Journal of the Academy
Asociación de Universidades del Perú, Lima, Perú.
ISSN 2707-0301
Núm. 15. Julio-Diciembre 2026
http://journalacademy.net/

A CONCEPTUAL AI-BASED ADAPTIVE MODEL FOR FRAUD DETECTION IN INTERNATIONAL TRANSACTIONS: INNOVATIONS, EMERGING RISKS, AND APPLICABILITY TO LATIN AMERICAN SMES

Vanessa SÁNCHEZ DEL CASTILLO[1]

Received	:	15/06/2026
Approved	:	28/09/2026
Published	:	13/09/2026

ABSTRACT:
The growth of digital international transactions has increased small and medium-sized enterprises' (SMEs) exposure to financial fraud, in a context where artificial intelligence (AI) can be used both to combat and commit this crime. In Mexico, losses of approximately 17.4 billion pesos were reported during the first half of 2025. This paper proposes, at a conceptual level, an adaptive fraud detection model under the Software as a Service (SaaS) modality aimed at Latin American SMEs. We used a mixed-methods approach with an exploratory-descriptive scope, combining a narrative documentary review, a descriptive analysis of aggregated operational records from a remittance organization (October 2024 to January 2025), and the design of an input, processing, and output data architecture. In the case analyzed, 103,720 calls were referred to the fraud department, and only 33,53% were confirmed as fraud, illustrating the friction created by fixed-rule systems. The proposed model combines supervised learning, unsupervised learning, and human review, and is designed to reduce that friction without weakening security. This study did not measure performance and requires subsequent empirical validation.

Keywords: artificial intelligence, financial fraud, international business, SMEs, machine learning, Industry 5.0.

[1]Student pursuing a Bachelor's degree in International Business. Universidad del Valle de México (UVM), Campus Puebla, Camino Real a San Andrés Cholula No. 4002, Emiliano Zapata, San Andrés Cholula 72810, México A830111224@my.uvm.edu.mx - https://orcid.org/0009-0003-0085-5885

INTRODUCTION

Digitalization and globalization have driven the growth of international transactions, particularly through digital platforms. This progress has increased the risk of financial fraud. According to the Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF, 2025), at least 80% of Mexican users have faced some form of scam attempt; during the first half of 2025, 3.5 million complaints were filed, of which 59% were confirmed as cyber fraud, resulting in losses of approximately 17,400 million pesos.

Small and medium-sized enterprises (SMEs) are particularly vulnerable. The Organization for Economic Cooperation and Development (OECD, 2021) warns that these companies face a significant cybersecurity technology gap and that their limited access to specialized personnel makes it difficult to respond to rapidly changing threats. Added to this is a fundamental problem: artificial intelligence (AI), which enables real-time anomaly detection, has also become a tool for making fraud more sophisticated—a feature Kshetri (2021) describes as the technology's dual nature.

Experience in fraud prevention also shows that many victims do not immediately realize they are being deceived. In documented cases, perpetrators use sophisticated techniques—such as voice cloning or impersonating trusted individuals—and exploit emotional vulnerability to carry out the deception.

Recent literature has made progress on two fronts. On the one hand, Hernández Aros et al. (2024) reviewed machine learning techniques for detecting financial fraud. On the other hand, the explainability of models—that is, the ability to understand and justify their decisions—has been discussed (Černevičienė & Kabašinskas, 2024; Hassija et al., 2024). However, the sources consulted for this study revealed few approaches that integrate, within a single design, three elements critical for Latin American SMEs: an accessible solution—requiring no proprietary infrastructure—delivered as Software as a Service (SaaS); the behavioral dimension of fraud, based on social engineering; and the operational friction experienced by legitimate customers when the system holds up their transactions. This study

How to cite: Sánchez del Castillo, V. (2026). A Conceptual Ai-Based Adaptive Model for Fraud Detection in International Transactions: Innovations, Emerging Risks, and Applicability to Latin American Smes. *Journal of the Academy,* (15), 94-114. https://doi.org/10.47058/joa15.7

aims to help fill that gap through a conceptual proposal, supported by a real-world operational case study of a remittance broker operating between the United States and Latin America.

The research question guiding this study is: How can an adaptive model based on artificial intelligence strengthen the detection of financial fraud in international transactions conducted by Latin American SMEs in the face of new threats, without creating excessive friction for legitimate users? The central objective is to propose, at a conceptual level, an adaptive AI-based anti-fraud model to strengthen the detection of emerging threats. Additionally, the study seeks to substantiate the impact of AI's dual nature in the face of threats such as deepfakes and advanced phishing; to describe, based on an operational case study, the limitations of a detection system based on fixed rules; to structure the model into three stages—data input, processing, and output—; and to make a preliminary assessment of the economic and operational viability of SaaS anti-fraud solutions for SMEs.

