interpretable indicators suitable for scoring and prioritisation (Bahnsen et al., 2016).

Temporal sequencing is important because fraudulent behaviour may unfold as a series of individually plausible events whose cumulative order reveals elevated risk. Sequence-based models have demonstrated value in credit-card fraud detection by learning patterns across successive transactions rather than treating each event independently. This supports alert logic that recognises sequences such as dormant account, sudden load, foreign purchase, repeated transfer and rapid cash-out, or multiple small authorisations followed by a larger transaction, strengthening detection without treating every unusual event as suspicious (Jurgovsky et al., 2018).

Alert systems must additionally account for class imbalance, concept drift and verification latency. Fraudulent events are rare relative to legitimate activity, customer habits change, and confirmed labels often become available only after investigation. Real-world fraud-detection research shows that these conditions can distort model performance if systems rely on unrealistic assumptions. Monitoring programmes should therefore emphasise precision, recall, investigator capacity and prioritisation, while recalibrating thresholds as legitimate cardholder behaviour and criminal techniques evolve (Dal Pozzolo et al., 2018).

Combining supervised and unsupervised methods can improve coverage of known and emerging typologies. Supervised models exploit confirmed patterns, whereas unsupervised methods identify unusual observations that may not resemble historical cases. Hybrid approaches are useful for cross-border prepaid activity because new corridors, devices, or transaction structures may initially lack labelled examples. However, anomaly scores should feed structured alert prioritisation rather than automatic determinations of wrongdoing, with investigator review providing validation and feedback for model refinement (Carcillo et al., 2021).

Finally, effective alert logic depends on selecting indicators that add discriminative value while avoiding unnecessary noise. South African research on machine-learning-based card-fraud detection demonstrates the importance of feature selection in improving performance within highly imbalanced transaction data. For enhanced due diligence, the objective should therefore be fewer, richer and more explainable alerts: each case should combine relevant indicators, show the behavioural deviation, identify linked transactions and explain escalation. Confirmed outcomes should then feed back into rule tuning, model validation and cardholder-risk recalibration (Ileberi, Sun & Wang, 2022).

6. Enhanced Due Diligence Investigation Frameworks

Enhanced due diligence (EDD) in prepaid and cross-border payment platforms should operate as a structured investigative process triggered when customer due diligence no longer provides sufficient assurance about identity, transaction purpose, ownership, funding, or geographic exposure. The framework should begin by reconstructing the customer relationship from verified onboarding information, account purpose, and subsequent changes in behaviour. South African analysis demonstrates that effective CDD depends on identification, verification, record keeping, ongoing monitoring and proportionate risk assessment rather than a single onboarding event (Chitimira & Munedzi, 2023).

A rigorous investigation should next test whether the alert is consistent with the known customer profile or represents a material departure requiring escalation. Investigators should validate identity information, examine counterparties, assess transaction purpose and reconcile observable payment behaviour with documentary and contextual evidence. In remote payment environments, distinguishing between collecting identity data, verifying its accuracy and confirming that it belongs to the person controlling the account is important for investigative reliability (Shust & Dostov, 2020).

EDD quality also depends on analyst judgement. Transaction alerts rarely establish misconduct independently; investigators must weigh incomplete evidence, distinguish plausible explanations from unresolved inconsistencies, and document the reasoning supporting escalation or closure. Experimental evidence from Malaysian banking shows that the rigor of customer due diligence and employee expertise materially influence money-laundering risk judgement, reinforcing the need for trained investigators, defined decision criteria and review mechanisms in prepaid cases (Mat-Isa et al., 2021).

Digital payment investigations should additionally connect customer verification with technological evidence. Device changes, authentication records, transaction timing, account linkages and channel usage may clarify whether observed activity is consistent with the verified cardholder or indicates unexplained control by another party. Research on CDD in technology-intensive financial environments emphasizes combining customer verification with technological capability, illustrating why EDD should integrate identity, transaction and system data rather than treating them as separate investigative domains (Johari et al., 2020).

Once evidence is assembled, investigation should move from anomaly description toward causal diagnosis. Root-cause analysis provides a useful discipline for separating immediate symptoms from underlying drivers by testing competing explanations against available evidence. Applied to prepaid monitoring, analysts should determine whether an alert reflects legitimate behavioural change, data-quality problems, account compromise, intermediary activity or unresolved

financial-crime risk. Structured causal analysis reduces premature assumptions and promotes reproducible investigative reasoning across comparable cases (Akanbi, Ganiu & Sunday, 2023a).

Statistical process-control principles further support disciplined EDD by distinguishing ordinary variation from deviations that warrant intervention. Investigative teams can use historical account behaviour, peer-group expectations and transaction distributions to determine whether observed changes are isolated, persistent or cumulative. Unusual activity becomes more significant when repeated deviations move beyond an established behavioural range or occur alongside independent risk indicators, reducing dependence on arbitrary single-event thresholds (Akanbi, Ganiu & Sunday, 2022).

