DOI: 10.55643/fcaptp.3.68.2026.5248

REGULATORY WHITELIST MECHANISMS IN FINANCIAL MONITORING AND STATE FINANCIAL SECURITY

Zhanna Dryha
D.Sc. in Economics, Professor, Department of National Security, Public Administration and Administration, Zhytomyr Polytechnic State University, Zhytomyr, Ukraine;
ORCID: 0000-0002-1844-5329

Viktor Trynchuk
PhD in Economics, Professor, Head of the Department of Finance, Accounting and Banking, Luhansk Taras Shevchenko National University, Lubny, Ukraine;
ORCID: 0000-0001-7435-0159

Oleksandr Levchenko
PhD in Economics, Member, Ukrainian Professional Public Organization «The Auditors' Union of Ukraine», Kyiv, Ukraine;
e-mail: oleksandr.levchenko@gmail.com
ORCID: 0009-0006-2798-8583
(Corresponding author)

Olena Sereda
PhD in Economics, Associate Professor of the Department of Finance, Kyiv National University of Technologies and Design, Kyiv, Ukraine;
ORCID: 0000-0003-0547-2077

Liubomyr Kochubei
Head, Association of IT Lawyers, Kyiv, Ukraine;
ORCID: 0009-0009-0707-7901

Oleksiy Domashenko
CEO, International Investments & Consulting LLC, Miami, United States;
ORCID: 0009-0005-9187-3759

Received: 11/05/2026
Accepted: 20/06/2026
Published: 30/06/2026

ABSTRACT

This article develops a regulatory model for implementing whitelist mechanisms in financial monitoring as an instrument of state financial security under conditions of digitalization and algorithmic transaction control. The study focuses on false-positive blocking of legitimate and legally mandatory transactions, especially public-law payments whose recipient, purpose, and legal basis can be verified through authoritative data. The methodology combines systemic, comparative, structural-functional, institutional, and conceptual modelling approaches. The article defines false-positive blocking as an automated or semi-automated high-risk classification or suspension of a financial transaction that is subsequently confirmed as legitimate on the basis of its legal nature, verified recipient status, payment purpose, customer due diligence data, or post-audit review. The study identifies the principal mechanism of such errors as a mismatch between behavioral risk indicators and the legal classification of transactions. It argues that large amounts, unusual frequency, atypical geography, new recipients, or customer-profile mismatches are not causes of illegitimacy in themselves, but risk indicators that may generate false-positive decisions when legal-context validation is absent. Based on this mechanism, the article proposes a three-level regulatory model consisting of institutional, informational, and algorithmic components: a centralized registry of verified public-law payment recipients, dual validation of risk and legal classification, real-time pre-blocking validation, low-risk eligibility testing, audit logging, human-in-the-loop review, and post-audit safeguards. The whitelist mechanism is not treated as an exemption from AML/CFT monitoring; rather, it functions as a validated processing regime for transactions that meet independent eligibility criteria and contain no critical risk flags. The proposed model is designed to reduce unjustified automatic blocking, preserve the continuity of state financial flows, and strengthen the explainability, proportionality, and accountability of algorithmic financial monitoring.

Keywords: financial monitoring, financial security, artificial intelligence, whitelist mechanism, public-law payments, false-positive blocking, risk-based approach, AML/CFT, RegTech

JEL Classification: G18, G28, H26, K22, K42

INTRODUCTION

In the current context of the globalization of financial markets and the rapid development of the digital economy, ensuring the financial security of the state has become a key priority of national policy. A decisive role in this process is played by the international system for combating money laundering, the financing of terrorism, and the proliferation of weapons of mass destruction, formed in accordance with the standards of the Financial Action Task Force. The central element of this system is the Risk-Based Approach (RBA), which provides for the concentration of financial institutions' resources on the most vulnerable segments of the financial system.

However, the implementation of the risk-based approach under contemporary conditions is impossible without taking into account fundamental changes in the very nature of financial infrastructure, which is increasingly acquiring a digital and algorithmic character. Transaction processing, risk management, and regulatory control processes are

being integrated into a unified algorithmic environment that enables automated decision-making in real time. This evolution changes the paradigm of financial monitoring from retrospective control to preventive, technologically mediated intervention.

At the same time, the algorithmization of financial monitoring gives rise to new types of systemic risks associated not so much with unlawful financial transactions as with the limitations of the models used to analyze them. The universalization of transaction assessment criteria often neutralizes their functional and legal purpose, which may lead to distortions in financial flows. This problem becomes particularly significant in the field of transactions related to the fulfillment of public-law obligations, which are critically important for the stability of public finances. This necessitates the development of new regulatory instruments capable of combining algorithmic risk assessment with consideration of the legal nature of transactions. These risks do not remain merely a theoretical construct; they have concrete manifestations in the actual practice of financial monitoring, which today demonstrates a number of systemic dysfunctions.

The central problem addressed in this article is not the mere presence of high-risk indicators in financial transactions. A large amount, unusual frequency, new recipient account, atypical geography, or mismatch with a customer profile should be understood primarily as risk indicators rather than as direct causes of false-positive blocking. False-positive blocking arises when an algorithm interprets such indicators without an additional legal-context layer capable of identifying the legal nature of the transaction. In the case of public-law and legally mandatory payments, the cause of a false-positive decision is therefore the mismatch between behavioral risk scoring and the legal classification of the payment.

The practical implementation of international financial monitoring standards, both in Ukraine and globally, has revealed a number of dysfunctions, among which the phenomena of de-risking and over-compliance are key. Seeking to minimize regulatory sanctions, financial institutions apply uniformly strict verification procedures to a broad range of clients. The consequences include the blocking of accounts of legitimate businesses, delays in transaction processing, increased transaction costs, and an overall slowdown in economic activity.

Thus, the paradoxical consequence of the excessively uniform application of strict procedures is that an instrument intended to protect the financial system begins to harm it by creating incentives for the shadowing of the economy. Financial monitoring, which is designed to ensure the transparency and stability of the financial system, in some cases transforms into a factor that restrains the development of bona fide entrepreneurship and stimulates the transfer of part of economic activity into the shadow sector. This highlights the need to establish differentiated mechanisms of regulatory influence that would make it possible to clearly distinguish between clients' risk levels and, accordingly, adapt the intensity of control procedures.

The proposed response to this problem is a regulatory whitelist mechanism aimed not at exempting entire categories of clients from financial monitoring, but at enabling the positive identification of a narrowly defined class of transactions whose legal nature can be verified in advance. In this study, the relevant class consists primarily of public-law and legally mandatory payments, where the recipient, payment purpose, and legal basis may be checked against authoritative regulatory data. Therefore, the whitelist is conceptualized as a validation mechanism rather than as a privilege, an AML/CFT exemption, or a substitute for transaction monitoring.

The novelty of this approach lies in combining behavioral risk scoring with legal classification and auditability. A transaction may be redirected from automatic blocking to priority validation only after independent eligibility criteria have been satisfied and only in the absence of sanctions, terrorist-financing, fraud, account-compromise, or other critical risk indicators. This makes it possible to preserve AML/CFT control while reducing the probability of unjustified interruption of legitimate public-law payments.

LITERATURE REVIEW

Contemporary studies of financial monitoring are based on a combination of statistical and algorithmic approaches to the detection of financial offenses. The classical works of Bolton and Hand (2002), as well as Bhattacharyya et al. (2011) and Ngai et al. (2011), formed the methodological foundation for the application of data mining and machine learning in the financial sector, while the works of Arner et al. (2015) emphasize the transformation of financial regulation under the influence of digitalization and the need to adapt regulatory models to new risks. Developing this approach, Arner et al. (2017) stress that the digitization of analog processes is insufficient in the digital financial world, and that the true potential of RegTech lies in the creation of a proportional real-time regulatory regime, which requires a rethinking of financial

DOI: 10.55643/fcaptp.3.68.2026.5248

regulation at the intersection of data, digital identity, and regulatory mechanisms. Traditional rule-based transaction monitoring systems in the field of anti-money laundering (AML) are characterized by a high level of false-positive alerts and insufficient flexibility in detecting new and complex risks (Kungu et al., 2026).

Compliance-oriented literature similarly emphasizes that algorithmic AML/CFT systems often evaluate transactions on the basis of predefined variables, such as jurisdiction, customer category, industry, transaction pattern, or politically exposed person status, while insufficiently accounting for the legal and economic context of the transaction. As Travis (2026) notes, algorithms may support transaction screening and sanctions compliance, but they cannot replace human judgment in matters requiring contextual assessment. This is particularly relevant for false-positive alerts, where the formal presence of a risk indicator does not necessarily mean that the transaction is unlawful or suspicious.

