

LUQRA

White Paper

Visa Acquirer Monitoring Program (VAMP) – 2026 Focus on Merchant Education, Best Practices, and Tools



Written by:

Jacob Bennett

Chief Risk Officer

luqra.com

Executive Summary

The Visa Acquirer Monitoring Program (VAMP) represents a major evolution in Visa's fraud and dispute risk controls. Launched April 1, 2025, VAMP replaces multiple legacy programs – including the Visa Fraud Monitoring Program (VFMP) and Visa Dispute Monitoring Program (VDMP) – with a unified, acquirer-centric approach to monitoring and managing fraud, disputes, and enumeration attacks.

In 2026, compliance expectations tighten further: merchant thresholds are set to reduce, counting rules are clarified, and enforcement mechanisms are fully operational across regions. This white paper outlines changes applicable in 2026 and provides guidance on merchant education, best practices, and available tools and data to help merchants proactively manage risk, maintain compliance, and avoid costly penalties.

These changes represent an opportunity and responsibility for payment ecosystem participants to engage with their merchants and partners to offer and utilize available reporting, resources, tools, and further education to address fraud and portfolio health.

1. VAMP Overview – Key 2026 Changes

1.1 Program Purpose and Structure

Visa's goal with VAMP is to enhance the integrity of the global payment ecosystem by:

- ✔ Consolidating fraud and dispute monitoring into a single global framework.
- ✔ Aligning performance standards across domestic and cross-border card-not-present transactions.
- ✔ Incorporating enumeration (card testing) monitoring.
- ✔ Shifting to a lifecycle-based risk management approach.

1.2 VAMP Ratios and Threshold Timeline

Core metric:

VAMP uses a single VAMP Ratio for fraud and disputes:

$(\text{TC40 fraud reports} + \text{TC15 disputes}) \div \text{total settled transactions (TC05)}$ in a given period.

Key 2026 changes:

- ✔ The merchant excessive threshold declines from 2.2% to 1.5% effective April 1, 2026 in major regions (U.S., EU, Canada, AP).
- ✔ Minimum count criteria remain (e.g., $\geq 1,500$ fraud + dispute events/month).
- ✔ An enumeration ratio remains a standalone trigger if suspicious authorization tests exceed 20% of authorizations.

These tighter 2026 thresholds heighten the need for ongoing monitoring to prevent penalties or account restrictions.

2. Merchant Education – Building Understanding and Awareness

2.1 Understanding VAMP Fundamentals

Merchants must be educated on the basic mechanics of VAMP, including:

- ✔ How **fraud (TC40)** and **disputes (TC15)** are collected, counted, and reported.
- ✔ The implications of transactions counted in more than one category (e.g., fraud that also becomes a chargeback).
- ✔ The role of enumeration monitoring and how bot-driven attempts impact merchant profiles.

Educational content should clarify that the program is acquirer-driven – acquirers aggregate merchant transaction data into a portfolio-level risk assessment.

2.2 VAMP Enforcement Dates Recap (Relevant for 2026)

- ✔ **April 1, 2025:** VAMP launched.
- ✔ **October 1, 2025:** Enforcement begins with excessive thresholds.
- ✔ **January 1, 2026:** Tighter acquirer portfolio enforcement applies.
- ✔ **April 1, 2026:** Merchant thresholds tighten further.

Merchants should be reminded of these milestones through outreach, statement messaging, and dashboard alerts with clear countdowns and risk impact summaries.

3. Best Practices for Merchant Compliance

To stay within acceptable risk performance, merchants should adopt a set of risk-aligned operational best practices.

3.1 Reduce Fraud and Dispute Volume Proactively

- ✔ Implement and enforce 3D Secure (3DS) for online transactions.
- ✔ Use tokenization and address verification systems to reduce the incidence of unauthorized card usage.
- ✔ Segment channel performance to identify high-risk customer segments or regions.

3.2 Improve Pre-Dispute Engagement

Resolving issues before they become formal disputes is crucial:

- ✔ Provide excellent customer support with clear refund, cancellation, and return policies to reduce conflict.
- ✔ Offer clear billing descriptors to prevent confusion that can lead to disputes.