Case handling should also include quality assurance and feedback. Lean Six Sigma principles emphasize reducing process variation, identifying recurring failure points and using measured outcomes to refine operating controls. In an EDD environment, these principles support standardized case templates, peer review, clear evidential requirements, timeliness measures and analysis of false-positive patterns. Feedback from completed cases can then improve alert scenarios, documentation standards and analyst workflows without sacrificing contextual judgement (Olutimehin & Ganiu, 2022).

Finally, EDD should function as an adaptive investigative architecture rather than a static checklist. Technology-enabled process improvement demonstrates how real-time monitoring, advanced analytics and continuous defect detection can be integrated with root-cause identification and corrective action. For payment platforms, a comparable structure links alert generation, investigator assessment, escalation decisions, case outcomes and subsequent recalibration of cardholder risk. This closed-loop design ensures that investigative findings become inputs to future monitoring while preserving auditability, accountability and proportionality (Akanbi, Ganiu & Sunday, 2023b).

7. Regulatory Governance and Cross-Border Compliance

Regulatory governance in prepaid and cross-border payment platforms requires a coordinated architecture aligning due diligence, monitoring, reporting, data governance, and cross-jurisdictional cooperation. Payment activity may be initiated in one country, processed in another, settled through a third jurisdiction, and ultimately benefit a recipient elsewhere. Governance must therefore extend beyond domestic compliance to establish risk ownership across processors, agents, correspondent institutions, and technology providers. International diffusion of anti-money-laundering standards has created substantial convergence, but implementation remains shaped by national institutions, regulatory capacity, and local incentives, making formal harmonisation an incomplete proxy for operational consistency (Sharman, 2008).

A risk-based compliance model is important where prepaid products differ in functionality, transaction limits, customer types, distribution channels, and geographic reach. Rather than applying identical controls to every cardholder, governance frameworks should document how product, customer, jurisdiction, delivery-channel, and transaction risks determine the depth of due diligence and monitoring. Comparative analysis of risk-based AML systems shows that poorly specified risk criteria can create legal and integrity risks when institutions cannot justify different levels of scrutiny (Simonova, 2011). Cross-border governance should therefore connect risk appetite, customer segmentation, escalation thresholds, and EDD requirements through auditable policies.

Nigeria illustrates why regulatory effectiveness depends on more than the existence of rules. Analysis of the global AML regime from a Nigerian institutional perspective highlights gaps between international standards and the practical ability of developing economies to identify and disrupt illicit financial flows. This supports governance arrangements in which compliance obligations are translated into operational models reflecting transaction behaviour, available data, investigative capacity, and local financial realities rather than relying only on formal adoption of international prescriptions (Sotande, 2018).

Distributed payment networks also require explicit internal governance. A supply-chain governance model developed for geographically dispersed retail operations demonstrates the value of accountability structures, standardised controls, information visibility, and continuous oversight across multi-tier networks. Applied to prepaid payment ecosystems, these principles support assigned responsibilities for onboarding, monitoring, sanctions screening, agent oversight, case investigation, regulatory reporting, and remediation across entities involved in service delivery (Akin-Oluyomi & Akhigbe, 2022).

Cross-border compliance additionally depends on leadership capable of connecting operational decisions to enterprise-wide risk objectives. Strategic alignment is essential because compliance failures may emerge when commercial expansion, technology deployment, and third-party relationships proceed faster than control functions adapt. Leadership models integrating data-driven decision support, cross-functional coordination, and adaptive governance provide a useful basis for ensuring that payment growth does not become detached from institutional risk appetite and compliance obligations (Akin-Oluyomi & Akhigbe, 2023).

Regional governance introduces another layer of complexity. SADC experience demonstrates that technological transformation and economic integration require ethical leadership, implementation discipline, institutional cooperation, and policy coherence. These principles are relevant to cross-border payment platforms operating across regulatory environments with different supervisory capacities, data rules, and enforcement practices. Effective compliance therefore requires mechanisms for reconciling jurisdictional differences while preserving

consistent minimum standards for customer identification, monitoring, record retention, escalation, and accountability (Enaifoghe, Dlamini & Agwuna, 2020).

Technology can strengthen this architecture when embedded within governance rather than treated as a substitute for it. Evidence from Bahrain indicates that RegTech-supported transaction monitoring can improve AML effectiveness and reduce compliance time and costs. For prepaid platforms, regulatory technology can support screening, case prioritisation, audit trails, and regulatory reporting across high-volume payment environments, provided models and data flows remain explainable and subject to human oversight (Turki et al., 2020).

Reporting governance is equally important because suspicious transaction reports are a principal channel through which private monitoring informs public enforcement. International experience shows that reporting effectiveness depends not simply on submission volume but on report quality, institutional incentives, information usability, and financial-intelligence capacity. Cross-border platforms should therefore establish escalation standards that produce contextualised reports while avoiding defensive over-reporting that can overwhelm investigative resources (Chaikin, 2009).

Finally, international cooperation should be treated as an operational component of governance rather than a general policy aspiration. Empirical analysis of AML regimes indicates that international cooperation is among the policy dimensions associated with stronger crime-control outcomes, underscoring the importance of timely information exchange and coordinated enforcement. For cardholder monitoring, this means preserving traceable records, consistent risk classifications, explainable alert decisions, and accessible investigative histories so that credible concerns can move efficiently between institutions and competent authorities when activity crosses borders (Ferwerda, 2009).