As shown by Jullum et al. (2020), the inclusion in the training sample not only of confirmed suspicious transactions but also of transactions that were reviewed but not recognized as risky, as well as ordinary unreviewed transactions, makes it possible to significantly improve prediction quality and reduce the number of false-positive alerts in financial monitoring systems. This approach demonstrates the need to take into account a broader behavioral and economic context when constructing risk assessment algorithms, especially under conditions of digital transformation of the financial environment. These changes are specifically highlighted by Glonti et al. (2024), who studied the transformation of enterprise business models under the influence of COVID-19 and Industry 4.0, accompanied by the digitalization of logistics, trade, and document flow, the automation of processes, and changes in customer segments; accordingly, these factors should be considered when developing modern regulatory mechanisms, including "whitelists" in financial monitoring. Despite the active development of digital technologies and AI-based solutions in the field of AML/CFT, scholarly discourse is predominantly focused on improving mechanisms for detecting risky operations and suspicious transactions.

Transaction-monitoring literature identifies a number of recurring risk indicators used by automated AML/CFT systems. These include atypical geographic parameters, inconsistency between the customer profile and the nature of the transaction, structuring or smurfing patterns, transactions involving new or non-standard financial instruments, unusual time-related characteristics, ambiguity of payment purpose, and interaction with accounts or counterparties associated with elevated risk (Columbia SIPA / School of International and Public Affairs, Columbia University, 2026; Gilson, 2024). However, these elements should be understood as risk indicators rather than as sufficient causes of illegality. A false-positive decision may arise when such indicators are treated as grounds for blocking without additional verification of the transaction's legal nature, payment purpose, and recipient status. Their use is connected with the risk-based logic of AML/CFT regulation, under which financial institutions are required to identify, assess, and monitor suspicious or unusual transaction patterns.

At the same time, it should be noted that most of these studies focus on identifying "blacklists" of suspicious transactions, leaving aside the potential of positive identification of bona fide clients — so-called "whitelists." However, the application of these methods is impossible without taking into account the institutional environment in which financial intermediaries operate. As Stulz (2019) notes, banks function in an environment of strict regulatory supervision, which is caused by their systemic role and vulnerability, in particular due to the need to prevent money laundering and comply with financial monitoring requirements. Yet such regulatory asymmetry creates preconditions for the emergence of alternative financial intermediaries and stimulates the development of new instruments for risk control. It is precisely among such instruments that mechanisms of selective access to financial services — "whitelists" — may be considered an important element in ensuring the financial security of the state. A critical issue remains the determination of objective criteria for assigning a client to a "whitelist" without violating the principle of equal access.

RegTech-oriented literature also discusses whitelisting, deduplication, and secondary transaction assessment as instruments for reducing excessive false-positive alerts in AML/CFT compliance systems. Cummings (2024) emphasizes that false-positive alerts overload compliance departments and may reduce the effectiveness of financial monitoring. In this context, whitelisting should not be understood as the removal of transactions from control, but as one element of a broader validation architecture that includes secondary review, auditability, and continuous monitoring.

The described regulatory asymmetry at the national level is largely adjusted by international standards, which establish a universal framework for constructing financial monitoring systems. At the international level, a key role is played by the standards of the Financial Action Task Force, which define the conceptual foundations for combating money laundering, terrorist financing, and the proliferation of weapons of mass destruction. According to the updated FATF Recommendations, an effective financial monitoring system should be based on a risk-based approach, which provides for the differentiation of customer due diligence measures depending on the level of risk, as well as the possibility of applying simplified procedures in low-risk cases (FATF, 2023). Such an approach is aimed at improving the efficiency of resource use by primary financial monitoring entities and reducing excessive regulatory burden without losing control over risky operations.

In this context, "whitelist" mechanisms may be viewed as an instrument for implementing FATF principles, enabling the identification of low-risk clients and the optimization of procedures for servicing them, while simultaneously strengthening the focus of control on suspicious transactions. Thus, the integration of FATF approaches into national regulatory models, in particular through the use of selective mechanisms of access to financial services, contributes to increasing the transparency of the financial system and strengthening the financial security of the state.

The logic of differentiated financial monitoring is also reflected in regulatory guidance that emphasizes customer-centered and risk-based transaction assessment. For low-risk entities or transactions, reduced intensity of control may be appropriate only where this does not weaken ongoing monitoring, suspicious transaction reporting, sanctions screening, or customer due diligence obligations. In this sense, whitelist-based mechanisms may be viewed as a form of justified differentiation within the risk-based approach, provided that they remain subject to continuous monitoring, periodic review, and audit safeguards (Central Bank of the United Arab Emirates, 2022).

Levytska et al. (2022) examined the specific features of implementing the risk-based approach in the internal audit system of financial monitoring entities in Ukraine. The authors determined that an effective internal control system should be based on the identification, assessment, and minimization of money laundering risks, as well as on the continuous monitoring of counterparties — clients, suppliers, and buyers — depending on their risk profile.

The implementation of the FATF risk-based approach into national legislation takes specific institutional forms. An important element of the national financial monitoring system is the legislative framework established by the Law of Ukraine "On Prevention and Counteraction to Legalization (Laundering) of Proceeds from Crime, Terrorist Financing, and Financing of Proliferation of Weapons of Mass Destruction." This law forms the institutional and organizational foundations for the functioning of the system for countering financial crimes, defining the obligations of primary financial monitoring entities regarding client identification, risk assessment, customer due diligence, and reporting of suspicious financial transactions. The key principle embedded in the law is the risk-based approach, which provides for the differentiation of control measures depending on the risk level of the client or transaction (Law of Ukraine, 2020). In this context, the implementation of "whitelist" mechanisms may be regarded as an instrument for the practical realization of this approach, allowing financial monitoring procedures to be optimized for low-risk clients. It should be noted, however, that current legislation does not contain a legal definition of a "whitelist," which complicates its direct application and requires the development of a separate regulatory model.

The development of the risk-based approach in financial monitoring necessitates the improvement of methods for assessing interconnections between financial institutions and identifying hidden risks arising in the course of transactions. In this context, Vnukova et al. (2019) proposed an approach to determining the level of connectivity of banks based on graph theory, which makes it possible to identify direct and inverse links between financial institutions, including hidden links that may indicate shared clients or a common economic source of funds. This, in turn, enables a more effective assessment of money laundering and terrorist financing risks within the framework of the risk-based approach.

The relevance of such approaches is confirmed by current trends in the development of the financial monitoring system in Ukraine. Sochka (2025) studied the organizational and legal foundations of financial monitoring in Ukraine for the period 2021–2024 and found that the total number of primary financial monitoring entities decreased by 24% as a result of strengthened regulatory requirements and market consolidation, while the share of suspicious financial transactions increased from 4.4% to 17.6%, indicating the strengthening of the risk-based approach.

As noted by Dokiienko et al. (2024), a comprehensive assessment of an enterprise's financial security should be based on a combination of indicators of financial stability, liquidity, and return on capital, which allows risk levels to be differentiated and a safety zone to be determined — an approach that may be adapted to client risk assessment in the financial monitoring system, analogously to the logic of forming "whitelists." At the same time, the practical implementation of such approaches requires their normative elaboration at the level of regulatory policy and subordinate legislation.

Legislative provisions, however, require further specification at the level of subordinate regulations. The regulatory acts of the National Bank of Ukraine (2018, 2019, 2020a, 2020b, 2024) provide for the need to improve risk management and financial monitoring systems with due regard to digitalization. Under the current conditions of transformation of Ukraine's financial system, the regulatory and legal framework for financial monitoring, formed on the basis of the risk-based approach and providing for the comprehensive identification, assessment, and minimization of risks of legalization or laundering of proceeds and terrorist financing, is of particular importance. As defined in the regulatory acts of the National Bank of Ukraine, banks and other institutions are obliged to implement effective systems of internal control, risk management, and customer due diligence that ensure the timely detection of suspicious financial transactions and compliance

DOI: 10.55643/fcaptp.3.68.2026.5248

with sanctions restrictions (National Bank of Ukraine, 2018, 2019, 2020a, 2020b). These requirements have become especially relevant under martial law, when the regulator additionally strengthened requirements for the organization of financial monitoring, currency supervision, and control over the implementation of special economic restrictions, orienting market participants toward greater flexibility and effectiveness of compliance procedures (National Bank of Ukraine, 2024). In this context, the implementation of "whitelist" mechanisms may be considered an instrument for improving the regulatory model, as it allows clients to be differentiated by risk level. At the same time, the NBU regulatory framework does not regulate the algorithmic component of "whitelists" — for example, automated updating and periodic review — which creates the risk of formalizing this mechanism without ensuring its functional effectiveness.

Hlibko et al. (2019) established that the implementation of risk-based requirements for bank capital in accordance with the recommendations of the Basel Committee on Banking Supervision reveals significant discrepancies in the calculation of required reserves for operational risk depending on the method used, while the obtained results are unprofitable. This indicates the need for further improvement of regulatory processes in the banking system. This confirms that even well-established risk-based approaches, such as Basel standards, require constant revision and adaptation, especially under conditions of digitalization, which is also relevant for the AML/CFT sphere.

As Kovalenko et al. (2024) note, despite the gradual improvement in the effectiveness of Ukraine's financial monitoring system after 2020, unresolved problems remain in the monitoring of cryptocurrency transactions, the implementation of artificial intelligence technologies, and the coordination of actions among various financial monitoring entities. This actualizes the need to develop new regulatory mechanisms, including "whitelists".