DEVELOPMENT

Incorporating machine learning into anti-fraud systems has changed how illicit transactions are identified. The OECD (2021) notes that these techniques enable processing large volumes of data and detecting atypical patterns with greater accuracy and fewer false alarms, especially in digital banking and money transfers. Hernández Aros et al. (2024), in their literature review, highlight that machine learning models recognize complex patterns and facilitate the early detection of fraudulent activities.

These techniques fall into two categories. Supervised learning is trained using historical records labeled as legitimate or fraudulent and is effective at recognizing recurring patterns. Unsupervised learning, by contrast, identifies unusual behaviors without prior examples and can therefore detect new forms of fraud. Samson-Onuorah (2023) argues that the best results come when machine learning is combined with continuous monitoring and governance processes that allow supervision, validation, and model updates as threats evolve.

The World Bank warns that the same tools that strengthen defenses are already in attackers' hands (Boeddu et al., 2021). Kshetri (2021) frames this as a duality: AI's ability to reinforce

How to cite: Sánchez del Castillo, V. (2026). A Conceptual Ai-Based Adaptive Model for Fraud Detection in International Transactions: Innovations, Emerging Risks, and Applicability to Latin American Smes. *Journal of the Academy,* (15), 94-114. https://doi.org/10.47058/joa15.7

protective mechanisms matches its potential to complicate attacks. Among the most concerning methods are deepfakes and identity theft using synthetic voices and images capable of evading biometric systems (Passos et al., 2024); advanced phishing, with personalized messages generated by language models (Boeddu et al., 2021); automated bots that carry out fraudulent operations on a massive scale; and adaptive fraud, in which criminals quickly learn to evade controls (Samson-Onuorah, 2023).

In Latin America, the rise in digital transactions, remittances, and SME activity has been matched by a proportional increase in identity theft and account misuse cases (OECD, 2021). Furthermore, fraud is not merely a technical phenomenon: many attacks rely on manipulating the victim's trust and sense of urgency—a behavioral dimension that any detection model must account for.

AI is part of the Fourth Industrial Revolution, driven by the integration of big data, cloud computing, artificial intelligence, and interconnectivity. Big data is indispensable because the volume of daily transactions would be impossible to review manually; its value lies in converting it into useful knowledge for decision-making (Hernández Aros et al., 2024). Cloud computing has lowered technological barriers for SMEs by giving them access to advanced monitoring tools without requiring large investments in their own infrastructure (OECD, 2021). Interconnectivity facilitates international trade, but it also multiplies vulnerabilities.

Industry 5.0 builds on that same technological environment but shifts the focus to the human being: technology should complement human capabilities, not replace them. Schmalzried et al. (2023) argue that although AI processes millions of records in a short time, specialists are still needed to interpret complex contexts and validate decisions that may affect legitimate customers. Tóth et al. (2023) point out that collaboration between intelligent systems and analysts results in more reliable and resilient processes than automation alone. This position resonates with the debate on model transparency: as algorithms grow more complex, accuracy alone is no longer sufficient; it is also important to be able to understand and justify their decisions (Černevičienė & Kabašinskas, 2024; Hassija et al., 2024).

How to cite: Sánchez del Castillo, V. (2026). A Conceptual Ai-Based Adaptive Model for Fraud Detection in International Transactions: Innovations, Emerging Risks, and Applicability to Latin American Smes. *Journal of the Academy,* (15), 94-114. https://doi.org/10.47058/joa15.7

This study adopts a middle ground, aligned with Industry 5.0: automating responses to low-risk transactions and reserving human intervention for ambiguous or high-risk cases. Systems based on fixed rules—such as monetary thresholds or name-matching verification—lose effectiveness when fraudsters use stolen real data or split transaction amounts. Anti-fraud systems must evolve toward architectures that feature continuous learning and constant updates in response to new threats (Samson-Onuorah, 2023), a need that is particularly acute among SMEs (OECD, 2021).

On that basis, we propose an AI-based adaptive model delivered as a SaaS solution, organized into three stages: data input, processing, and output. Unlike traditional systems, which operate using predefined rules, the model is designed to adapt to constant changes in digital fraud.

During the input stage, the system collects information from each transaction to build a user behavior profile. The integrated variables are: amount, transaction frequency, geographic location, countries of origin and destination, user history, device used, and date and time. Combining these variables makes it possible to recognize typical behaviors and detect deviations associated with identity theft, unauthorized access, or unusual patterns.

The processing is organized into three interrelated layers: data acquisition, intelligent analysis, and results management. This study proposes a hybrid approach for intelligent analysis. Supervised learning recognizes recurring patterns based on labeled historical records (Hernández Aros et al., 2024); unsupervised learning identifies unusual behaviors not previously recorded, which is useful in international transactions where new patterns emerge. Samson-Onuorah (2023) notes that the most effective systems combine multiple analysis mechanisms, continuous monitoring, and ongoing updates. Through this combination, the system identifies common patterns, detects anomalies, assesses risk, and learns continuously.

