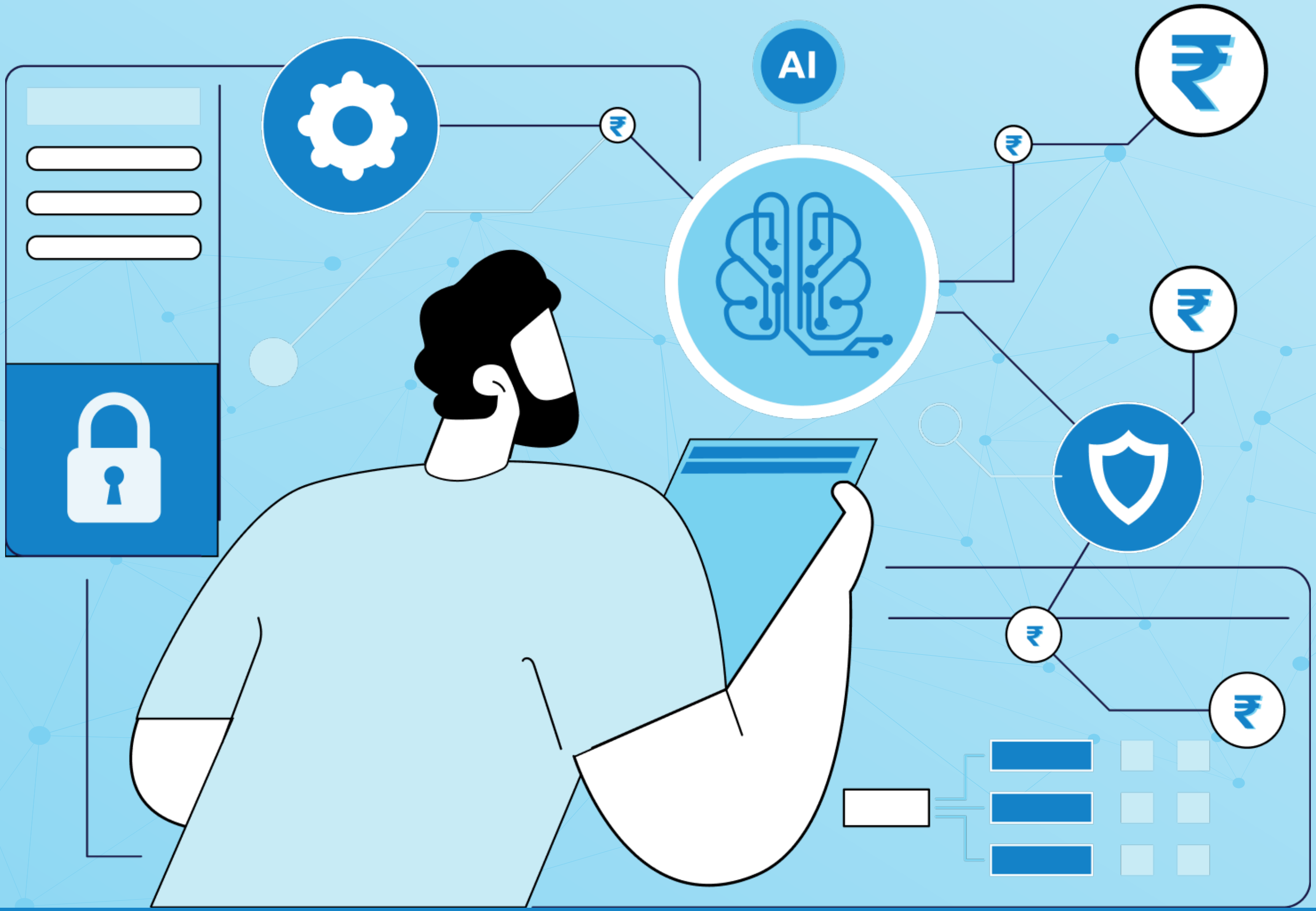
Innovation in every *byte*

Building Trust in Digital Payments



Content

Building Trust in Digital Payments: The Need for Predictive Fraud Prevention

Trust is at the foundation of the real-time digital payments' economy. As UPI payment volumes soar and e-commerce platforms proliferate, fraudsters are seizing opportunities to exploit vulnerabilities on an unprecedented scale. While transaction-level fraud, is largely mitigated by checks such as two-factor authentication (2FA), merchant-level fraud presents a much larger threat, with far-reaching implications for payment service providers.