Unlike the predominantly centralized European and Ukrainian model, U.S. legislation forms a somewhat different configuration of financial control. The U.S. legislative framework, in particular the Bank Secrecy Act (1970), the Electronic Fund Transfer Act (1978), and the Dodd–Frank Act (2010), establishes the institutional framework for financial control, while modern payment systems, including the Federal Reserve System (n.d.), reflect the trend toward instant transactions, which increases requirements for the speed and accuracy of monitoring. The American model traditionally emphasizes reporting, particularly Suspicious Activity Reports (SARs), rather than the preventive filtering of low-risk clients, which limits the direct application of the "whitelist" concept. OECD reports (2026) emphasize that effective public regulation in the digital era requires a balanced and integrated policy that combines innovation, transparency, control, and the minimization of systemic threats in the financial sector, in particular through mechanisms of trust and market openness. By contrast, the National Institute of Standards and Technology (NIST, 2023), in its AI Risk Management Framework, emphasizes that any regulatory instruments aimed at increasing the security and reliability of systems must be based on measurable risks, a balance between control and socio-economic interests, and the principles of accountability and transparency.

Both European and American practices converge in recognizing the key role of artificial intelligence in financial monitoring; however, their approaches to its regulation differ significantly. In European practice, the adoption of the EU Artificial Intelligence Regulation (EUR-Lex, 2024) classifies financial monitoring systems as high-risk and establishes mandatory requirements for the transparency, explainability, and control of algorithms. In parallel, the development of the institutional architecture, in particular the establishment of the AMLA authority (EUR-Lex, 2021), is aimed at unifying approaches to financial control and strengthening coordination among regulators. The provisions of the GDPR and PSD2 (EUR-Lex, 2015, 2016) also play an important role, as they establish principles of data protection, the right to an explanation of automated decisions, and the increased responsibility of financial institutions. Additional emphasis is placed on the need to control the use of machine learning algorithms in the AML/CFT sphere and to implement mechanisms for their audit (European Banking Authority, 2025). For the whitelist concept, this means that any automated decision to classify a transaction or recipient as eligible for simplified processing must be explainable, auditable, and subject to review. Existing regulatory frameworks may allow financial institutions to apply internal exception logic or risk-reduction procedures, but they do not establish a uniform regulatory architecture that combines a centralized public-law recipient registry, legal-priority validation, pre-blocking verification, standardized audit trails, and appealable post-audit procedures.

The literature on AI governance in financial services also emphasizes that the expansion of autonomous decision-making increases the need for human oversight, explainability, and accountability. FinCrimeTech50 (2026) distinguishes between machine processing of predictable patterns and human oversight of decisions requiring legal and contextual assessment. Similarly, Maheshwari (2026) notes that AI systems in banking and payments increasingly perform critical functions, including fraud detection, sanctions control, customer assessment, and account restrictions, which require transparent governance mechanisms. This position is consistent with the AI risk-management approach for critical infrastructure, which stresses the importance of transparency, explainability, and human control in high-impact automated systems (Sheh & Stanley, 2026). For the present study, this literature supports the need for an AI Audit Layer and human-in-the-loop control in whitelist-based financial monitoring.

Synthesizing the reviewed international approaches and domestic experience, some authors already address the concept of the "whitelist" directly. The scholarly contribution of Dryha (2026) consists in identifying a new type of systemic risk — the algorithmic blocking of mandatory payments to public authorities in the digital economy — and substantiating the need to implement "whitelist" mechanisms as an instrument of positive transaction identification. However, this study focuses primarily on the technical aspect of preventing erroneous blockages, while leaving aside the regulatory formalization of the "whitelist" as an integrated model.

Thus, the analysis of international experience — the United States, the European Union, and Ukraine — confirms that contemporary approaches are oriented toward combining risk-based control with algorithmic transparency. Existing scholarship creates theoretical and practical prerequisites for the implementation of "whitelist" mechanisms; however, a systematic study of their regulatory model in financial monitoring remains fragmentary. In particular, the following aspects remain beyond the scope of scholarly analysis: legal criteria for differentiating clients for inclusion in a "whitelist"; algorithmic liability for erroneous classification, including false negatives and false positives in the context of positive identification; compatibility of "whitelists" with the requirements of the GDPR and the future AI Act regarding automated decision-making; and procedures for periodic review and appeal of status. Filling these gaps constitutes the scientific novelty and relevance of the proposed article, which is devoted to the development of a regulatory model for implementing "whitelist" mechanisms in financial monitoring as an instrument of state financial security.

The reviewed literature shows that false-positive alerts are usually considered either as a technical problem of model performance or as an operational burden for compliance departments. However, insufficient attention has been paid to the legal mechanism by which false-positive blocking arises in algorithmic financial monitoring. In particular, the literature does not sufficiently distinguish between risk indicators that trigger algorithmic suspicion and the actual cause of a false-positive decision, namely the absence of a legal-context validation layer. This gap is especially relevant for public-law and legally mandatory payments, where formal behavioral deviation may coexist with a verified legal obligation to pay. The present article addresses this gap by developing a conceptual and regulatory model that combines risk scoring, legal classification, whitelist eligibility criteria, and auditability.

AIMS AND OBJECTIVES

The purpose of the study is to substantiate and develop a regulatory model for implementing "whitelist" mechanisms in financial monitoring systems as an instrument for ensuring the financial security of the state under conditions of digitalization and algorithmization of financial processes.

To achieve this purpose, the article addresses the following objectives:

1. To define false-positive blocking in algorithmic financial monitoring and to distinguish it from legitimate high-risk classification.
2. To distinguish between risk indicators and the causal mechanisms that generate false-positive blocking decisions.
3. To develop independent low-risk eligibility criteria for public-law and legally mandatory payments.
4. To substantiate the feasibility of using whitelist mechanisms as a targeted validation tool rather than as a general exemption from AML/CFT monitoring.
5. To develop a regulatory model of financial monitoring based on the combination of algorithmic risk assessment, legal classification of transactions, registry-based recipient verification, and auditability.
6. To propose safeguards that preserve AML/CFT effectiveness while reducing unjustified automatic blocking of verified public-law payments.

METHODS

The research methodology is based on a combination of general scientific and applied approaches, which made it possible to analyze the development of financial monitoring under conditions of digital transformation and to formulate the "whitelist" mechanism. The systemic approach allowed financial monitoring to be considered as an integrated structure of interaction between regulatory, informational, and algorithmic elements, while comparative analysis made it possible to identify differences between traditional risk-based and algorithmic models of control.

DOI: 10.55643/fcaptp.3.68.2026.5248

The method of analysis and generalization was applied to examine international AML/CFT standards, RegTech approaches, regulatory legal acts, and concepts of AI use in financial monitoring.

The classification method was used to divide transactions according to their legal nature and to systematize the factors of algorithmic blocking.

The conceptual foundations of the "whitelist" mechanism were formed through theoretical modeling, which made it possible to develop a comprehensive financial monitoring model, a Dual Validation Model, a Real-Time Validation Layer, and to formalize the decision-making algorithm.

Structural-functional and institutional analysis was used to determine the functions of the regulator, financial institutions, and the key elements of the model, in particular the White List Registry and the AI Audit Layer.

The methodological basis of the study was the risk-based approach, adapted to the needs of algorithmic financial monitoring and the minimization of false-positive blockages. The source basis of the study consisted of regulatory legal acts, scholarly sources, and analytical materials of international organizations.

The study does not rely on proprietary bank transaction datasets or statistical measurement of actual false-positive cases. Therefore, the identification of false-positive cases in this article should be understood as conceptual and regulatory identification of possible mechanisms rather than empirical attribution based on internal bank data. The proposed taxonomy links common algorithmic risk indicators with legal-context failures capable of producing false-positive decisions in the specific category of public-law and legally mandatory payments. Accordingly, Table 1 should be read as a conceptual mapping based on AML/CFT risk indicators, transaction-monitoring logic, regulatory requirements, and legal analysis of public-law payments, rather than as a statistical output from a transactional dataset.

RESULTS

The study produced five interrelated findings: first, a definition and causal model of false-positive blocking in algorithmic financial monitoring; second, a conceptual taxonomy distinguishing risk indicators from false-positive mechanisms; third, independent low-risk eligibility criteria for public-law and legally mandatory payments; fourth, a whitelist-based regulatory architecture combining registry verification, legal classification, and algorithmic risk scoring; and fifth, an accountability framework based on audit logging, human review, and post-audit safeguards.

Definition and causal mechanism of false-positive blocking

For the purposes of this article, a false-positive alert or blocking is understood as an automated or semi-automated classification, suspension, or interruption of a financial transaction as high-risk or suspicious that is subsequently confirmed as legitimate on the basis of legal obligation, verified recipient status, standardized payment purpose, customer due diligence data, or post-audit review.

The study identifies the main cause of false-positive blocking in the analyzed category of transactions as a mismatch between behavioral risk indicators and the legal nature of the transaction. In algorithmic financial monitoring, a large amount, unusual frequency, new recipient, atypical geography, unclear payment purpose, or mismatch with the customer profile may trigger a higher risk score. However, these elements are risk indicators, not sufficient causes of illegitimacy. A false-positive decision arises when the system treats such indicators as grounds for blocking without verifying whether the transaction represents a legally mandatory or public-law payment.