The proposal's central feature is its adaptability: each transaction, confirmed alert, or detected fraud attempt can progressively adjust the analysis parameters. At the same time, the problem of “black boxes” (Hassija et al., 2024) is acknowledged; therefore, AI is viewed as a tool to

How to cite: Sánchez del Castillo, V. (2026). A Conceptual Ai-Based Adaptive Model for Fraud Detection in International Transactions: Innovations, Emerging Risks, and Applicability to Latin American Smes. *Journal of the Academy,* (15), 94-114. https://doi.org/10.47058/joa15.7

support decision-making rather than as a substitute for human judgment (Schmalzried et al., 2023; Tóth et al., 2023).

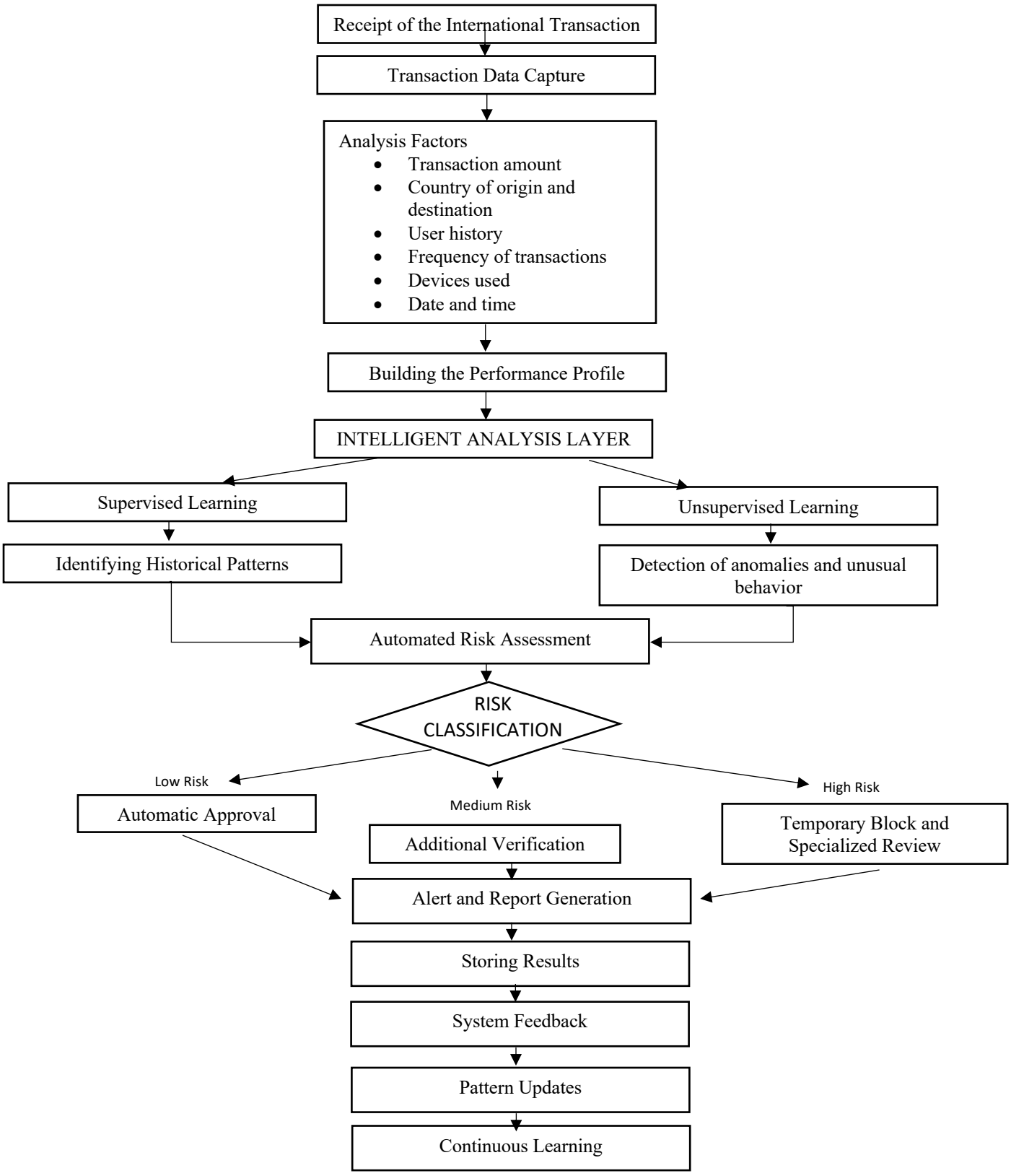
The risk classification system has three levels. High risk results in a temporary hold and a specialized manual review, without permanently canceling the transaction. Medium risk requires additional authentication or a brief verification check. Low risk allows for immediate approval. This classification focuses oversight on potentially risky transactions without significantly affecting legitimate users' experience.