8. Technology Innovation and Future Research

Technology innovation is reshaping enhanced due diligence by shifting account monitoring from static, rules-based surveillance toward adaptive systems capable of integrating transaction, identity, device, geographic, and behavioural data continuously. For prepaid and cross-border platforms, this transition is important because risks are dispersed across high-volume payment environments. Predictive and prescriptive analytics can help institutions anticipate emerging patterns, prioritise investigative resources and identify operational bottlenecks before they undermine monitoring effectiveness, provided that model outputs remain subject to governance and validation (Akin-Oluyomi & Akhigbe, 2023).

Real-time operational intelligence is important because illicit behaviour may evolve between periodic reviews. Integrating workforce behaviour, service data and live operational indicators demonstrates how heterogeneous data streams can support faster, context-sensitive decisions.

Applied to payment monitoring, this principle supports architectures that combine cardholder profiles with transaction velocity, beneficiary relationships, channel activity and case outcomes, enabling investigators to distinguish isolated anomalies from sustained deviations that justify enhanced due diligence (Akhigbe, Falemi & Akin-Oluyomi, 2023).

Artificial intelligence can strengthen detection by processing complex signal combinations that are difficult to evaluate manually. Research integrating AI with advanced biosensing illustrates the broader analytical value of rapid pattern recognition, sensitivity enhancement and automated classification within high-volume detection environments. In payment platforms, analogous capabilities can support anomaly scoring, typology recognition and prioritisation of accounts whose behaviour departs materially from expected patterns, although financial models require domain-specific validation and regulatory controls (Olorunkosebi et al., 2023).

Technologies supporting identification and traceability are relevant to future monitoring architectures. RFID-based systems demonstrate how automated identification can connect unique identifiers with recorded events while reducing manual processing errors. In prepaid ecosystems, comparable design principles could strengthen linkage across cards, devices, accounts, and authenticated interactions, improving entity resolution and investigative reconstruction where multiple instruments or access points are associated with the same underlying customer (Yusuf et al., 2023).

Future innovation should also connect technology performance with human investigative capacity. Integrated analytics frameworks show the value of combining operational metrics with workforce information and continuous feedback loops. Within EDD, this suggests monitoring not only model accuracy but also alert handling time, investigator workload, escalation consistency, false-positive rates and case outcomes. Such integration would show whether technology improves compliance productivity rather than merely increasing machine-generated alerts (Falemi, Akhigbe & Akin-Oluyomi, 2023).

Machine learning is promising for mobile and cross-border payments because models can evaluate nonlinear relationships among transaction amount, timing, destination, account history, and other attributes. Evidence from mobile-money fraud prediction shows that ensemble approaches can outperform simpler baselines and that transaction characteristics can materially influence predictive performance. Future studies should test models on realistic prepaid datasets, compare performance across jurisdictions, and examine how well algorithms remain reliable when criminal strategies or customer behaviour change over time (Lokanan, 2023).

Innovation must nevertheless remain explainable and rights-sensitive. AI can accelerate AML detection and asset recovery, but opaque systems may create problems for accountability, supervisory review, privacy and procedural fairness. Future research should investigate explainable model architectures, human-in-the-loop decision systems, auditable feature selection

and governance mechanisms that allow institutions to justify why a cardholder was escalated for enhanced review without exposing sensitive security logic or relying on discriminatory proxies (Pavlidis, 2023).

Research should finally recognise that technological controls operate within human behavioural environments. Kenyan evidence on digital-finance scams shows that consumer education alone may not reliably distinguish fraudulent from genuine communications and can sometimes increase over-caution. This finding supports future research combining behavioural evidence with technical monitoring, particularly around social engineering, account takeover and scam-induced transfers. The next generation of EDD systems should therefore evaluate transaction anomalies alongside the interaction between customer behaviour, communication channels and platform-level risk signals (Kubilay et al., 2023).

Conclusion

This review fulfilled its central aim by developing an integrated understanding of how enhanced due diligence can be strengthened across prepaid and cross-border payment environments through risk-based cardholder monitoring. The analysis showed that effective oversight depends on linking customer identity, product characteristics, transaction behaviour, geographic exposure, counterparties, delivery channels, and technological infrastructure within a unified risk architecture. It further demonstrated that financial-crime typologies are most useful when treated as evolving behavioural patterns rather than fixed indicators, enabling monitoring systems to distinguish legitimate variation from activity requiring escalation.

The review also established that cardholder risk profiling should remain dynamic throughout the account lifecycle. Static onboarding classifications are insufficient where transaction velocity, funding sources, jurisdictional exposure, device usage, or beneficiary relationships change materially. Accordingly, monitoring systems should combine behavioural baselines, contextual thresholds, anomaly detection, sequential analysis, and cumulative alert logic to improve precision while limiting unnecessary investigative burden. Enhanced due diligence was shown to be most effective when structured as a closed investigative cycle encompassing alert triage, contextual verification, source-of-funds assessment, relationship mapping, root-cause analysis, documented judgement, escalation, and feedback into future monitoring.

