INETCO BullzAI

How leading acquirers reduce exposure to card network enforcement actions

Card scheme penalties have changed

Card scheme penalty programs are changing fast. Driven by rising payment fraud, card testing attacks and dispute volumes, networks like Visa, Mastercard and American Express are enforcing stricter thresholds that expose merchants, processors and banks (acquirers) to fines for excessive declines, card scheme message errors, fraud and chargebacks. Typically, acquirers can't simply block transactions outright. The final risk and credit decision sits with the issuer.

So has the way risk is measured

Historically, card scheme penalty programs were based on rule violations at the individual merchant level. Today, programs like the Visa Acquirer Monitoring Program (VAMP) have fundamentally changed the model, introducing portfolio-wide accountability. A single fraud and dispute threshold now applies across all card-not-present (CNP) transactions, meaning performance is judged at the aggregate level, not merchant by merchant.

As of January 2026, acquirers must maintain a combined fraud and dispute ratio below **0.5% of total transaction volume**. Breach that threshold and the entire portfolio is at risk, exposing acquirers to penalties, heightened network scrutiny and potential operational restrictions.

At the same time, card networks now target card testing attacks — high-volume, bot-driven authorization attempts — through a separate enumeration ratio that can independently trigger monitoring, fines and assessments.

Blocking transactions that trigger scheme penalties in real time is key to staying compliant

Staying below fraud, dispute and enumeration thresholds and adhering to scheme-penalty conditions requires a shift from reactive response to proactive control.

Acquirers need to:

- **Invest in automated detection and precision blocking to stop transactions that trigger scheme penalties without increasing false positives**
- **Create a real-time, field-level view across authorization and clearing transactions**
- **Continuously monitor CNP transaction activity in real time**
- **Identify "borderline" merchant behavior before it becomes non-compliant**
- **Detect emerging risk signals such as retries, suspicious payment patterns, enumeration attacks and card scheme message errors before they impact portfolio ratios**
- **Provide defensible, auditable data for card scheme dispute management**

A single attack can now impact your entire portfolio

Portfolio-level accountability changes everything. A handful of bad merchants or a single bot-driven card testing attack can push an acquirer's entire portfolio over card scheme thresholds. The consequences escalate quickly: monthly fines scaling to $50,000 - $100,000+, forced entry into compliance monitoring programs, added operational cost and audit complexity, and even risk of license termination. The onus is on acquirers to detect and stop fraudulent transactions in real time without impacting legitimate customer activity and merchant revenue.

Relying on issuers to defend the integrity of payment transactions is no longer enough

By the time an offending transaction is identified at the issuer level, the transaction has already moved through the acquiring environment, increasing risk of card scheme penalties, fraud loss and customer friction.

Acquirers are now expected to detect and stop suspicious activity earlier in the transaction lifecycle across ATM, POS and digital channels while minimizing false positives.

Common threats include:

- **Card testing bot attacks that precede fraud**
- **Mismatched billing descriptors leading to disputes**
- **"Free trial" subscription traps generating chargebacks**
- **Velocity spikes in new merchants indicating bust-out fraud**
- **Cross-border mishandling of CNP transactions**

Key takeaway

- **Scheme penalties are rarely caused by isolated incidents. They are the result of issues that go undetected.**
- **Real-time visibility, automated fraud detection and precision blocking allow acquirers to identify payment fraud, enumeration attacks and card scheme message errors earlier, respond faster and reduce compliance risk.**

What AI-driven prevention changes

A modern, AI-driven payment transaction monitoring solution such as **INETCO BullzAI** automates real-time detection and prevention, enabling acquirers to block suspicious activity before authorization and reduce exposure to chargebacks, penalties and fraud loss.

With adaptive AI:

- **Risk scores and behavioral models update continuously for every in-flight transaction**
- **Behavioral drift and anomalies are pre-emptively detected across individual merchants, cards, devices and terminals**
- **Suspicious activity and compromised terminals or devices can be blocked with precision at the transaction level without increasing false positives**
- **Explainable AI and intelligent agents accelerate investigation and decision making**
- **Response code errors, missing or mismatched field errors, connectivity issues, unexpected declines and recurring retry loops are instantly flagged and remediated**

INETCO BullzAI enables precise, real-time intervention, blocking transactions that trigger scheme penalties instantly without introducing customer friction. Acquirers are empowered to automatically detect and block high risk transactions before card scheme thresholds are reached, while gaining access to defensible, auditable data to support card scheme dispute management and chargebacks. The result is earlier identification of transaction issues, blocking of suspicious activity and reduced risk of triggering card scheme penalties.

Ready to take action before penalties, fraud losses or customer friction impact your business?
Contact sales@inetco.com