As an output, the model generates real-time risk alerts, transaction classifications, automated responses, and reports for further analysis. The main contribution is the shift from static validation to behavioral analysis: instead of a permanent block, the system routes suspicious transactions to a priority review list, where an analyst can contact the customer for brief verification; if there is no response, automated messages are sent. This approach balances security and user experience. These are design properties that must be empirically verified.

Figure 1

Conceptual architecture of the AI-based anti-fraud model for SMEs

How to cite: Sánchez del Castillo, V. (2026). A Conceptual Ai-Based Adaptive Model for Fraud Detection in International Transactions: Innovations, Emerging Risks, and Applicability to Latin American Smes. *Journal of the Academy,* (15), 94-114. https://doi.org/10.47058/joa15.7



How to cite: Sánchez del Castillo, V. (2026). A Conceptual Ai-Based Adaptive Model for Fraud Detection in International Transactions: Innovations, Emerging Risks, and Applicability to Latin American Smes. *Journal of the Academy,* (15), 94-114. https://doi.org/10.47058/joa15.7

METHODOLOGY

This exploratory-descriptive study uses a mixed-methods approach that is predominantly qualitative. It was conducted in three complementary phases: a literature review on financial fraud and artificial intelligence; a descriptive analysis of the operational records of a remittance organization; and the conceptual design of an adaptive anti-fraud model under the SaaS model, theoretically validated against the gathered evidence.

It is important to clarify the scope from the outset. In this study, no algorithm was developed, trained, or tested using real data. Therefore, the model's performance—accuracy, reduction of false positives, response times—was not measured. This study presents design characteristics and expected benefits, subject to subsequent empirical validation. The only results observed come from the literature review and the organizational case study.

The literature review was narrative in nature, not systematic. The selection of sources was guided by an academic advisor and based on the author's prior knowledge and professional experience in fraud prevention. No formal protocol involving databases, search terms, or a selection flowchart was applied; consequently, the study does not claim that the search was exhaustive or reproducible. Scientific articles with DOIs published in journals specializing in finance, technology, and risk management were consulted, as well as documents from international organizations and regulatory bodies: OECD (2021), World Bank (Boeddu et al., 2021), Organización Mundial del Comercio (2024), Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, 2022), and CONDUSEF (2025). The criteria applied were thematic relevance, recency—with priority given to publications from the last five years—and the ability to identify authorship and verify the source. Institutional reports were used to assess the scale of the problem and contextualize the figures, not as evidence of the algorithms' performance.

The material was organized into four main areas: machine learning techniques applied to fraud detection; the use of AI for fraudulent purposes; explainability and human oversight within the Industry 5.0 framework; and conditions for technology adoption in SMEs.

How to cite: Sánchez del Castillo, V. (2026). A Conceptual Ai-Based Adaptive Model for Fraud Detection in International Transactions: Innovations, Emerging Risks, and Applicability to Latin American Smes. *Journal of the Academy,* (15), 94-114. https://doi.org/10.47058/joa15.7

Divergent viewpoints were compared: Hernández Aros et al. (2024) highlight machine learning's ability to identify complex patterns, while Hassija et al. (2024) and Černevičienė and Kabašinskas (2024) caution that complexity compromises transparency. This discussion supported positioning AI as a complement to human judgment rather than a substitute. A systematic review following the PRISMA protocol is proposed as a future line of research.

For the organizational case, we analyzed operational records from a transnational remittance organization that operates from the United States to Mexico, Colombia, Peru, and Chile. For confidentiality reasons, we are withholding its identity. The records cover October 2024 to January 15, 2025—about three and a half months, including the year-end holiday season. The author consolidated the monthly reports to obtain the totals for the period. She worked for over a year in the organization's fraud prevention and response department and was responsible for preparing and editing these reports. For this study, a collaborator who remains with the organization provided her only with the data strictly necessary, in aggregated form and without names, account numbers, or customer information. Due to their confidential nature, the original records cannot be disclosed or independently verified, which is acknowledged as a limitation.

The three figures in this case share the same unit of analysis: the call. An “interaction” is defined as a call handled through general customer service or support channels; a “fraud referral” is a monitored call whose case was transferred to the fraud department, where a cross-check was performed to validate a possible irregularity; and a “confirmed case” is a referral in which the cross-check confirmed fraud or in which the claim was formalized, according to the organization’s own criteria. Referrals that did not result in confirmed fraud are not considered, in their entirety, to be false positives. Based on the author’s experience, this group included service complaints, operational errors, false fraud alarms, and users who abandoned the verification process due to lack of time or delayed response. Since no quantitative breakdown is available, this group is referred to as “unconfirmed referrals.”

In addition, we reviewed more than 100 complaints to identify recurring types of fraud and seasonal patterns. This is a case review for exploratory purposes, not a statistically

How to cite: Sánchez del Castillo, V. (2026). A Conceptual Ai-Based Adaptive Model for Fraud Detection in International Transactions: Innovations, Emerging Risks, and Applicability to Latin American Smes. *Journal of the Academy,* (15), 94-114. https://doi.org/10.47058/joa15.7

representative sample. The author used observations from operational experience solely to interpret recurring behaviors and supplement the records, not to replace them.