Regulatory governance emerged as equally critical. Cross-border compliance requires consistent internal accountability, jurisdiction-sensitive controls, secure information exchange, explainable reporting, and coordination among institutions and competent authorities. Technological innovation offers significant potential through machine learning, real-time analytics, automated identification, and adaptive risk scoring, but these tools must remain transparent, validated, and subject to human oversight.

The review therefore recommends continuous recalibration of risk models, stronger cross-border data governance, periodic validation of alert scenarios, investment in investigator expertise, and greater use of explainable analytics. Future research should test typology frameworks on realistic multi-jurisdictional datasets and examine how behavioural, technological, and regulatory signals can be integrated without compromising proportionality, privacy, or financial inclusion. These priorities provide a practical foundation for resilient compliance systems.

References

1. Abdallah, A., Maarof, M.A. and Zainal, A. (2016) 'Fraud detection system: A survey', *Journal of Network and Computer Applications*, 68, pp. 90–113. DOI: [10.1016/j.jnca.2016.04.007](https://doi.org/10.1016/j.jnca.2016.04.007)
2. Abdul Rani, M.I., Syed Mustapha Nazri, S.N.F. and Zolkafli, S. (2023) 'A systematic literature review of money mule: Its roles, recruitment and awareness', *Journal of Financial Crime*, 31(2), pp. 347–361. DOI: [10.1108/JFC-10-2022-0243](https://doi.org/10.1108/JFC-10-2022-0243)
3. Agwuna, L., Kaseeram, I. 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. DOI: [10.18639/MERJ.2022.9900060](https://doi.org/10.18639/MERJ.2022.9900060)
4. Agwuna, L.U. (2022) 'Entrepreneurship financial stability and implications', in Eniola, A.A., Iwu, C.G. and Opute, A.P. (eds.) *The Future of Entrepreneurship in Africa: Challenges and Opportunities Post-pandemic*. Abingdon: Routledge, pp. 116–142.
5. Ahmad, A.H., Green, C. and Jiang, F. (2020) 'Mobile money, financial inclusion and development: A review with reference to African experience', *Journal of Economic Surveys*, 34(4), pp. 753–792. <https://doi.org/10.1111/joes.12372>.
6. Ajayi, K. and Abdulkareem, H. (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](https://doi.org/10.1108/13685201011010191)
7. Akanbi, O., Ganiu, O.S. and Sunday, E.A. (2022) 'Comprehensive review of statistical process control (SPC) for precision weight management in global food manufacturing', *Gyanshauryam: International Scientific Refereed Research Journal*, 5(3), pp. 433–461.
8. Akanbi, O., Ganiu, O.S. and Sunday, E.A. (2023a) 'A review of industrial equipment restoration strategies: Integrating design of experiments (DOE) and root-cause analysis', *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 9(10), pp. 444–462.
9. Akanbi, O., Ganiu, O.S. and Sunday, E.A. (2023b) 'Technological advances in Lean Six Sigma methodologies for reducing process failures in high-speed packaging lines', *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 9(10), pp. 463–492.

10. Akanfe, O., Valecha, R. and Rao, H.R. (2020) ‘Assessing country-level privacy risk for digital payment systems’, *Computers & Security*, 99, Article 102065. DOI: [10.1016/j.cose.2020.102065](https://doi.org/10.1016/j.cose.2020.102065)
11. 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](https://doi.org/10.54660/IJMRGE.2023.4.6.1322-1338)
12. 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](https://doi.org/10.54660/IJMRGE.2022.3.6.860-878)
13. Akin-Oluyomi, O.T. and Akhigbe, R. (2023) ‘A conceptual supply chain leadership model for aligning logistics decisions with enterprise strategy’, *International Journal of Advanced Multidisciplinary Research and Studies*, 3(1), pp. 1725–1744. DOI: [10.62225/2583049X.2023.3.1.5340](https://doi.org/10.62225/2583049X.2023.3.1.5340)
14. Akin-Oluyomi, O.T. and Akhigbe, R. (2023) ‘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](https://doi.org/10.62225/2583049X.2023.3.1.5338)
15. 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](https://doi.org/10.1108/JMLC-03-2018-0023)
16. Amrani, H. and Ali, M. (2022) ‘A new criminal jurisdiction to combat cross-border money laundering’, *Journal of Money Laundering Control*, 25(3), pp. 540–550. DOI: [10.1108/JMLC-06-2021-0059](https://doi.org/10.1108/JMLC-06-2021-0059)
17. Arner, D.W., Zetsche, D.A., Buckley, R.P. and Barberis, J.N. (2019) ‘The identity challenge in finance: From analogue identity to digitized identification to digital KYC utilities’, *European Business Organization Law Review*, 20(1), pp. 55–80. DOI: [10.1007/s40804-019-00135-1](https://doi.org/10.1007/s40804-019-00135-1)
18. Bahnsen, A.C., Aouada, D., Stojanovic, A. and Ottersten, B. (2016) ‘Feature engineering strategies for credit card fraud detection’, *Expert Systems with Applications*, 51, pp. 134–142. DOI: [10.1016/j.eswa.2015.12.030](https://doi.org/10.1016/j.eswa.2015.12.030)
19. Balogun, C.T. and Sabboh, 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. Beebeejaun, A. and Dulloo, L. (2023) ‘A critical analysis of the anti-money laundering legal and regulatory framework of Mauritius: A comparative study with South Africa’,