The causal chain may therefore be described as follows: risk indicator → algorithmic risk interpretation → absence of legal-context validation → automatic blocking or suspension → subsequent confirmation of legitimacy. The whitelist mechanism proposed in this article is designed to intervene at the stage of legal-context validation, before an automatic blocking decision is executed.

Whitelist-based regulatory architecture

Before describing the operational sequence of transaction processing, the proposed whitelist-based regulatory model should be presented as a three-level architecture. The model consists of institutional, informational, and algorithmic levels, each of which performs a separate regulatory function. The institutional level defines the regulator, competent authorities, inclusion and removal procedures, oversight, and appeal mechanisms. The informational level provides verified data infrastructure, including the White List Registry, authoritative public-law recipient data, payment-purpose templates, and registry update procedures. The algorithmic level integrates risk scoring, legal-context validation, low-risk eligibility testing,

critical-risk screening, the AI Audit Layer, and human-in-the-loop control. Together, these levels form the regulatory basis for distinguishing verified public-law payments from transactions that merely contain formal risk indicators.

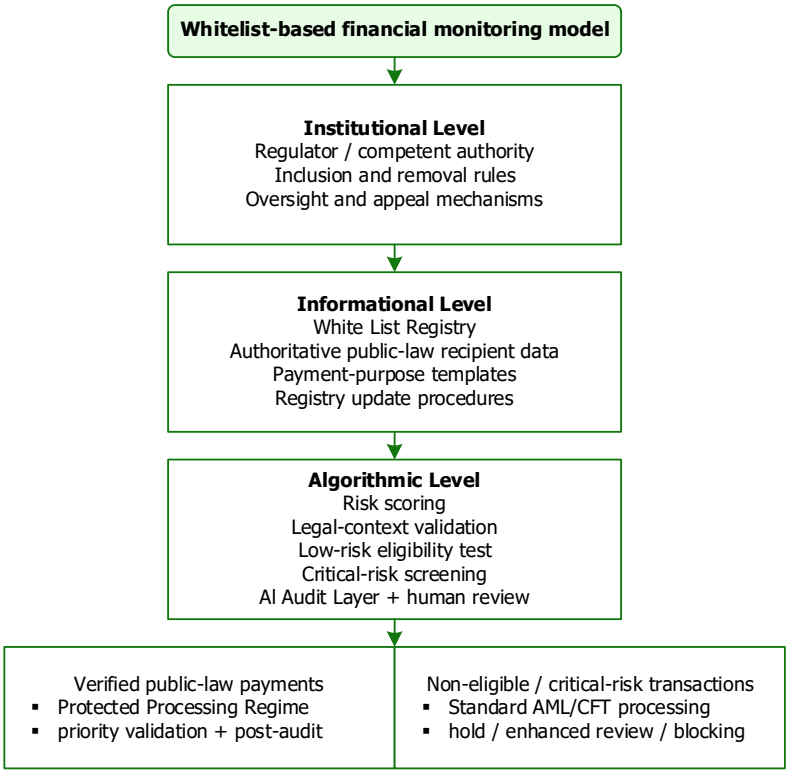

Figure 1. Three-level regulatory model of whitelist-based financial monitoring.

Based on the three-level model presented in Figure 1 and the identified causal mechanism, the proposed architecture combines algorithmic transaction analysis with legal classification and registry-based verification of public-law payment recipients. Within this architecture, a transaction passes through initial risk scoring, legal-context validation, recipient verification, low-risk eligibility testing, and audit logging. This structure allows the system to distinguish between transactions that are genuinely suspicious and transactions that merely contain formal risk indicators but have a verified legal basis.

The practical implementation of such a model requires the creation of a unified information mechanism capable of ensuring the automated verification of the legal status of payment recipients and minimizing the risks of unjustified transaction blocking. A key element of the model is the introduction of a centralized regulatory register of public-law payment recipients — the White List Registry — which is integrated with the payment infrastructure of banks and non-bank financial institutions. Unlike traditional account directories, such a register performs the function of an algorithmic decision-making instrument, making it possible to identify transactions as public-law transactions before they are blocked. Thus, the "whitelist" is transformed from a technical element of compliance verification into a comprehensive regulatory mechanism for risk management aimed at ensuring the continuity of legitimate financial transactions.

The "whitelist" mechanism is an instrument for validating transactions that satisfy independent low-risk eligibility criteria. It includes institutional, informational, and algorithmic levels and provides for integration into financial systems. Its implementation ensures the stability of financial flows and the reduction of risks.

To ensure a balance between automated risk control and the continuity of legitimate financial transactions, the model applies a special decision-making mechanism based on the combination of algorithmic analysis and legal assessment of transactions. The decision-making logic in the proposed model is implemented through the Dual Validation Model, which combines the assessment of transaction risk with its legal identification. In cases where a transaction receives an elevated algorithmic risk score but satisfies all low-risk eligibility criteria and no critical sanctions, terrorist-financing, fraud, account-compromise, or registry-integrity flags are present, automatic blocking is replaced by priority validation, enhanced logging, and post-audit. If any critical flag is detected, whitelist-based processing is suspended, and the transaction is subject to standard AML/CFT blocking, temporary hold, or enhanced review procedures.

DOI: 10.55643/fcaptp.3.68.2026.5248

The operational logic of the proposed model can be represented as a sequential decision-making architecture in which initial algorithmic risk assessment is supplemented by legal classification, recipient verification, low-risk eligibility testing, decision routing, audit logging, and post-audit control. Figure 2 illustrates the operational interaction between the main components of the whitelist-based financial monitoring model at the transaction-processing level.

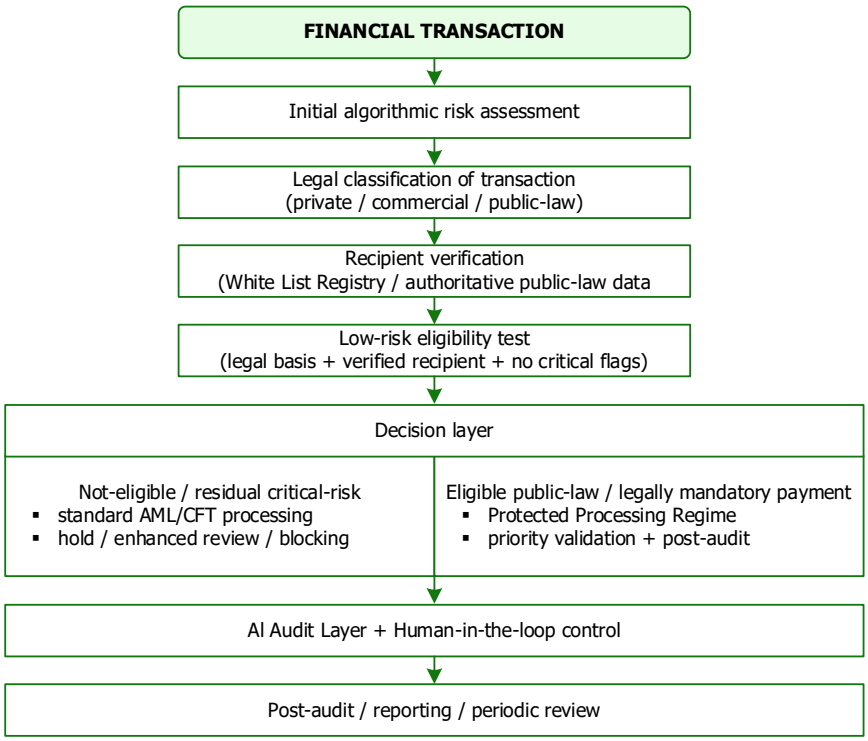

Figure 2. Operational decision-making architecture of the whitelist-based financial monitoring model.

Table 1 presents a conceptual mapping of recurring risk indicators, algorithmic assumptions, and false-positive mechanisms in financial monitoring, together with the methodological basis and validation response for each category.

Table 1. Conceptual mapping of risk indicators and false-positive mechanisms in algorithmic financial monitoring. Note: The table is a conceptual mapping based on AML/CFT risk indicators, transaction-monitoring logic, regulatory requirements for risk-based monitoring, and legal analysis of public-law payments. It does not represent statistical findings from proprietary bank transaction datasets. The term "false-positive mechanism" refers to the legal-context failure that may transform a risk indicator into an unjustified blocking decision.

Risk indicator used by monitoring system	Algorithmic assumption	False-positive mechanism	Basis for identification	Validation / whitelist-based response
One-time large payment	The transaction deviates from the customer's usual financial behavior	A legally mandatory payment may be misclassified as suspicious because the system evaluates the amount without legal purpose	AML/CFT risk indicators; legal analysis of statutory and public-law payments	Verify legal classification, recipient status, and payment purpose before blocking
Short-interval recurring payments	The transaction pattern may indicate structuring or smurfing	Periodic taxes, fees, enforcement payments, or administrative payments may resemble suspicious recurrence	Transaction-monitoring typologies; legal analysis of periodic public-law obligations	Compare frequency with statutory or administrative payment schedules
Payment to a new recipient account	Lack of prior interaction increases uncertainty	A first-time payment to a public authority or budgetary institution may be treated as risky despite official recipient status	Customer due diligence logic; registry-based recipient verification	Check recipient against the White List Registry or authoritative public-law recipient data
Rare client activity	Insufficient behavioral history makes the customer profile unstable	A legitimate mandatory payment by an otherwise inactive client may be treated as anomalous	Behavioral risk scoring logic; legal analysis of occasional mandatory payments	Give priority to legal classification and recipient verification over behavioral history alone

(continued on next page)

Table 1. Continued.