Based on the above, the adaptive model was designed. The input variables were selected based on their frequency in the reviewed literature and their relationship to the fraud schemes observed in the case. The architecture was organized into three stages—input, processing, and output—using a hybrid approach combining supervised and unsupervised learning, as supported by Samson-Onuorah (2023) and Hernández Aros et al. (2024). The comparison involved verifying correspondence between each fraud vector identified in the case, each model component, and findings from the literature and specialized agencies. This is an assessment of theoretical consistency and not a predictive or empirical validation. The cost estimate was prepared using publicly available prices from technology providers consulted during the first half of 2025, based on the assumption of an SME with approximately 20 employees, and constitutes a preliminary approximation, not a cost-benefit analysis.

How to cite: Sánchez del Castillo, V. (2026). A Conceptual Ai-Based Adaptive Model for Fraud Detection in International Transactions: Innovations, Emerging Risks, and Applicability to Latin American Smes. *Journal of the Academy,* (15), 94-114. https://doi.org/10.47058/joa15.7

RESULTS

The organization under analysis acts as a conduit for high-volume financial flows from the United States to Latin America. Between October 2024 and January 15, 2025, the figures summarized in Table 1 were recorded.

Table 1

Operational indicators for the case (October 2024 to January 15, 2025)

Metric	Records	Ratio
Interactions handled through service channels	256,943	100%
Referrals to the fraud department for verification	103,720	40.37% of interactions
Confirmed cases of fraud	34,782	33.53% of referrals; 13.54% of interactions
Referrals not confirmed as fraud	68,938	66.47% of referrals

Note. Prepared in-house using aggregated and anonymized data from a remittance organization whose identity is being withheld.

Four out of every ten monitored calls were referred to the fraud department, but only one out of every three referrals was confirmed as fraud. This data reveals a structural inefficiency: the organization's rules-based system flagged many cases that, upon review, did not constitute fraud. As explained in the methodology, this group does not entirely correspond to false positives, because it includes service complaints, operational errors, and users who abandoned the process.

Abandonment warrants its own attention. According to the author's observations, several flagged customers decided not to continue the verification process because they lacked time or faced slow response times. Regarding processing times, the organization communicated a 21-day refund policy to staff, but the department responsible for processing refunds often took more than two months to validate claim eligibility. These timeframes are based on the author's direct experience and not on the records analyzed.

How to cite: Sánchez del Castillo, V. (2026). A Conceptual Ai-Based Adaptive Model for Fraud Detection in International Transactions: Innovations, Emerging Risks, and Applicability to Latin American Smes. *Journal of the Academy,* (15), 94-114. https://doi.org/10.47058/joa15.7

A qualitative analysis of the complaints showed that criminal networks did not seek to circumvent the system's code, but rather to exploit user psychology and biases. Four recurring types of social engineering were identified. The first, known as a "relationship scam," involves prolonged emotional manipulation in which the scammer builds trust to request money transfers under the pretext of medical emergencies or the purchase of travel tickets. The second is e-commerce fraud, which involves fraudulent websites that steal money by offering nonexistent products. The third involves fake discounts, which pressure victims by threatening to immediately cut off essential services unless they make a quick deposit in exchange for a supposed discount. The fourth, and most aggressive, is the immigration scam: fraudsters use real personal data, obtained from previous data breaches, to impersonate government agency officials and force immediate money transfers under threat of deportation.

The amounts defrauded did not follow a specific pattern; fraudsters diversified them to circumvent established limits. However, seasonality was observed, with spikes on dates marked by high transaction volumes and emotional significance—such as Christmas, Mother's Day, and the Super Bowl—as well as during political and social events in each destination country. The quantitative period analyzed covers only the year-end; spikes on other dates are observations by the author that were not quantified in this study.

Table 2 lists each observed fraud vector, the limitation of the traditional system, and the component of the proposed model designed to address it.

Table 2

Observed fraud vectors and components of the proposed model

Observed vector	**Limitations of the rule-based system**	**Component of the proposed model (design)**
Impersonation using real data and immigration scams	Manual verification of name matches—useless if the criminal already has the actual data	Real-time multifactorial assessment (IP geolocation, device metadata, history); priority review list and brief contact with the customer

How to cite: Sánchez del Castillo, V. (2026). A Conceptual Ai-Based Adaptive Model for Fraud Detection in International Transactions: Innovations, Emerging Risks, and Applicability to Latin American Smes. *Journal of the Academy,* (15), 94-114. https://doi.org/10.47058/joa15.7

Diversified amounts	Fixed monetary thresholds	Individual behavioral profile: deviation from the user's usual pattern is assessed
Seasonal spikes	Staff overload and burnout during critical periods	Supervised learning using historical seasonality; expedited approval of low-risk transactions
Relationship scams	Fixed rules do not trigger alerts	Unsupervised learning that calculates deviations from typical behavior
New users with no history	No comparison reference	Profile built starting with the first transaction; initial baseline available starting with the second
Friction-driven churn	Slow manual review and indiscriminate blocking	Classification by risk level, priority review, and automated contact messages

Note. Prepared by the author based on the case study and the reviewed literature.