- Journal of Money Laundering Control, 26(2), pp. 401–417. DOI: [10.1108/JMLC-12-2021-0141](https://doi.org/10.1108/JMLC-12-2021-0141)
21. Canhoto, A.I. (2021) ‘Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective’, *Journal of Business Research*, 131, pp. 441–452. DOI: [10.1016/j.jbusres.2020.10.012](https://doi.org/10.1016/j.jbusres.2020.10.012)
 22. Carcillo, F., Le Borgne, Y.-A., Caelen, O., Kessaci, Y., Oblé, F. and Bontempi, G. (2021) ‘Combining unsupervised and supervised learning in credit card fraud detection’, *Information Sciences*, 557, pp. 317–331. DOI: [10.1016/j.ins.2019.05.042](https://doi.org/10.1016/j.ins.2019.05.042).
 23. Chaikin, D. (2009) ‘How effective are suspicious transaction reporting systems?’, *Journal of Money Laundering Control*, 12(3), pp. 238–253. DOI: [10.1108/13685200910973628](https://doi.org/10.1108/13685200910973628)
 24. Chen, T.-H. (2020) ‘Do you know your customer? Bank risk assessment based on machine learning’, *Applied Soft Computing*, 86, Article 105779. DOI: [10.1016/j.asoc.2019.105779](https://doi.org/10.1016/j.asoc.2019.105779)
 25. Cheng, D., Xiang, S., Shang, C., Zhang, Y., Yang, F. and Zhang, L. (2020) ‘Spatio-temporal attention-based neural network for credit card fraud detection’, *Proceedings of the AAAI Conference on Artificial Intelligence*, 34(1), pp. 362–369. DOI: [10.1609/aaai.v34i01.5371](https://doi.org/10.1609/aaai.v34i01.5371)
 26. Chitimira, H. and Munedzi, S. (2023) ‘Historical aspects of customer due diligence and related anti-money laundering measures in South Africa’, *Journal of Money Laundering Control*, 26(7), pp. 138–154. DOI: [10.1108/JMLC-01-2023-0016](https://doi.org/10.1108/JMLC-01-2023-0016)
 27. Choo, K.K.R. (2009) ‘Money laundering and terrorism financing risks of prepaid card instruments?’, *Asian Journal of Criminology*, 4(1), pp. 11–30. DOI: [10.1007/s11417-008-9051-6](https://doi.org/10.1007/s11417-008-9051-6)
 28. Couchoro, M.K., Sodokin, K. and Koriko, M. (2021) ‘Information and communication technologies, artificial intelligence, and the fight against money laundering in Africa’, *Strategic Change*, 30(3), pp. 281–291. DOI: [10.1002/jsc.2410](https://doi.org/10.1002/jsc.2410)
 29. Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C. and Bontempi, G. (2018) ‘Credit card fraud detection: A realistic modeling and a novel learning strategy’, *IEEE Transactions on Neural Networks and Learning Systems*, 29(8), pp. 3784–3797. DOI: [10.1109/TNNLS.2017.2736643](https://doi.org/10.1109/TNNLS.2017.2736643).
 30. David-West, O., Iheanachor, N. and Umukoro, I. (2020) ‘Sustainable business models for the creation of mobile financial services in Nigeria’, *Journal of Innovation & Knowledge*, 5(2), pp. 105–116. <https://doi.org/10.1016/j.jik.2019.03.001>.
 31. de Koker, L. and Jentzsch, N. (2013) ‘Financial inclusion and financial integrity: Aligned incentives?’, *World Development*, 44, pp. 267–280. <https://doi.org/10.1016/j.worlddev.2012.11.002>.
 32. Djurisic, V., Kascelan, L., Rogic, S. and Melovic, B. (2020) ‘Bank CRM optimization using predictive classification based on the support vector machine method’, *Applied Artificial Intelligence*, 34(12), pp. 941–955. DOI: [10.1080/08839514.2020.1790248](https://doi.org/10.1080/08839514.2020.1790248)