3.3 Monitor Performance Internally

Track key indicators regularly that feed into VAMP calculations:

Metric	Source
TC40 fraud reports	Acquirer/processor reporting
TC15 dispute events	Chargeback reporting systems
Total settled transactions	Merchant sales records

3.4 Engage in Timely Evidence Management

How to avoid a rise in disputes:

- ✔ Compile compelling evidence (including Order Insight details) promptly.
- ✔ Respond within dispute windows to avoid escalation.
- ✔ Track outcomes to refine internal dispute handling procedures.

4. Tools and Data to Support VAMP Compliance

Merchants should deploy both Visa-offered and third-party tools to manage risk data and mitigate disputes.

4.1 Visa-Native Tools

Pre-dispute alert and resolution tools:

- ✔ **Order Insight (PREVENT):** Shares transaction/order details with issuers during inquiries to deflect disputes.
- ✔ **Rapid Dispute Resolution (RDR):** Enables merchants to issue refunds quickly at the pre-dispute stage.
- ✔ **Cardholder Dispute Resolution Network (CDRN):** Alerts merchants when a dispute starts, giving a short window to prevent it from becoming a chargeback.

These tools, often offered via processors/acquirers, are critical for reducing TC15 counts – and where possible, minimizing TC40 events if disputes never become formal chargebacks.

4.2 Acquirer/Processor Reporting Dashboards

Partner with your acquirer or payment processor to receive:

- ✓ Monthly TC40 + TC15 breakouts.
- ✓ Calculated VAMP ratio data.
- ✓ Trends and alerts before thresholds are approached.
- ✓ Real time VAMP reporting data to identify trends and outliers on a daily basis.

Where possible, access real-time dashboards – either native or via API – to automate monitoring and flag high-risk trends early.

4.3 Third-Party Risk Platforms

Deploy third-party risk and analytics platforms that can integrate multiple signals, including:

- ✓ AI-driven fraud scoring.
- ✓ Authorization risk indicators.
- ✓ Chargeback pattern detection.

These platforms enhance visibility and allow merchants to test mitigation strategies based on real transaction data.

5. Data Considerations for Merchants

- ✔ **Data Quality:** Ensure consistent and accurate reporting of transactions, fraud indicators, and disputes.
- ✔ **Timeliness:** Acquirers often pull data on periodic cycles; ensure your internal and external reporting aligns. Some processors may offer real time data to assist merchants with actionable information.
- ✔ **Transparency:** Request detailed VAMP data from your acquirer/processor, especially TC40s and enumeration indicators.

Data segmentation by channels and product lines can reveal hidden risk vectors that disproportionately affect your VAMP ratio.

6. Conclusion

In 2026, VAMP represents a modern fraud program with tighter thresholds and clearer expectations for merchants and acquirers alike. Understanding how VAMP ratios are calculated, educating merchant stakeholders, implementing risk best practices, and leveraging a robust suite of tools and data sources are essential for maintaining compliance and minimizing financial exposure. Proactive management and collaboration with acquirers will be key to long-term success under the Visa Acquirer Monitoring Program.

References

- ✔ Visa Acquirer Monitoring Program Overview – Visa’s official program description and rationale.
- ✔ VAMP implementation and thresholds – details on thresholds and enforcement timelines.
- ✔ Threshold adjustments for 2026 – updated metric thresholds and fee structures.
- ✔ VAMP updates including ratio and enforcement dates – further breakdown on effective dates and rules.

About the Author



Jacob Bennett is a senior risk and operations executive with extensive experience in payment operations, regulatory compliance, underwriting, fraud prevention, and large-scale operational leadership. His career reflects a progressive trajectory across high-growth payment organizations where he has led risk mitigation, merchant onboarding, credit analysis, and enterprise operational strategy.

Jacob currently serves as Chief Risk Officer for Luqra, overseeing risk governance, loss mitigation, regulatory compliance, and operational oversight. His background demonstrates expertise in managing complex payment ecosystems, collaborating with acquiring banks and card brands, and designing risk monitoring methodologies aligned with regulatory requirements and industry standards.

Learn more

For Luqra’s latest thought leadership, industry perspectives, and educational resources, visit luqra.com and follow us on social media.