Two aspects are worth explaining. First, when the algorithm detects something unusual, the transaction is not automatically canceled: it is moved to a priority review list, where an analyst can contact the customer for a brief verification interview lasting no more than five minutes; if there is no response, the system sends automated emails or messages prompting the user to get in touch, thereby protecting the funds without triggering a definitive rejection. Second, in a so-called "cold start," the model begins building the profile from the first transaction, and by the second transaction, it already has a frame of reference. This foundation is enriched by human interaction, because during interviews, customers often voluntarily reveal the purpose of the transaction—information that the analyst records and uses to provide feedback to the algorithm.

To estimate costs, publicly available prices from technology providers were reviewed during the first half of 2025 (Amazon Web Services, 2026; Bitdefender, 2026; CrowdStrike, 2026; Forter, 2025; Google Cloud, n.d.; Microsoft Security, n.d.; Mimecast, 2026; Proofpoint, 2026; Riskified, 2026; SEON, n.d.; SentinelOne, n.d.), and these were compared with market reports (McKinsey, 2022; Statista, 2025) and recent studies (Samson-Onuorah, 2023;

Hernández Aros et al., 2024). The reference scenario is an SME with approximately 20 employees. Table 3 summarizes the results.

Table 3

Estimated Costs of Cybersecurity Protection for SMEs (USD)

Concept	**Estimated cost**	**Risks if not implemented**	**Impact on International Business**
Endpoint protection (EDR)	15–25 per user/month	Malware, data theft	Loss of critical information and customers
Email security (anti-phishing)	5–15 per user/month	Phishing, financial fraud	Fraudulent international transfers
Multifactor authentication (MFA)	Low or free	Identity theft	Unauthorized access to financial systems
Cloud backup	100–300 per month	Total data loss	Disruption of international operations
Anti-fraud SaaS (AI-powered detection)	20–100 per month, depending on usage	Undetected fraud	Direct financial losses
Continuous monitoring	1,000 per month	Prolonged, undetected attacks	Reputational and financial damage
Cost of a fraud incident	N/A	10,000–100,000 or more per incident	Loss of global competitiveness or bankruptcy

Note. Prepared by the author based on OECD (2021), World Bank (Boeddu et al., 2021), and published prices from providers consulted during the first half of 2025. The figures are reference estimates and vary by provider, plan, and usage volume. The range of costs per incident is taken from the World Bank (Boeddu et al., 2021) and CONDUSEF (2025).

Based on these assumptions, a package that includes all the items in the table—except for the cost per incident—would total between $1,520 and $2,200 per month for an SME with 20 employees. This range excludes integration, training, and maintenance costs and includes continuous monitoring, the most expensive component. An SME that limits itself to basic protection—multi-factor authentication, secure email, and anti-fraud SaaS—would significantly reduce that figure. Even so, the reference range for the cost of a single incident

far exceeds the estimated investment. This is an illustrative comparison: it does not constitute a cost-benefit analysis nor does it, on its own, demonstrate the economic viability of the complete model.

DISCUSSION OF RESULTS

The case study results and the reviewed literature suggest that AI has improved financial fraud detection but has also enabled new types of attacks. This aligns with the duality described by Kshetri (2021) and the World Bank's warnings (Boeddu et al., 2021). The case analyzed adds a nuance: even without technological sophistication on the attacker's part, fraud thrives because it exploits victims' trust, sense of urgency, and emotional vulnerability, and because a system of fixed rules ultimately affects legitimate customers as well, causing them to abandon the process.

From a theoretical perspective, the study suggests that the discussion of anti-fraud models should not be limited to predictive performance or explainability. The friction legitimate users experience and the behavioral dimension of fraud are design variables that receive little attention in the reviewed literature and are linked here to the Industry 5.0 approach (Schmalzried et al., 2023; Tóth et al., 2023). We also propose distinguishing between alerts, referrals, complaints, and confirmed fraud—a distinction necessary to avoid treating everything unconfirmed as a false positive.

Practically, for an SME, the model suggests protection can begin with SaaS solutions and low-cost measures, without building proprietary infrastructure. For providers of these services, the case study shows the value of recording why a referral is not confirmed—error, disagreement, abandonment, false alarm—since this data would allow measurement of the actual false positive rate and better model training. As a next step, it would be advisable to conduct a pilot test using real data to measure accuracy, sensitivity, the false positive rate, the abandonment rate, and resolution time compared to a rule-based system.