33. Dornadula, V.N. and Geetha, S. (2019) 'Credit card fraud detection using machine learning algorithms', *Procedia Computer Science*, 165, pp. 631–641. DOI: [10.1016/j.procs.2020.01.057](https://doi.org/10.1016/j.procs.2020.01.057)
34. Dumitrescu, B., Băltoiu, A. and Budulan, Ș. (2022) 'Anomaly detection in graphs of bank transactions for anti-money laundering applications', *IEEE Access*, 10, pp. 47699–47714. DOI: [10.1109/ACCESS.2022.3170467](https://doi.org/10.1109/ACCESS.2022.3170467)
35. 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/jebis.v12i6\(J\).3102](https://doi.org/10.22610/jebis.v12i6(J).3102)
36. Esoimeme, E.E. (2018) 'A comparative analysis of the prepaid card laws/regulations in Nigeria, the UK, the USA and India', *Journal of Money Laundering Control*, 21(4), pp. 481–493. DOI: [10.1108/JMLC-03-2017-0010](https://doi.org/10.1108/JMLC-03-2017-0010)
37. Esoimeme, E.E. (2020) 'Identifying and reducing the money laundering risks posed by individuals who have been unknowingly recruited as money mules', *Journal of Money Laundering Control*, 24(1), pp. 201–212. DOI: [10.1108/JMLC-05-2020-0053](https://doi.org/10.1108/JMLC-05-2020-0053)
38. Ezeani, P.T. and Sabboh, G.M. (2021) 'Psychosocial predictors of the changing role of husbands as breadwinners in a depressed economy in Ibadan Metropolis, Oyo State, Nigeria', *British Journal of Education, Learning and Development Psychology*, 4(2), pp. 31–42. DOI: [10.52589/BJELDP-ZU3KSUJU](https://doi.org/10.52589/BJELDP-ZU3KSUJU)
39. 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](https://doi.org/10.62225/2583049X.2023.3.1.5339)
40. Ferwerda, J. (2009) 'The economics of crime and money laundering: Does anti-money laundering policy reduce crime?', *Review of Law & Economics*, 5(2), pp. 903–929. DOI: [10.2202/1555-5879.1421](https://doi.org/10.2202/1555-5879.1421)
41. 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](https://doi.org/10.1108/JMLC-06-2023-0103)
42. 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, Article 15. DOI: [10.1140/epjds/s13688-022-00328-8](https://doi.org/10.1140/epjds/s13688-022-00328-8)
43. Hayashi, F. and Cuddy, E. (2014) 'General purpose reloadable prepaid cards: Penetration, use, fees, and fraud risks', *Federal Reserve Bank of Kansas City Research Working Paper*, RWP 14-01. <https://doi.org/10.2139/ssrn.2398607>.
44. Henning, J. and Hauman, M. (2017) 'Fortifying a risk-based approach in the South African AML/CFT process', *Journal of Financial Crime*, 24(4), pp. 520–528. DOI: [10.1108/JFC-01-2017-0007](https://doi.org/10.1108/JFC-01-2017-0007)

45. Ileberi, E., Sun, Y. and Wang, Z. (2022) 'A machine learning-based credit card fraud detection using the GA algorithm for feature selection', *Journal of Big Data*, 9, Article 24. DOI: [10.1186/s40537-022-00573-8](https://doi.org/10.1186/s40537-022-00573-8).
46. Jensen, R.I.T. and Iosifidis, A. (2023) 'Fighting money laundering with statistics and machine learning', *IEEE Access*, 11, pp. 8889–8903. DOI: [10.1109/ACCESS.2023.3239549](https://doi.org/10.1109/ACCESS.2023.3239549)
47. Johari, R.J., Zul, N.B., Talib, N. and Sayed Hussin, S.A.H. (2020) 'Money laundering: Customer due diligence in the era of cryptocurrencies', in *Proceedings of the 1st International Conference on Accounting, Management and Entrepreneurship (ICAMER 2019)*, *Advances in Economics, Business and Management Research*, pp. 130–135. DOI: [10.2991/aebmr.k.200305.033](https://doi.org/10.2991/aebmr.k.200305.033)
48. Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P.-E., He-Guelton, L. and Caelen, O. (2018) 'Sequence classification for credit-card fraud detection', *Expert Systems with Applications*, 100, pp. 234–245. DOI: [10.1016/j.eswa.2018.01.037](https://doi.org/10.1016/j.eswa.2018.01.037).
49. Kovács, T., Ko, A. and Asemi, A. (2021) 'Exploration of the investment patterns of potential retail banking customers using two-stage cluster analysis', *Journal of Big Data*, 8, Article 141. DOI: [10.1186/s40537-021-00529-4](https://doi.org/10.1186/s40537-021-00529-4)
50. Kubilay, E., Raiber, E., Spantig, L., Cahliková, J. and Kaaria, L. (2023) 'Can you spot a scam? Measuring and improving scam identification ability', *Journal of Development Economics*, 165, Article 103147. DOI: [10.1016/j.jdeveco.2023.103147](https://doi.org/10.1016/j.jdeveco.2023.103147)
51. Lee, C.-C., Chen, P.-F. and Chu, P.-J. (2023) 'Green recovery through financial inclusion of mobile payment: A study of low- and middle-income Asian countries', *Economic Analysis and Policy*, 77, pp. 729–747. <https://doi.org/10.1016/j.eap.2022.12.012>.
52. Linn, C.J. (2008) 'Regulating the cross-border movement of prepaid cards', *Journal of Money Laundering Control*, 11(2), pp. 146–171. DOI: [10.1108/13685200810867474](https://doi.org/10.1108/13685200810867474)
53. Lokanan, M.E. (2023) 'Predicting mobile money transaction fraud using machine learning algorithms', *Applied AI Letters*, 4(2), Article e85. DOI: [10.1002/ail.2.85](https://doi.org/10.1002/ail.2.85)
54. Lozano-Medina, J.I., Hervert-Escobar, L. and Hernandez-Gress, N. (2020) 'Risk profiles of financial service portfolio for women segment using machine learning algorithms', in Krzhizhanovskaya, V.V. et al. (eds.) *Computational Science – ICCS 2020. Lecture Notes in Computer Science*, 12143, pp. 561–574. Cham: Springer. DOI: [10.1007/978-3-030-50436-6_42](https://doi.org/10.1007/978-3-030-50436-6_42)
55. Mat-Isa, Y., Mohd-Sanusi, Z., Sabri, S.-S. and Barnes, P.A. (2021) 'Money laundering risk judgement and decision-making: Influences of customer due diligence process and bank employees' expertise', *International Journal of Economics and Business Research*, 22(1), pp. 1–20. DOI: [10.1504/IJEER.2021.116299](https://doi.org/10.1504/IJEER.2021.116299)
56. Mohammed, H.N., Malami, N.S., Thomas, S., Aiyelabegan, F.A., Imam, F.A. and Ginsau, H.H. (2022) 'Machine learning approach to anti-money laundering: A review', in 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for