Merchant-Level Fraud and Its Complexities

Robust merchant onboarding processes are critical for fraud prevention and preserving the integrity of the payment ecosystem. However, identifying fraudulent merchants is becoming increasingly complex. Today, malicious actors can create convincing digital storefronts in mere minutes, using platforms to sell counterfeit goods, distribute illicit products, or launder money—all while maintaining a facade of legitimacy.

Merchant-Level Fraud Can Take Multiple Forms, Including:

- ✓ **Fake businesses** posing as legitimate operations.
- ✓ **Restricted or prohibited businesses** misrepresenting their industry classification.
- ✓ **Bust-out fraud,** where merchants establish accounts, rapidly process transactions, and disappear before chargebacks occur.
- ✓ **Transaction laundering,** in which illicit businesses process unauthorized payments through legitimate merchant accounts.
- ✓ **Identity fraud,** including assuming an existing merchant's identity or creating a new, fake one altogether.
- ✓ **Collusive fraud,** where legitimate merchants such as factoring (allowing unapproved affiliates to use their payment credentials) or engaging in money laundering/tax evasion.

These activities endanger consumers & expose acquirers to significant financial & reputational risks.

The Acquirer's Dilemma: Balancing Growth & Risk

Acquirers navigate a dual role—supporting legitimate merchants while safeguarding against fraud, compliance violations, and financial crimes. The exposure to these risks depends on their operating environment and risk assessment maturity. However, the acquiring model presents a challenge: while revenue comes from transaction fees, losses from fraud, fines, or non-compliance are based on total transaction value.

To sustain a secure ecosystem, acquirers must implement stringent underwriting and fraud prevention measures that comply with regulations and payment schemes. At the same time, to effectively combat merchant fraud, acquirers must integrate advanced risk assessment tools with robust regulatory governance frameworks and a deep understanding of payment scheme rules, to reduce their exposure to fraud while maintaining a smooth and efficient operational flow.

The Shortcomings of Traditional Fraud Detection

Digital merchant transactions generate massive volumes of data daily. Given the scale, speed, and complexity of modern payments, traditional fraud detection methods—primarily reliant on static rule-based systems—often fall short. While these systems provide a foundational level of protection, they have several critical limitations:

Limited Adaptability: As fraud tactics evolve quickly, static rules become ineffective, leaving systems vulnerable to emerging threats.

High False Positive Rates: Fixed rules can trigger unnecessary alerts resulting in inefficiencies that can burden organizations with unnecessary investigations and disruptions to legitimate transactions

Inability To Integrate Diverse Data Sources: Traditional systems struggle to incorporate signals from multiple sources, weakening their detection capabilities. These systems lack the profiling methods to assess complex transaction behaviours, potentially missing subtle fraudulent activities.

The Shift from Rule-Based to AI-Powered Fraud Detection

Traditional rule-based systems operate on fixed criteria, which can become ineffective as fraud tactics evolve. In contrast, advanced Artificial Intelligence (AI) and Machine Learning (ML) tools can discern underlying patterns by dynamically adjusting rules to enhance fraud detection, reduce chargebacks, and increase the approval of legitimate transactions. As an example, a rule-based system may set up 100 rules but an AI-based system may learn from data patterns to discern new frauds and create new rules.

Preemptive Monitoring

AI-ML models detect complex, nonlinear relationships, improving risk assessment accuracy. For instance, AI can dynamically adjust transaction thresholds based on observed volume trends, proactively preventing fraud. Similarly, while traditional systems flag dormant accounts, AI predicts dormancy likelihood, enabling preemptive intervention.

Optimized Variable Selection

Robust, data-driven models that integrate ML algorithms with Big Data analytics efficiently handle vast amounts of data that enhance decision-making. : AI can automate decision-making processes in fraud case management, such as flagging suspicious transactions for review or blocking potentially fraudulent activities. This automation speeds up the detection and response process, reducing the time it takes to mitigate fraud.

Richer Data Segmentation

Machine Learning enables granular data segmentation to analyse numerous attributes. Utilizing unsupervised learning techniques, such as clustering, allows for the identification of subtle patterns and anomalies, thereby improving model accuracy and explanatory power.

Scalability and Efficiency

As transaction volumes increase, traditional systems may struggle to keep up. AI and ML-based solutions offer unparalleled scalability, efficiently handling large datasets without compromising performance. This scalability ensures that fraud detection systems can accommodate growth in transaction volume, maintaining effectiveness across various operational scales.