In Mexico and Latin America, SMEs are highly vulnerable to sophisticated AI-driven fraud, largely because of limited technological infrastructure and access to advanced systems

How to cite: Sánchez del Castillo, V. (2026). A Conceptual Ai-Based Adaptive Model for Fraud Detection in International Transactions: Innovations, Emerging Risks, and Applicability to Latin American Smes. *Journal of the Academy,* (15), 94-114. https://doi.org/10.47058/joa15.7

(OECD, 2021). Anti-fraud SaaS platforms offer an accessible alternative: they enable detection of unusual activity, real-time monitoring, and automatic alerts without proprietary infrastructure. Adopting intelligent, adaptive models is expected to reduce financial losses and improve operational efficiency; however, empirical evidence must support this expectation.

Since fraud is not solely due to technological failures, AI-based models must be complemented by awareness-raising strategies, digital training, and comprehensive risk management. Training programs should cover phishing and social engineering, ethics and regulatory compliance, corporate fraud prevention, and detecting deepfakes and AI-assisted fraud. It is also advisable to develop digital and financial literacy skills to identify red flags, such as fear-mongering, requests for verification codes, implausible offers, and communications with a sense of urgency.

Complementary, low-cost strategies include basic cybersecurity training for staff, multi-factor authentication, and simple access control policies. This trend aligns with findings documented by PwC (2024) regarding the increase in cybersecurity investment by SMEs globally. Samson-Onuorah (2023) adds that, beyond the initial cost, these systems require feedback loops to be updated as fraudsters' tactics evolve.

How to cite: Sánchez del Castillo, V. (2026). A Conceptual Ai-Based Adaptive Model for Fraud Detection in International Transactions: Innovations, Emerging Risks, and Applicability to Latin American Smes. *Journal of the Academy,* (15), 94-114. https://doi.org/10.47058/joa15.7

CONCLUSIONS

With regard to the research question, we conclude that an adaptive model combining supervised learning, unsupervised learning, and human review constitutes a conceptually sound alternative for strengthening fraud detection in international transactions by Latin American SMEs. This conclusion is based on the consistency between the proposed design, the reviewed literature, and the operational case analyzed, rather than on a performance test.

The study found the following: Over three and a half months, 40.37% of a remittance organization's interactions were referred to the fraud department, and only 33.53% of those referrals were confirmed as fraud, while a portion of the remainder was lost due to abandonment. The identified scams exploited the human factor more than the infrastructure. The proposed solution, however, is an architecture for input, processing, and output—with tiered risk classification and prioritized review—designed to reduce friction with legitimate customers. Its effectiveness and economic viability require further empirical testing.

AI is now a strategic resource for preventing fraud in international business, but its dual nature poses a structural challenge: it strengthens defenses while also being exploited by malicious actors to launch more sophisticated attacks. This situation leaves SMEs particularly vulnerable, although the SaaS model offers a more accessible path to security mechanisms without unduly straining their resources. In a context where fraud is constantly evolving, integrating technological solutions, personal data protection, and human analytical judgment will remain a central challenge to the operational sustainability of SMEs in international trade.

The model was not developed, trained, or tested using real data; therefore, its benefits are expected but not proven, and the comparison made is based on theoretical consistency. The case data come from a single organization, cover a period of three and a half months, and are confidential; thus, they cannot be independently verified or generalized. Observations regarding seasonality outside the year-end closing and reimbursement times are based on the author's direct experience. The literature review was narrative in nature and did not follow a systematic protocol. Fieldwork was limited: it was not possible to interview a broad group of people, and direct knowledge is restricted to a few SMEs who have been victims of fraud.

How to cite: Sánchez del Castillo, V. (2026). A Conceptual Ai-Based Adaptive Model for Fraud Detection in International Transactions: Innovations, Emerging Risks, and Applicability to Latin American Smes. *Journal of the Academy,* (15), 94-114. https://doi.org/10.47058/joa15.7

The author previously worked at the organization whose aggregated data are analyzed in the case study and currently has no relationship with it. She declares that she has no other conflicts of interest. This research has not received any funding. Writing assistance tools were used during the preparation of the article; the author is responsible for the ideas, analysis, and conclusions.

How to cite: Sánchez del Castillo, V. (2026). A Conceptual Ai-Based Adaptive Model for Fraud Detection in International Transactions: Innovations, Emerging Risks, and Applicability to Latin American Smes. *Journal of the Academy,* (15), 94-114. https://doi.org/10.47058/joa15.7

REFERENCES

Amazon Web Services. (2026). *AWS Backup pricing*. https://aws.amazon.com/backup/pricing/

Bitdefender. (2026). *Está explorando las soluciones de seguridad de Bitdefender GravityZone*. https://www.bitdefender.com/es-es/business/campaign/new-compare50

Boeddu, G. L., Chien, J., Grady, R. C., & Istuk, I. (2021). *Consumer Risks in Fintech - New Manifestations of Consumer Risks and Emerging Regulatory Approaches: Policy Research Paper (English)*. World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/515771621921739154

Černevičienė, J., & Kabašinskas, A. (2024). Explainable artificial intelligence (XAI) in finance: a systematic literature review. *Artificial Intelligence Review*, *57*(216). https://doi.org/10.1007/s10462-024-10854-8