- Sustainable Development (NIGERCON), Lagos, Nigeria, pp. 1–5. DOI: [10.1109/NIGERCON54645.2022.9803072](https://doi.org/10.1109/NIGERCON54645.2022.9803072)
57. Mothobi, O. and Grzybowski, L. (2017) ‘Infrastructure deficiencies and adoption of mobile money in Sub-Saharan Africa’, *Information Economics and Policy*, 40, pp. 71–79. <https://doi.org/10.1016/j.infoecopol.2017.05.003>.
58. 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](https://doi.org/10.1016/j.jbusres.2023.113820)
59. Olorunkosebi, M.T., Ayinde, M.K., Mensah, G.K. and Penddah, A.L. (2023) ‘Integrating artificial intelligence and advanced biosensors for rapid and sensitive detection of antimicrobial-resistant foodborne pathogens’, *Journal of Advances in Microbiology Research*, 4(2), pp. 175–182. DOI: [10.22271/micro.2023.v4.i2b.293](https://doi.org/10.22271/micro.2023.v4.i2b.293)
60. Olutimehin, A.O. and Ganiu, O.S. (2022) ‘Integrating Lean Six Sigma with reliability-centered maintenance: A unified framework for manufacturing excellence’, *International Journal of Multidisciplinary Research and Growth Evaluation*, 3(6), pp. 983–996. DOI: [10.54660/IJMRGE.2022.3.6.983-996](https://doi.org/10.54660/IJMRGE.2022.3.6.983-996)
61. Omoegun, G.O., Sunday, E.A., Essien, M.A. and Oluokun, O.A. (2023) ‘Vibration-based condition monitoring of rotating machinery using LabVIEW’, *International Journal of Scientific Research in Civil Engineering*, 7(6), pp. 82–108. DOI: [10.32628/IJSRCE237529](https://doi.org/10.32628/IJSRCE237529).
62. Pavlidis, G. (2023) ‘Deploying artificial intelligence for anti-money laundering and asset recovery: The dawn of a new era’, *Journal of Money Laundering Control*, 26(7), pp. 155–166. DOI: [10.1108/JMLC-03-2023-0050](https://doi.org/10.1108/JMLC-03-2023-0050)
63. Reite, E.J., Oust, A., Bang, R.M. and Maurstad, S. (2023) ‘Changes in credit score, transaction volume, customer characteristics, and the probability of detecting suspicious transactions’, *Journal of Money Laundering Control*, 26(6), pp. 1165–1178. DOI: [10.1108/JMLC-06-2022-0087](https://doi.org/10.1108/JMLC-06-2022-0087)
64. Rella, L. (2019) ‘Blockchain technologies and remittances: From financial inclusion to correspondent banking’, *Frontiers in Blockchain*, 2, Article 14. DOI: [10.3389/fbloc.2019.00014](https://doi.org/10.3389/fbloc.2019.00014)
65. Rodima-Taylor, D. and Grimes, W.W. (2019) ‘International remittance rails as infrastructures: Embeddedness, innovation and financial access in developing economies’, *Review of International Political Economy*, 26(5), pp. 839–862. DOI: [10.1080/09692290.2019.1607766](https://doi.org/10.1080/09692290.2019.1607766)
66. Sabboh, 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.
67. Sabboh, G.M. (2022) Development and validation of the revised self-esteem scale for Nigerian adolescents and youths. Master’s thesis. Moscow, Russia: National Research University Higher School of Economics.