Risk indicator used by monitoring system	Algorithmic assumption	False-positive mechanism	Basis for identification	Validation / whitelist-based response
Atypical geography	The transaction falls outside the customer's ordinary jurisdictional pattern	Public-law, consular, tax, customs, or administrative payments may involve unusual geographic parameters	AML/CFT geographic risk indicators; legal analysis of official cross-jurisdictional payments	Verify official account status and legal basis; apply enhanced review only if residual risk remains
Mismatch with customer profile	Amount or purpose does not correspond to expected customer behavior	A legally required payment may conflict with the customer's ordinary commercial profile	Risk-based monitoring logic; legal analysis of mandatory payment obligations	Validate payment type as legally mandatory before applying blocking measures
Unclear payment purpose	Ambiguity increases the risk score	Non-standard wording by the payer may obscure an otherwise legitimate public-law payment	Payment-purpose classification; legal analysis of payment templates	Use standardized templates and payment-purpose classifiers
Atypical transaction time	Timing deviates from normal activity	Public-law deadlines, tax periods, or enforcement requirements may require payment outside ordinary time patterns	Transaction-monitoring logic; legal analysis of statutory deadlines	Verify statutory or administrative timing before blocking
Transaction involving elevated-risk account features	Account-level signals may indicate counterparty risk	A verified public authority account may be treated as risky if account data are incomplete, outdated, or associated with technical anomalies	CDD/EDD requirements; registry integrity checks	Apply registry verification, sanctions screening, and temporary enhanced review if compromise indicators exist

Low-risk eligibility criteria for whitelist-based processing

The proposed model distinguishes between low-risk eligibility and whitelist status. A transaction is not considered low-risk merely because it is associated with a whitelist. On the contrary, whitelist-based processing may be applied only after independent validation criteria have been satisfied. These criteria include: legal classification of the transaction as public-law or legally mandatory; verification of the recipient through an authoritative registry or other reliable public-law data source; conformity of the payment purpose with an approved template or legally identifiable payment category; absence of sanctions, terrorist-financing, fraud, account-compromise, or other critical risk indicators; and consistency of amount and frequency with statutory, contractual, administrative, or historically justified parameters.

Therefore, the whitelist mechanism functions as an output of legal and risk validation rather than as an unexplained input variable. It does not eliminate AML/CFT monitoring, but changes the processing logic for a narrow category of transactions from automatic blocking to priority validation, audit logging, and post-audit control.

In the proposed model, a financial transaction passes through successive processing stages:

1. Initial risk scoring and identification of transaction parameters.
2. Classification according to legal nature, including private, commercial, and public-law payments.
3. Recipient verification and payment-purpose validation through authoritative public-law data.
4. Low-risk eligibility testing, including critical-risk screening.
5. Routing either to standard AML/CFT processing or to protected processing with priority validation, audit logging, and post-audit control.

This approach allows the legal characteristics of financial transactions to be integrated directly into algorithmic decision-making. The key innovation of the model is not the automatic priority of legal status over risk scoring, but the introduction of a legal-context validation stage that must be combined with sanctions screening, fraud detection, account-compromise checks, registry-integrity verification, and residual-risk assessment. For verified public-law payments, the model replaces automatic blocking based solely on formal risk indicators with priority validation and post-audit control; where critical risk flags are present, standard AML/CFT measures continue to apply.

The further development of the model involves shifting the focus from ex post control to preventive real-time transaction verification, which makes it possible to minimize the risk of erroneous blocking before the payment transaction is completed. To improve the effectiveness of control, the introduction of a Real-Time Validation Layer is proposed, which verifies transactions before a decision on their blocking is made. Such verification includes identification of the recipient through the regulatory register, analysis of the payment purpose template, and assessment of the regularity of the transaction.

DOI: 10.55643/fcaptp.3.68.2026.5248

The effectiveness of preventive verification directly depends on the ability to ensure the transparency of algorithmic decisions and control over their justification at all stages of transaction processing.

The AI Audit Layer is not an additional AI model that independently "tests" transactions. It is an accountability, explainability, and logging layer embedded into the decision-making architecture of financial monitoring systems. Its purpose is to make every automated or semi-automated decision reconstructable for compliance officers, regulators, auditors, and, where legally required, affected customers.

For each transaction, the AI Audit Layer should record at least the following elements: transaction identifier or pseudonymized reference; timestamp; risk score; triggered rules or model features; model version; applicable risk threshold; legal classification of the transaction; recipient verification result; payment-purpose validation result; sanctions and critical-risk screening result; whitelist eligibility status; registry version used for verification; decision outcome; reason code; human review or override decision; responsible compliance role; and post-audit or appeal outcome.

Functionally, the AI Audit Layer operates after initial risk scoring and in parallel with legal-context validation. It does not replace human compliance judgment. Instead, it creates an auditable record explaining why a transaction was blocked, suspended, redirected to enhanced review, processed under the protected regime, or released after validation. This layer is necessary to prevent both unjustified false-positive blocking and uncontrolled false-negative processing.

Difference between existing AML/CFT monitoring and the proposed model

The proposed model should not be interpreted as a claim that banks do not use internal exception lists, risk-reduction rules, or manual override procedures under existing regulation. Such internal mechanisms may exist as part of proprietary compliance systems. The difference lies in the level of regulatory standardization, legal-context validation, and auditability. Existing systems are primarily designed to detect suspicious activity and manage risk exposure, whereas the proposed model introduces a formalized regulatory architecture for the positive identification of verified public-law payments before automatic blocking is executed.

Table 2 summarizes the main differences between existing AML/CFT monitoring practices and the proposed whitelist-based regulatory model.

Table 2. Existing system vs proposed approach.

Element	Existing AML/CFT monitoring	Proposed whitelist-based model
Main logic	Detection of suspicious or high-risk transactions	Combination of risk detection with positive legal identification
Treatment of public-law payments	Usually processed under general transaction-monitoring rules unless internal exceptions exist	Subject to separate legal classification and recipient verification before automatic blocking
Whitelist or exception logic	May exist internally as bank-specific compliance logic	Standardized regulatory mechanism with defined eligibility criteria
Registry component	No uniform public-law recipient registry as a mandatory decision layer	Centralized White List Registry or authoritative public-law recipient data source
Blocking decision	Based on risk score, rules, sanctions screening, and internal compliance policy	Based on risk score plus legal classification, registry verification, critical-risk screening, and auditability
Auditability	Internal logs and compliance documentation vary by institution	Standardized AI Audit Layer with model versioning, reason codes, registry versioning, human override logs, and post-audit records
Human control	Applied according to internal procedures	Mandatory for ambiguous, high-impact, or residual-risk whitelist cases
Safeguards against abuse	Internal review and regulatory supervision	Periodic registry review, suspension procedures, appeal mechanism, independent audit, and critical-risk override

A further development of the principle of algorithmic accountability is the establishment of special regulatory regimes for processing socially significant transactions, aimed at guaranteeing the continuity of critically important financial flows.

Within the proposed concept, the expediency of creating a Protected Processing Regime for verified public-law payments is substantiated. This regime does not exempt such transactions from AML/CFT monitoring. Rather, it prevents automatic blocking based solely on behavioral or contextual risk indicators when the transaction has passed legal classification, recipient verification, payment-purpose validation, and critical-risk screening. Where residual risk remains, the transaction

may be subject to temporary suspension, enhanced review, or post-audit. Where sanctions, terrorist-financing, fraud, account-compromise, or registry-integrity flags are detected, the protected processing regime does not apply.

Formalization of the model

The decision-making logic should first determine whether a transaction is independently eligible for low-risk whitelist-based processing. Whitelist status is therefore not an input that automatically explains low risk; it is an output of prior validation.

Let transaction t be assessed according to the following criteria:

- $LC(t)$ — legal classification of the transaction as public-law or legally mandatory;
- $VR(t)$ — verification of the recipient through an authoritative registry or equivalent public-law data source;
- $PT(t)$ — conformity of the payment purpose with an approved template or legally identifiable payment category;
- $CF(t)$ — presence of critical flags, including sanctions, terrorist-financing, fraud, account-compromise, or registry-integrity indicators;
- $AF(t)$ — consistency of amount and frequency with statutory, contractual, administrative, or historically justified parameters.

Low-risk eligibility may be represented as follows:

$$LRE(t) = 1 \Leftrightarrow LC(t) = 1 \wedge VR(t) = 1 \wedge PT(t) = 1 \wedge CF(t) = 0 \wedge AF(t) = 1$$

Thus, a transaction is eligible for whitelist-based processing only when its legal nature, recipient, payment purpose, and amount/frequency parameters are verified, and no critical risk flags are present.