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros - CONDUSEF. (2025). *Comercio Electrónico — Estadísticas*. https://www.condusef.gob.mx/index.php/necesitas-ayuda?p=estadisticas

CrowdStrike. (2026). *Tailored bundles to stop breaches*. https://www.crowdstrike.com/pricing/

Forter. (2025). *Contact Sales – Forter*. https://www.forter.com/pricing/

Google Cloud. (s.f.). *Precios de Cloud Storage*. https://cloud.google.com/storage/pricing

Hassija, V., Chamola, V., Mahapatra, A., Singal, A., Goel, D., Huang, K., Scardapane, S., Spinelli, I., Mahmud, M., & Hussain, A. (2024). Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence. *Cognitive Computation*, *16*(1), 45–74. https://doi.org/10.1007/s12559-023-10179-8

Hernández Aros, L., Bustamante Molano, L. X., Gutiérrez-Portela, F., Moreno Hernández, J. J., & Rodríguez Barrero, M. S. (2024). Financial fraud detection through the application of machine learning techniques: a literature review. *Humanities and Social Sciences Communications*, *11*(1130). https://doi.org/10.1057/s41599-024-03606-0

Kshetri, N. (2021). The role of artificial intelligence in promoting financial inclusion in developing countries. *Journal of Global Information Technology Management*, *24*(1), 1–6. https://doi.org/10.1080/1097198X.2021.1871273

McKinsey. (2022). *The State of AI in 2022—and a Half Decade in Review*. QuantumBlack. https://www.mckinsey.com/~/media/mckinsey/business%20functions/quantumblack/our%20insights/the%20state%20of%20ai%20in%202022%20and%20a%20half%20decade%20in%20review/the-state-of-ai-in-2022-and-a-half-decade-in-review.pdf?shouldIndex=false

Microsoft Security. (n.d.). *Why Microsoft Security Secure from end to end*. https://www.microsoft.com/en-us/security

Mimecast. (2026). *Mimecast Plans to Mitigate Human Risk*. https://www.mimecast.com/products/mimecast-plans/

Oficina de las Naciones Unidas contra la Droga y el Delito - UNODC. (2022). *Compendio de Ciberdelincuencia Organizada*. Naciones Unidas. https://www.unodc.org/documents/Cybercrime/publications/compendio_de_delincuencia_organizada_es.pdf?v=3.6digest_cyber_organized_crime_2nd_ed.pdf?v=3.6

Organización Mundial del Comercio. (2024). *Informe sobre el comercio mundial 2024 — Comercio e inclusividad: Por un comercio que beneficie a todos*. https://www.wto.org/spanish/res_s/publications_s/wtr24_s.htm

Organización para la Cooperación y el Desarrollo Económicos (OECD). (2021). *The digital transformation of SMEs*. OECD Publishing. https://doi.org/10.1787/bdb9256a-en

Passos, L. A., Jodas, D., Costa, K. A. P., Souza Júnior, L. A., Rodrigues, D., Del Ser, J., Camacho, D., & Papa, J. P. (2024). A review of deep learning-based approaches for deepfake content detection. *Expert Systems*, *41*(8), e13570. https://doi.org/10.1111/exsy.13570

Proofpoint. (2026). *Complete Microsoft 365 Security for MSPs*. https://www.proofpoint.com/us/partners/msp

PwC. (2024). *Global Economic Crime Survey 2024. Meeting tomorrow's challenges, embracing risk intelligently*. PricewaterhouseCoopers. https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

Riskified. (2026). *AI fraud prevention fueling ecommerce success.* https://www.riskified.com/

Samson-Onuorah, C. I. (2023). Data-driven fraud detection frameworks integrating machine learning, transaction monitoring, and governance across modern banking platforms. *International*

Journal of Research in Finance and Management, *6*(2), 318–329. https://doi.org/10.33545/26175754.2023.v6.i2c.670

Schmalzried, D., Hurst, M., Wentzien, M., & Gräser, M. (2023). Analyse der Rolle Künstlicher Intelligenz für eine menschenzentrierte Industrie 5.0. *HMD Praxis der Wirtschaftsinformatik*, *60*, 1143–1155. https://doi.org/10.1365/s40702-023-01001-y

SentinelOne. (n.d.). *PRICING & PACKAGES. Secure More. Spend Less*. https://www.sentinelone.com/pricing/

SEON. (n.d.). *Pricing Plans. Select a Plan That Best Fits Your Needs*. https://seon.io/pricing/

Statista. (2025). *E-commerce fraud* - statistics & facts. https://www.statista.com/topics/9240/e-commerce-fraud/

Tóth, A., Nagy, L., Kennedy, R., Bohuš, B., Abonyi, J., & Ruppert, T. (2023). The human-centric Industry 5.0 collaboration architecture. *MethodsX*, *11*, 102260. https://doi.org/10.1016/j.mex.2023.102260