Applications of AI

Monitoring Health of Merchant Portfolio

Traditionally, regulatory guidelines have required acquirers to perform periodic merchant reviews at set intervals. However, these periodic checks may leave exploitable gaps between cycles. Acquirers can enhance their revenue and portfolio health by implementing continuous monitoring systems that utilize AI-driven models to assess merchant risk and assign trust scores. These models synthesize data from multiple sources—including Know Your Business (KYB) documents, merchant business and transaction records (such as chargeback and refund data), watch lists, and social sentiment—to evaluate each merchant during onboarding and throughout their engagement. Trust scores are continually updated, enhancing the overall health and profitability of their merchant portfolios.

Fraudulent merchants may attempt to circumvent Know Your Customer (KYC) efforts and avoid acquirer scrutiny by establishing storefront websites that fall into "low-risk" merchant categories. This deceptive practice enables illegal businesses—such as those involved in unlawful gaming—to mask their operations by using fake or stolen identities or creating bogus online storefronts to obtain merchant accounts.

After passing initial KYC checks and establishing their merchant accounts, these criminals begin retailing illegal products and services. The proliferation of micro-merchants, coupled with an explosion of transactions and data overload, makes it challenging to detect merchants whose Merchant Category Codes (MCC) do not correspond to their actual activities. By integrating AI into KYC processes, financial institutions can achieve more efficient, cost-effective, and secure systems, ultimately benefiting both the organization and its customers.

Implementing AI-driven monitoring systems can significantly reduce the high costs associated with traditional KYC processes. By automating data collection and verification, AI enhances efficiency, accuracy, and security, leading to substantial cost savings.

Identity Swap and Transaction Laundering

Transaction laundering is a growing concern in the payments industry, involving unauthorized businesses processing transactions through the payment credentials of approved merchants without the acquirer's knowledge. These entities may appear legitimate initially and might not trigger immediate chargeback issues; however, regulators mandate that acquirers perform comprehensive due diligence to prevent the approval of such fraudulent accounts. Failing to detect and halt these activities can result in severe penalties, including substantial fines and significant reputational harm.

Artificial Intelligence (AI) based risk intelligence platforms can combat transaction laundering by analyzing data from mystery shopping alongside transaction records. By monitoring critical transaction parameters—such as time, frequency, and amount—AI systems can identify unusual patterns indicative of fraudulent behavior. For instance, AI can detect anomalies like high-value transactions occurring at atypical hours for a business that usually operates during standard daytime hours, signaling potential illicit activity.

Transaction Monitoring and Scoring

Acquirers can proactively identify anomalies by monitoring multiple risk indicators, including transaction volume, velocity, time of day, and merchant category. Sudden spikes in transaction amounts or frequency, unusual transaction timings, and discrepancies between a merchant's registered business type and transaction patterns can signal potential fraud. Artificial Intelligence (AI)-driven behavioral models analyse these parameters to assign a trust score to each transaction, enabling acquirers to mitigate fraud risks while reducing false positives and ensuring a seamless payment experience for legitimate merchants.

Staying a Step Ahead of Fraud

Acquirers must take proactive steps to combat fraud within their merchant network. Relying solely on in-house tools can be costly and less effective against sophisticated fraud schemes. Partnering with a specialized PayTech firm that understands the evolving fraud landscape is crucial.

NPST's Risk Intelligent Decisioning Platform empowers acquirers to detect fraudulent merchants early, preventing money laundering and illicit activities from infiltrating the payment ecosystem.

Offered as an As-a-Service model, this AI-driven platform continuously analyzes vast datasets, leveraging machine learning to identify hidden risks and emerging fraud patterns in real time.

About NPST

Founded in 2013, NPST is a leading fintech firm in India, part of the Make in India initiative and listed on the NSE Small and Medium Exchange. We specialize in UPI payments and digital banking, operating as both a Technology Service Provider (TSP) and a Payment Platform as a Service Provider (PPaaS). Our solutions include online and offline transaction processing, banking super apps, fraud prevention, dispute management, and compliance technology.

Our mission is to deliver technology solutions across the financial value chain — serving banks, fintechs, and other industry players — and drive the growth of the digital payments ecosystem. NPST supports over 100 clients and processes more than 60 million transactions daily, advancing businesses, individuals, communities, and economies through its innovative technology.

NPST
Innovation in every *byte*

Network People Services Technologies Ltd.

427/428/429, A-Wing, NSIL, Lodha Supremus
II,Near New Passport office, Road No. 22,
Wagle Industrial Estate, Thane (W) – 400604

Email: vv, sales@npstx.com