Whitelist eligibility may then be represented as:

$$WE(t) = 1 \Leftrightarrow LRE(t) = 1$$

The decision rule may be expressed as:

$$Decision(t) = \begin{cases} Block/Hold/Enhanced\ Review, & \text{if } CF(t) = 1; \\ Priority\ Validation + Post\ Audit, & \text{if } WE(t) = 1 \text{ and } CF(t) = 0; \\ Standard\ AML/CFT\ Processing, & \text{if } WE(t) = 0 \text{ and } R(t) < \theta; \\ Enhanced\ Review\ or\ Blocking, & \text{if } WE(t) = 0 \text{ and } R(t) \geq \theta. \end{cases}$$

where $R(t)$ denotes the algorithmic risk score and θ denotes the applicable risk threshold.

This structure prevents circular reasoning: a transaction is not low-risk because it is whitelisted; rather, it becomes eligible for whitelist-based processing only after independent legal, registry, purpose, critical-risk, and amount/frequency validation.

The institutional implementation of the model involves the integration of three levels:

1. The institutional level, represented by the regulator.
2. The informational level, represented by registers and databases.
3. The algorithmic level, represented by artificial intelligence systems.

Such an architecture corresponds to modern RegTech approaches and ensures the comprehensive implementation of the "whitelist" mechanism in the financial system.

To ensure the practical applicability and regulatory accountability of the proposed whitelist-based model, its key components should be operationalized through a system of safeguards and measurable assessment indicators. Table 3 summarizes the main regulatory functions, risks, safeguards, and possible indicators for evaluating the implementation of the proposed model in financial monitoring systems.

DOI: 10.55643/fcaptp.3.68.2026.5248

Table 3. Operational and regulatory safeguards matrix for the whitelist-based financial monitoring model.

Model component	Regulatory function	Main risk addressed	Required safeguard	Possible assessment indicator
White List Registry	Provides positive identification of verified public-law payment recipients	Erroneous blocking of legitimate public-law payments	Centralized regulatory administration; periodic verification of registry entries	Number of validated public-law recipients; frequency of registry updates
Legal Priority Override	Ensures that the legal nature of a transaction prevails over formal algorithmic risk signals	Over-compliance and excessive reliance on behavioral risk indicators	Mandatory legal classification of transaction type before blocking	Share of transactions redirected from automatic blocking to priority validation
Dual Validation Model	Combines algorithmic risk scoring with legal classification	False-positive alerts caused by uniform algorithmic assessment	Parallel assessment of risk score, payment purpose, recipient status, and legal nature	False-positive rate before and after model implementation
Low-risk eligibility test	Determines whether a transaction qualifies for whitelist-based processing	Circular classification of transactions as low-risk merely because of whitelist status	Independent verification of legal classification, recipient status, payment purpose, critical flags, and amount/frequency consistency	Share of transactions passing each eligibility criterion; number of rejected whitelist-processing attempts
Real-Time Validation Layer	Verifies transaction legitimacy before a blocking decision is executed	Delayed or interrupted public-law payments	Pre-blocking verification through recipient registry and payment templates	Average validation time; number of prevented erroneous blockings
AI Audit Layer	Records and explains algorithmic decisions	Lack of transparency, accountability, and appealability of automated decisions	Logging of risk score, triggered rules, model version, registry version, legal classification, validation results, reason codes, human overrides, and post-audit outcomes	Percentage of decisions with complete audit trail; number of successfully reviewed cases
Protected Processing Regime for verified public-law payments	Prevents automatic blocking based solely on behavioral risk indicators after legal and critical-risk validation	Disruption of state financial flows and mandatory public-law payments	Priority validation, post-audit, and suspension of protected processing if critical flags are detected	Number of verified public-law payments redirected from automatic blocking; number of cases later escalated due to residual or critical risk
Human-in-the-loop control	Preserves human accountability for critical decisions	Autonomous algorithmic decisions without legal responsibility	Mandatory compliance officer review for ambiguous or high-impact cases	Share of high-risk whitelist cases reviewed by a human officer
Periodic review and appeal mechanism	Prevents abuse, outdated whitelist status, and regulatory capture	Unlawful inclusion in whitelist or failure to remove compromised entities	Scheduled reassessment, independent audit, and appeal procedure	Number of status reviews; number of removals, suspensions, or appeals

The proposed approach is designed to reduce unjustified automatic blocking of verified public-law and legally mandatory payments by addressing the legal-context failure that underlies this specific class of false-positive decisions. At the same time, it does not remove such transactions from AML/CFT monitoring. Its regulatory value lies in redirecting validated transactions from automatic blocking to priority validation, enhanced auditability, human review where necessary, and post-audit control.

DISCUSSION

The obtained results have important theoretical and practical implications that go beyond the mere technical improvement of compliance procedures. The study conceptually develops a number of propositions highlighted in the contemporary literature, while also proposing a distinct regulatory interpretation of false-positive blocking in algorithmic financial monitoring.

Comparison with previous studies shows that the proposed conceptual model is consistent with the current critique of AML/CFT systems based on rules and algorithmic risk assessment models. In particular, the conclusion regarding the systemic nature of false-positive blockages in such systems correlates with the position of Kungu et al. (2026) and Gilson (2024), who emphasize the excessive formalization of risk criteria and the insufficient consideration of the context and legal nature of financial transactions. However, unlike the approach of Jullum et al. (2020), who propose improving models by enriching training datasets, including unconfirmed but reviewed transactions, our work shifts the focus from adapting risk detection algorithms to the preventive positive identification of legitimate transactions.

The proposed Legal Priority Override mechanism responds to the prevailing practice of de-risking by introducing a structured legal-context validation stage before automatic blocking is executed. While Stulz identifies the problem, our model proposes an institutional solution that makes it possible to avoid over-compliance without weakening general anti-money laundering standards. This resonates with the ideas of Arner et al. (2017) regarding the need for "proportional real-time regulation," but gives them a concrete operational form through a three-level architecture and the Dual Validation Model.

Particular importance should be attached to the comparison with the findings of Dryha (2026), who first raised the issue of algorithmic blocking of mandatory payments. While the previous work focused on identifying the risk, our study proposes a full-fledged regulatory response by integrating the "whitelist" into the general architecture of financial monitoring. Moreover, we introduce a new term — the regulatory risk of algorithmic blocking of public-law payments — as a separate type of systemic risk requiring a special management regime.

The proposed model does not contradict but, on the contrary, develops the FATF risk-based approach (2023), which expressly provides for the possibility of simplified due diligence for low-risk clients. Our model specifies how this principle may be implemented at the level of algorithmic decision-making. However, a potential stumbling block is the FATF requirement for universal transaction monitoring without "blind spots." The Protected Processing Regime for verified public-law payments may be perceived by some national regulators or FATF auditors as an impermissible exception. Therefore, in practical implementation, we insist not on the abolition of control but on its transfer to a priority post-audit regime, which is a legitimate risk management instrument.

A further point concerns the relationship between the proposed model and existing bank-level compliance practices. The article does not claim that financial institutions never use internal exception lists, manual overrides, or risk-reduction rules. Such mechanisms may exist as proprietary elements of internal AML/CFT systems. The proposed model differs because it formalizes whitelist-based processing as a regulatory architecture rather than as a discretionary internal exception. Its distinctive elements are the public-law focus, independent low-risk eligibility criteria, centralized or authoritative recipient verification, pre-blocking legal-context validation, standardized audit logging, and post-audit accountability.

In the context of European regulation, our model demonstrates a high degree of compatibility with the requirements of the AI Act (EUR-Lex, 2024). The classification of financial monitoring systems as high-risk requires precisely the mechanisms we propose: explainability through the AI Audit Layer, human control through Human-in-the-loop via Dual Validation, and accountability. At the same time, the question remains open as to the application of the right to an explanation of an automated decision in cases where a transaction from the "whitelist" is nevertheless erroneously blocked due to a technical failure. This requires a separate legal compensation mechanism.

Despite its theoretical substantiation, the study has important limitations. The first limitation is the absence of empirical verification based on proprietary bank transaction datasets. The article does not measure the actual frequency of false-positive blocking and does not statistically attribute specific blocking cases to particular algorithmic causes. Instead, it develops a conceptual and regulatory taxonomy of false-positive mechanisms based on AML/CFT risk indicators, transaction-monitoring logic, regulatory requirements, and legal analysis of public-law payments. To confirm the practical effectiveness of the proposed model, future research should test it using real or simulated transactional data, including precision, recall, false-positive rate, false-negative rate, and post-audit validation outcomes.

The problem of compromising the "whitelist" also constitutes a significant limitation of the proposed model. The study does not examine in detail a scenario in which an entity included in the White List Registry, for example, a public authority or budgetary institution, becomes the target of a cyberattack or its account is used for the legalization of criminal proceeds without the owner's knowledge. In such a case, the positive identification mechanism may create a risk of legitimizing unlawful transactions through the automated reduction of the risk level for transactions associated with the relevant entity. This indicates the need to introduce dynamic mechanisms for monitoring the integrity and relevance of the White List Registry, including procedures for continuous verification, behavioral analysis, automated anomaly detection, and mechanisms for the prompt temporary exclusion of entities from the "whitelist" if signs of compromise are detected.

