



First Party Fraud, Chargeback Abuse and the Acquirer Visibility Gap

For Safer Merchant Payments



Trudenty

trudenty.com

SECTION 01

Executive Thesis.

Acquirers sit at the centre of a fraud ecosystem they can only partially see. The merchant fraud intelligence flowing through their portfolio every day — **chargeback patterns, refund abuse, first-party misuse** — carries signals relevant to mule detection and APP fraud that are not reaching the institutions that need them.

The visibility gap is structural, not technical. Closing it requires intelligence that crosses perimeters without moving raw data.

SECTION 02

Key Findings.

01

First-party fraud is not a merchant problem. It is an ecosystem problem.

Industry estimates place first-party misuse at 75–86% of all chargebacks — not stolen cards, not account takeover, but consumers knowingly exploiting the dispute process. The same individual filing repeated INR claims across a merchant portfolio may carry a behavioural profile relevant to mule risk at their bank. The merchant fraud layer and the banking fraud layer are connected; acquirers see the former in detail.

03

Scheme ratio pressure is intensifying and the rules are changing.

Visa's VAMP regime, live since April 2025, merged fraud and dispute monitoring into a single ratio with tightening thresholds. Phase 2 thresholds from January 2026 set merchants at 1.5% above standard and 0.9% excessive. TC40 alerts resolved via Rapid Dispute Resolution now count toward VAMP ratios; Mastercard's SMMP, effective July 2026, mandates 72-hour investigation of flagged merchants and immediate termination where scam activity is confirmed.

02

Acquirers can see their merchants. They cannot see the consumer on the other side.

An acquirer has visibility of transaction data, dispute patterns and chargeback volumes across their merchant portfolio. They have almost no visibility into the consumer's behaviour across other merchants, other acquirers, or the banking system. When a consumer with a history of refund abuse initiates a payment, that history is invisible to the acquirer processing it.

04

Chargeback tooling addresses the dispute. It does not prevent it.

Most chargeback management focuses on representment, evidence packs and ratio management after the dispute has happened. Dispute tools that process claims efficiently do not stop the same consumer from returning. Without behavioural intelligence spanning the consumer's activity across the ecosystem, acquirers are managing the symptom rather than the exposure — the fraud infrastructure stays intact.

SECTION 03

Why This Matters to Acquirers.

VAMP and SMMP create direct commercial pressure. Acquirers bear scheme liability for merchants that breach thresholds. The cost of remediation, restricted processing or termination falls upstream. Earlier fraud intelligence reduces that exposure — and the RDR/VAMP interaction means getting fraud-coding right before the ratio moves matters more than ever.

EVIDENCE · METRICS

75% – 86%

First-party misuse share of all chargebacks reported under fraud reason codes — consumers knowingly exploiting the dispute process, not stolen cards or account takeover.

FINDING 1 · SOURCE ¹

\$4.61

Real cost to US merchants for every \$1 of fraud loss, once fees, product cost and overhead are factored in. A 32% increase since 2022.

FINDING 1 · SOURCE ²

19% · 1 in 3

Year-on-year increase in chargeback fraud in 2024; one in three merchants worldwide hit by chargeback fraud in some form.

FINDING 1 · SOURCES ^{4, 6}

SECTION 04

Adoption & Regulation.

ADOPTION PATTERNS OBSERVED

Acquirers are exploring how cross-ecosystem trust intelligence can close the visibility gap — connecting merchant-side fraud signals with risk intelligence from the banking layer.

REGULATORY / INDUSTRY DIRECTION

- **Visa VAMP:** Phase 1 live April 2025; Phase 2 thresholds from January 2026 (1.5% standard, 0.9% excessive); TC40/RDR change from March 2025. ⁵
- **Mastercard SMMP:** effective July 2026; 72-hour investigation of flagged merchants, immediate termination where scam activity is confirmed. ³

SECTION 05

Common Blockers.

SECURITY

Centralised signal pooling concentrates risk across the participating network.

DATA & CONSENT

GDPR and EEA residency rule out raw data sharing; federated architectures keep raw data inside each environment.

INTEGRATION

Acquirer fraud stacks process disputes, not external pre-auth signals; cross-ecosystem intelligence requires re-architecture.

GOVERNANCE

Acquirer and merchant data must not leave the regulated perimeter.

SECTION 06

What Is Not Working Today.

01

Chargeback processing is reactive by design. By the time a dispute is filed, the acquirer is managing a loss, not preventing one.

02

Consumer behaviour is invisible across the portfolio. An acquirer can see a merchant's chargeback ratio — not that the same consumer is driving disputes across multiple merchants.

03

Merchant-side fraud signals are not connected to the banking layer. Refund abuse and first-party dispute patterns can indicate elevated mule risk downstream — that connection is currently invisible.

Detection after dispersion is documentation, not prevention.

SECTION 07

What Acquirers Should Prioritise in the Next 30–90 Days.

01 **Model your VAMP and SMMP exposure by merchant segment.**

Understand which parts of your portfolio are approaching threshold and what proportion of disputes are first-party misuse versus genuine unauthorised fraud. The two require different responses.

02 **Audit your RDR usage against the post-March 2025 VAMP rules.**

If RDR is being applied to fraud-coded disputes, your ratios are being inflated in ways that may not be visible until a threshold is breached.

03 **Establish what consumer behavioural intelligence is available beyond your data perimeter.**

Under Mastercard's SMMP, acquirers have 72 hours to investigate a flagged merchant. The intelligence that would make that investigation faster and more defensible — repeat dispute patterns, consumer fraud history across merchants, behavioural signals from the banking side — is mostly not reaching acquirer fraud operations in a structured or scalable way. Understanding where it sits is the starting point.

SECTION 08

About Trudenty.

Trudenty operates the **Trust Network** — infrastructure for federated trust intelligence that delivers consumer trust signals across issuers, acquirers and merchants into pre-authorisation, account opening and ongoing monitoring, and reimbursement decisioning — without centralising raw data.

trudenty.com

AUTHORS

Lerato Matsio, CEO · **Colin McCloskey**, Head of Fraud Risk Intelligence

For more of our perspectives, visit our [Insights Hub](#).

SOURCES

Sources.

-
- 01** **Mastercard**, First-Party Trust: Getting to the Bottom of First-Party Fraud (2024) — first-party misuse accounts for 75% of chargebacks reported under fraud reason codes.

 - 02** **LexisNexis Risk Solutions**, True Cost of Fraud Study 2025 — US merchants lose \$4.61 for every \$1 of fraud loss, a 32% increase since 2022.

 - 03** **Mastercard**, State of Chargebacks 2025 — global cost of chargebacks to merchants forecast to rise to \$42 billion by 2028.

 - 04** **Chargebacks911**, Chargeback Statistics 2026 — a customer who successfully commits chargeback fraud is 9x more likely to repeat; one in three merchants worldwide has been hit.

 - 05** **Visa**, VAMP Merchant and Acquirer Monitoring Programme — Phase 1 live April 2025; Phase 2 thresholds from January 2026; TC40/RDR change from March 2025.

 - 06** **Cybersource / Mastercard**, 2024 Global Fraud and Payments Report — first-party misuse ranked second most common fraud attack method globally; 19% year-on-year increase in chargeback fraud.



Trudenty

trudenty.com