68. Sabboh, 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](https://doi.org/10.37745/bjmas.2022.0261)
69. Sharman, J.C. (2008) ‘Power and discourse in policy diffusion: Anti-money laundering in developing states’, *International Studies Quarterly*, 52(3), pp. 635–656. DOI: [10.1111/j.1468-2478.2008.00518.x](https://doi.org/10.1111/j.1468-2478.2008.00518.x)
70. Shittu, H. and Nabil, M. (2023) ‘Smart supply chain management with attribute-based encryption access control’, in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 198–204. DOI: [10.1109/CCWC57344.2023.10099268](https://doi.org/10.1109/CCWC57344.2023.10099268)
71. Shittu, H.A., Shittu, M.A., Adeleke, O.J. and Adedokun, O.J. (2021) ‘Blockchain-based energy trading models for peer-to-peer renewable microgrids’, *International Journal of Research in Electrical and Electronics Engineering*, 4(3), pp. 1–19. DOI: [10.34218/IJREEE_04_03_001](https://doi.org/10.34218/IJREEE_04_03_001)
72. 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](https://doi.org/10.64388/IREV6I3-1714041)
73. Shittu, M.A., Shittu, H.A., 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](https://doi.org/10.34218/IJIERD_14_02_003).
74. Shust, P.M. and Dostov, V. (2020) ‘Implementing innovative customer due diligence: Proposal for universal model’, *Journal of Money Laundering Control*, 23(4), pp. 871–884. DOI: [10.1108/JMLC-01-2020-0007](https://doi.org/10.1108/JMLC-01-2020-0007)
75. Simonova, A. (2011) ‘The risk-based approach to anti-money laundering: Problems and solutions’, *Journal of Money Laundering Control*, 14(4), pp. 346–358. DOI: [10.1108/13685201111173820](https://doi.org/10.1108/13685201111173820)
76. 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](https://doi.org/10.1108/JMLC-11-2017-0066)
77. Sunday, E.A. and Omoegun, G.O. (2022a) ‘Smart fault detection in HVAC systems using sensor-based monitoring’, *International Journal of Scientific Research in Science, Engineering and Technology*, 7(4), pp. 380–403.
78. Sunday, E.A. and Omoegun, G.O. (2022b) ‘Automation of process control systems using Siemens TIA Portal: A case study approach’, *International Journal of Scientific Research in Mechanical and Materials Engineering*, 6(5), pp. 30–55.
79. Sunday, E.A., Omoegun, G.O., Essien, M.A. and Oluokun, O.A. (2020) ‘Transitioning from reactive to predictive maintenance in mechanical systems’, *International Journal of*

- Scientific Research in Computer Science, Engineering and Information Technology, 6(6), pp. 425–447.
80. Suri, T. and Jack, W. (2016) ‘The long-run poverty and gender impacts of mobile money’, *Science*, 354(6317), pp. 1288–1292. <https://doi.org/10.1126/science.aah5309>.
81. Toh, Y.L. (2021) ‘Prepaid cards: An inadequate solution for digital payments inclusion’, *Economic Review*, 106(4). <https://doi.org/10.18651/ER/v106n4Toh>.
82. Turki, M., Hamdan, A., Cummings, R.T., Sarea, A., Karolak, M. and Anasweh, M. (2020) ‘The regulatory technology “RegTech” and money laundering prevention in Islamic and conventional banking industry’, *Heliyon*, 6(10), Article e04949. DOI: [10.1016/j.heliyon.2020.e04949](https://doi.org/10.1016/j.heliyon.2020.e04949)
83. Vlcek, W. (2011) ‘Global anti-money laundering standards and developing economies: The regulation of mobile money’, *Development Policy Review*, 29(4), pp. 415–431. DOI: [10.1111/j.1467-7679.2011.00540.x](https://doi.org/10.1111/j.1467-7679.2011.00540.x)
84. Wanjohi, P.M. (2017) ‘Curbing mobile phone terrorism and financial fraud: A Kenyan perspective’, *Journal of ICT Standardization*, 4(3), pp. 237–246. DOI: [10.13052/jicts2245-800X.434](https://doi.org/10.13052/jicts2245-800X.434)
85. Whisker, J. and Lokanan, M.E. (2019) ‘Anti-money laundering and counter-terrorist financing threats posed by mobile money’, *Journal of Money Laundering Control*, 22(1), pp. 158–172. DOI: [10.1108/JMLC-10-2017-0061](https://doi.org/10.1108/JMLC-10-2017-0061)
86. Yeşilkanat, A., Bayram, B., Koroğlu, B. and Arslan, S. (2020) ‘An adaptive approach on credit card fraud detection using transaction aggregation and word embeddings’, in Maglogiannis, I., Iliadis, L. and Pimenidis, E. (eds.) *Artificial Intelligence Applications and Innovations. IFIP Advances in Information and Communication Technology*, 583, pp. 3–14. Cham: Springer. DOI: [10.1007/978-3-030-49161-1_1](https://doi.org/10.1007/978-3-030-49161-1_1)
87. Yusuf, M., Akintunde, A., Habeeb, S. and Quadri, A. (2023) ‘Radio Frequency Identification (RFID) based library management system’, *International Journal of Technology and Systems*, 8(2), pp. 21–35. DOI: [10.47604/ijts.2041](https://doi.org/10.47604/ijts.2041)