Jurisdictional and legal uncertainty is also an important limitation of the proposed model. The developed approach is primarily oriented toward functioning within a national payment system and domestic financial monitoring infrastructure. At the same time, in the field of cross-border transfers, international payment platforms, and transactions involving central bank digital currencies (CBDCs), the problem arises of mutual recognition and compatibility of "whitelist" mechanisms between different jurisdictions.

The risk of regulatory capture is another significant challenge for the practical implementation of the proposed model. Procedures for including entities in the "whitelist" must not turn into a source of corrupt practices, political influence, or an instrument of unfair competition through the granting of privileged status to certain market participants. Although the

DOI: 10.55643/fcaptp.3.68.2026.5248

study substantiates the need for independent audit and periodic review of the White List Registry, mechanisms for preventing lobbying, conflicts of interest, and unlawful influence on verification procedures have not been developed in detail. This highlights the need to establish transparent criteria for inclusion in the "whitelist," multi-level verification procedures, external regulatory oversight, and mechanisms of public accountability, which should become the subject of separate further research.

The proposed regulatory model is not a finalized applied solution but rather a theoretical foundation for further interdisciplinary research at the intersection of financial law, computer science, RegTech, and public administration. Its scientific value lies not only in the development of a specific "whitelist" mechanism, but also in framing the problem of algorithmic blocking of legitimate financial transactions as a separate regulatory challenge of digital financial infrastructure and in substantiating a systemic pathway for addressing it.

CONCLUSIONS

As a result of the conducted conceptual and regulatory analysis, the study argues that algorithmic financial monitoring, while increasing the speed and scalability of risk detection, may generate a specific regulatory risk: false-positive blocking of legitimate financial transactions, especially public-law and legally mandatory payments. The principal mechanism of such false-positive decisions lies not in the mere presence of risk indicators, such as large amounts, unusual frequency, atypical geography, or mismatch with the customer profile, but in the absence of a legal-context validation layer capable of distinguishing suspicious deviation from legally required payment behavior.

The article substantiates the whitelist mechanism as a targeted regulatory instrument for positive identification of verified public-law and legally mandatory payments. The model does not treat whitelist status as an automatic exemption from AML/CFT monitoring. Instead, whitelist-based processing is available only after independent low-risk eligibility criteria have been satisfied, including legal classification, recipient verification, payment-purpose validation, absence of critical risk flags, and consistency of amount and frequency with legally or economically justified parameters.

The article develops a regulatory model for implementing "whitelist" mechanisms based on the integration of three interrelated levels: institutional, informational, and algorithmic. The institutional level provides for the identification of entities responsible for forming, administering, and auditing the "whitelist"; the informational level provides for the creation of a centralized register of public-law payment recipients — the White List Registry; and the algorithmic level provides for the implementation of the Dual Validation Model, the Real-Time Validation Layer, the AI Audit Layer, and a special regime for the protected processing of public-law payments. The proposed model ensures the combination of AML/CFT requirements with the need to maintain the stability and continuity of state financial flows.

The theoretical significance of the study lies in expanding the classical risk-based approach in financial monitoring by integrating mechanisms of positive identification of legitimate transactions. The category of "regulatory risk of algorithmic blocking of public-law payments" is introduced for the first time as a separate type of systemic risk within digital financial infrastructure. The proposed approach develops contemporary concepts of RegTech and AI governance, forming a basis for the development of algorithmically accountable models of financial monitoring, in which automated decision-making is combined with the principles of explainability, accountability, and human control over critically important decisions — human-in-the-loop.

The practical significance of the obtained results lies in the possibility of using the proposed model by central banks, financial regulators, and primary financial monitoring entities to improve AML/CFT systems, optimize compliance procedures, and reduce the level of false-positive blockages. Conceptual modeling suggests that the integration of whitelist mechanisms and dual validation may reduce the risk of unjustified automatic blocking of verified public-law payments, provided that the model is combined with critical-risk screening, audit logging, human review, periodic registry verification, and post-audit control.

At the same time, the study has certain limitations. The proposed model is conceptual and theoretical in nature and requires further empirical verification based on real transactional data and the practical operation of AI systems in financial monitoring. A separate challenge remains the risk of unlawful inclusion of entities in the "whitelist," which may create threats of regulatory capture and abuse. This requires the formation of independent audit procedures, mechanisms for the periodic review of the status of "whitelist" participants, and procedures for appealing automated decisions. Additional attention should be paid to ensuring the compatibility of the proposed model with the requirements of the GDPR, the AI Act, and FATF international standards concerning automated decision-making, personal data protection, and the transparency of algorithmic control.

Prospects for further research should focus on transforming the proposed conceptual model into an empirically tested and technically secure regulatory instrument. The first direction concerns the development of a protocol for the secure cryptographic protection of the White List Registry, including the possible use of distributed ledger technology to prevent unauthorized changes and ensure registry integrity. The second direction involves empirical testing of the model using real or simulated transactional data and quantitative performance metrics, including precision, recall, F1-score, false-positive rate, and false-negative rate. The third direction concerns the adaptation of the model to instant payment systems, open banking infrastructures, central bank digital currencies, and cross-border digital financial ecosystems, where decision-making time and interoperability are critical. The fourth direction requires a comparative analysis of low-risk eligibility criteria based on legal nature, transaction history, reputational data, recipient verification, and payment-purpose classification.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

All authors have contributed equally.

FUNDING

The Authors received no funding for this research.

CONFLICT OF INTEREST

The Authors declare that there is no conflict of interest.

REFERENCES

1. Arner, D. W., Barberis, J., & Buckley, R. P. (2015). *The evolution of FinTech: A new post-crisis paradigm?* (University of Hong Kong Faculty of Law Research Paper No. 2015/047; UNSW Law Research Paper No. 2016-62). SSRN. https://doi.org/10.2139/ssrn.2676553
2. Arner, D. W., Barberis, J., & Buckley, R. P. (2017). FinTech, RegTech, and the reconceptualization of financial regulation. *Northwestern Journal of International Law & Business, 37*(3), 371–413. https://ssrn.com/abstract=2847806
3. *Bank Secrecy Act*, 31 U.S.C. § 5311 et seq. (1970). Financial Crimes Enforcement Network. https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act
4. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems, 50*(3), 602–613. https://doi.org/10.1016/j.dss.2010.08.008
5. Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science, 17*(3), 235–255. https://doi.org/10.1214/ss/1042727940
6. Central Bank of the United Arab Emirates. (2022). *Anti-money laundering and combating the financing of terrorism and illegal organisations: Guidance for licensed financial institutions on suspicious transaction reporting*. https://rulebook.centralbank.ae/en/entiresection/465
7. Cummings, F. (2024). Three keys to false positive remediation in AML/CTF compliance. *AML Partners*. https://amlpartners.com/insights/false-positive-remediation-aml-ctf/
8. *Dodd–Frank Wall Street Reform and Consumer Protection Act*, Pub. L. No. 111–203, 124 Stat. 1376 (2010). https://www.congress.gov/111/plaws/publ203/PLAW-111publ203.pdf
9. Dokiienko, L., Hrynyuk, N., Britchenko, I., Trynchuk, V., & Levchenko, V. P. (2024). Determinants of enterprise's financial security. *Quantitative Finance and Economics, 8*(1), 52–74. https://doi.org/10.3934/QFE.2024003
10. Dryha, Z. V. (2026). Artificial intelligence in systems for combating financial fraud by banks and the risk of blocking mandatory payments to state authorities. In *SCIENTIA: Scientific forum: Theory and practice of research. Proceedings of the International Scientific and Practical Conference* (March 13, 2026, San Francisco, CA, United States). Scientific Publishing.
11. *Electronic Fund Transfer Act*, 15 U.S.C. § 1693 et seq. (1978). Board of Governors of the Federal Reserve System. https://www.federalreserve.gov/boarddocs/caletters/2008/0807/08-07_attachment.pdf
12. European Parliament and Council of the European Union. (2015, November 25). *Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366
13. European Parliament and Council of the European Union. (2016, April 27). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. EUR-Lex. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
14. European Commission. (2021, July 20). *Proposal for a regulation establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism, COM(2021) 420*

DOI: 10.55643/fcaptp.3.68.2026.5248

final. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0420

15. European Parliament and Council of the European Union. (2024, June 13). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. EUR-Lex. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
16. European Banking Authority. (2025). *Opinion of the European Banking Authority on money laundering and terrorist financing risks affecting the European Union financial sector and report on money laundering and terrorist financing risks affecting the European Union financial sector*. https://www.eba.europa.eu/sites/default/files/2025-07/13ae2f94-dc04-4a50-9f24-af2808e78944/Opinion%20and%20Report%20on%20ML%20TF%20risks.pdf
17. Federal Reserve System. (n.d.). *FedNow Service*. https://www.frbservices.org/financial-services/fednow
18. Financial Action Task Force. (2023, February). *International standards on combating money laundering and the financing of terrorism and proliferation: The FATF recommendations*. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html
19. FinCrimeTech50. (2026). What decisions can machines be allowed to make? *FinTech Global*. https://fintech.global/fincrime50/what-decisions-can-machines-be-allowed-to-make/
20. Gilson, C. (2024). Are the old ways of transaction monitoring dead? *Journal of Financial Compliance, 8*(2), 102–111. https://doi.org/10.69554/RJCX4578
21. Glonti, V., Polinkevych, O., Khovrak, I., Levchenko, V., Trynchuk, V., & Beridze, I. (2024). Transformation of business models in the context of achieving sustainable development. *Quality – Access to Success, 25*(202), 40–52. https://doi.org/10.47750/QAS/25.202.05
22. Hlibko, S. V., Vnukova, N., Hontar, D. D., Anisimova, H. V., & Liubchych, A. N. (2019). Risk-oriented approach to determining bank capital size according to the requirements of the Basel Committee on Banking Supervision. *Economic Studies Journal*, *(1),* 56–71.
23. Jullum, M., Loland, A., Huseby, R. B., Anonsen, G., & Lorentzen, J. (2020). Detecting money laundering transactions with machine learning. *Journal of Money Laundering Control, 23*(1), 173–186. https://doi.org/10.1108/JMLC-07-2019-0055
24. Kovalenko, V., Shevtsova, O., Sheludko, S., Matskiv, O., & Azarenkov, S. (2024). Effectiveness of regulatory enforcement for anti-money laundering in Ukraine: Is it all quiet on the financial front? *Financial and Credit Activity: Problems of Theory and Practice, 6*(59), 353–370. https://doi.org/10.55643/fcaptp.6.59.2024.4550
25. Kungu, C. O., Senagi, K., & Omondi, E. (2026). Hybrid deep learning for anti-money laundering: Unsupervised detection of emerging schemes via feature fusion and explainable artificial intelligence. *Machine Learning with Applications, 23*, 100856. https://doi.org/10.1016/j.mlwa.2026.100856
26. Law of Ukraine No. 361-IX. (2019, December 6). *On prevention and counteraction to legalization (laundering) of proceeds of crime, financing of terrorism and financing of proliferation of weapons of mass destruction*. Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/laws/show/361-20
27. Levytska, S., Pershko, L., Akimova, L., Akimov, O., Havrilenko, K., & Kucherovskii, O. (2022). A risk-oriented approach in the system of internal auditing of subjects of financial monitoring. *International Journal of Applied Economics, Finance and Accounting, 14*(2), 194–206. https://doi.org/10.33094/ijaefa.v14i2.715
28. Maheshwari, A. (2026). From black boxes to boardrooms: How banks must govern artificial intelligence. *Global Association of Risk Professionals*. https://www.garp.org/risk-intelligence/culture-governance/black-boxes-boardrooms-260220
29. National Bank of Ukraine. (2018, June 11). *Resolution No. 64 on approval of the regulation on the organization of risk management systems in banks of Ukraine and banking groups*. https://zakon.rada.gov.ua/laws/show/v0064500-18
30. National Bank of Ukraine. (2019, July 2). *Resolution No. 88 on approval of the regulation on the organization of internal control systems in banks of Ukraine and banking groups*. https://zakon.rada.gov.ua/laws/show/v0088500-19
31. National Bank of Ukraine. (2020, May 19). *Resolution No. 65 on approval of the regulation on the implementation of financial monitoring by banks*. https://zakon.rada.gov.ua/laws/show/v0065500-20
32. National Bank of Ukraine. (2020, July 28). *Resolution No. 107 on approval of the regulation on the implementation of financial monitoring by financial institutions*. https://zakon.rada.gov.ua/laws/show/v0107500-20
33. National Bank of Ukraine. (2024, December 20). *Resolution No. 153 on approval of the regulation on the procedure for organizing the implementation of certain requirements of legislation in the field of financial monitoring, currency supervision, supervision in the field of implementation of special economic and other restrictive measures (sanctions) during martial law, and amendments to certain regulatory legal acts of the National Bank of Ukraine*. https://zakon.rada.gov.ua/laws/show/v0153500-24
34. National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0).* U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
35. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection. *Decision Support Systems, 50*(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006
36. Organisation for Economic Co-operation and Development. (2026). *The OECD going digital integrated policy framework 2026*. OECD Publishing. https://www.oecd.org/en/publications/the-oecd-going-digital-integrated-policy-framework-2026_0254ae07-en.html
37. Sheh, R., & Stanley, M. (2026). *Concept note: Artificial intelligence risk management framework—Trustworthy AI in*

critical infrastructure profile. National Institute of Standards and Technology. https://www.nist.gov/system/files/documents/2026/04/08/Concept%20Note_%20Development%20of%20the%20NIST%20AI%20RMF%20Trustworthy%20Use%20of%20AI%20in%20Critical%20Infrastructure%20Profile.pdf

38. Columbia University, School of International and Public Affairs. (2026). *Detecting financial crimes: Evaluating the efficacy of automated transaction monitoring*. https://www.sipa.columbia.edu/detecting-financial-crimes-evaluating-efficacy-automated-transaction-monitoring

39. Sochka, K. (2025). Financial monitoring in Ukraine: Organizational and legal principles and tasks in the context of modern challenges. *Acta Academiae Beregsasiensis. Economics, 1*(11), 442–457. https://doi.org/10.58423/2786-6742/2025-11-442-457

40. Stulz, R. M. (2019). FinTech, BigTech, and the future of banks. *Journal of Applied Corporate Finance, 31*(4), 86–97. https://doi.org/10.1111/jacf.12378

41. Travis, E. (2026). Compliance without conscience: Why algorithms cannot replace ethical judgement. *OpusDatum*. https://www.opusdatum.com/post/compliance-without-conscience-why-algorithms-cannot-replace-ethical-judgement

42. Vnukova, N., Kavun, S., Kolodiziev, O., Achkasova, S., & Hontar, D. (2019). Determining the level of bank connectivity for combating money laundering, terrorist financing and proliferation of weapons of mass destruction. *Banks and Bank Systems, 14*(4), 42–54. https://doi.org/10.21511/bbs.14(4).2019.05

Дрига Ж., Тринчук В., Левченко В., Середа О., Кочубей Л., Домашенко О.

РЕГУЛЯТОРНІ МЕХАНІЗМИ «БІЛОГО СПИСКУ» У ФІНАНСОВОМУ МОНІТОРИНГУ ДЛЯ ДЕРЖАВНОЇ ФІНАНСОВОЇ БЕЗПЕКИ

Автори розробили регуляторну модель упровадження механізмів «білого списку» у фінансовому моніторингу як інструменті забезпечення фінансової безпеки держави в умовах цифровізації та алгоритмічного контролю транзакцій. Дослідження зосереджене на проблемі хибнопозитивного блокування легітимних і юридично обов'язкових транзакцій, насамперед публічно-правових платежів, щодо яких отримувач, призначення та правова підстава можуть бути перевірені за допомогою авторитетних даних. Методологія дослідження поєднує системний, порівняльний, структурно-функціональний, інституційний підходи та метод концептуального моделювання. Хибнопозитивне блокування визначене як автоматизована або напівавтоматизована класифікація чи призупинення фінансової транзакції як високоризикової, яка згодом підтверджується як легітимна на підставі її правової природи, верифікованого статусу отримувача, призначення платежу, даних належної перевірки клієнта або пост-аудиту. Встановлено, що ключовий механізм таких помилок полягає в невідповідності між поведінковими ризик-індикаторами та правовою класифікацією транзакції. Обґрунтовано, що велика сума, незвична частота, нетипова географія, новий отримувач або невідповідність профілю клієнта самі собою не є причинами нелегітимності, а становлять ризик-індикатори, які можуть породжувати хибнопозитивні рішення за відсутності правоконтекстної валідації. На цій основі запропоновано трирівневу регуляторну модель, що включає інституційний, інформаційний та алгоритмічний компоненти: централізований реєстр верифікованих отримувачів публічно-правових платежів, подвійну валідацію ризику та правової класифікації, оперативну передблокувальну перевірку, тест незалежної відповідності критеріям низького ризику, журналювання рішень, людський контроль і постаудитні запобіжники. Механізм «білого списку» автори розглядають не як виняток із AML/CFT-моніторингу, а як верифікований режим обробки транзакцій, що відповідають незалежним критеріям прийнятності й не містять критичних ризикових ознак. Практичне значення моделі полягає в можливості її використання фінансовими регуляторами та суб'єктами фінансового моніторингу для підвищення прозорості автоматизованих рішень. Запропонована модель спрямована на зменшення необґрунтованого автоматичного блокування, забезпечення безперервності державних фінансових потоків і підвищення пояснюваності, пропорційності й підзвітності алгоритмічного фінансового моніторингу.

Ключові слова: фінансовий моніторинг, фінансова безпека, штучний інтелект, механізм «білого списку», публічно-правові платежі, хибнопозитивне блокування, ризик-орієнтований підхід, AML/CFT, RegTech

JEL Класифікація: G18, G28, H26, K22, K42

DOI: 10.55643/fcaptp.3.68.2026.5248