SLYCE360

YOUR ESSENTIAL GUIDE

Preparing for VAMP

A Handbook for Merchants

MERCHANT

With Visa's updated Acquirer Monitoring Program (VAMP) launching on **April 1, 2025**, merchants need to act quickly. Don't be fooled by the new program's name! VAMP imposes new fraud limits on merchants that are count and not dollar based, which have significant implications for how you manage your payments, especially if your business model is card not present and/or recurring payments. Preparing now is necessary to manage dispute and fraud exposure before enforcement begins. To help you navigate these critical changes, we've developed a comprehensive guide with urgent steps and best practices.

Here's your action plan to prepare for VAMP's impact:

1 Calculate Your Current VAMP Ratio

- **Understand Acquirer's Thresholds:** Reach out to your acquirer to learn about their specific thresholds, as these will guide your compliance efforts under VAMP. If your acquirer hasn't published specific thresholds, use Visa's standards as a guideline.
- **Start Now:** If you have access to TC40 or Visa Inform fraud data, along with metrics from RDR (Rapid Dispute Resolution) or CDRN (Cardholder Dispute Resolution Network), calculate these ratios immediately. Establishing even a basic fraud rate baseline is a crucial first step.
- **Establish Benchmarks:** Assess your current VAMP ratio to determine how it aligns with Visa's standards. This assessment provides valuable insights into your current standing and highlights areas that may need improvement.
- **Plan Ahead:** If you do not have all the necessary data to calculate your ratios, start collaborating with your acquirer and Payment Service Providers (PSPs) to gather this information as soon as possible. Work with your acquirer or Verifi to access your TC40 fraud data so you can monitor fraud levels daily.

2 Implement Strong Fraud Prevention and Security Tools

- **Strengthen Defenses:** Implement tools like **3-D Secure, AVS, and CVV checks** to detect fraud early.
- **Use Advanced Fraud Tools:** Leverage **multi-factor authentication, pre-authorization tools, velocity checks, and Captcha** to prevent enumeration attacks.
- **Consult Visa's Best Practices:** Use Visa's anti-enumeration and account testing guidance to bolster your security protocols. Find Visa's full guidance here: Visa Anti-Enumeration and Account Testing Best Practices.

3 Use Dispute Mitigation Resolution Tools

- **Enroll in Visa Mitigation Programs:** Prioritize enrollment in the **Rapid Dispute Resolution (RDR)** and **Cardholder Dispute Resolution Network (CDRN)** programs, as "resolved" disputes for RDR and non-fraud CDRNs are excluded from your VAMP calculation, thereby lowering your VAMP ratio. Note, however, that as of this writing, it's unclear whether a mitigated TC40 fraud dispute doesn't count toward the 1,000 TC40 fraud dispute threshold at which measurement of your rate kicks in for enforcement purposes. We'll have more on this later as guidance rolls in. Check Slyce360 Bytes at our website regularly for updates.
- **Then Actively Decision and Refund Mitigation Alerts:** A dispute is considered "resolved" when you've refunded the customer, avoided a chargeback, and, even if TC40 fraud was reported, the mitigated dispute is removed from your VAMP ratio's numerator, effectively

4 Improve Customer Experience and Security Tools

- **Billing Descriptors:** Test billing descriptors to ensure they are clear and accurate on customer statements, helping to avoid customer confusion and reduce potential disputes. Descriptors displayed to cardholders often don't match those you've submitted to your processor. Check both online app and statement descriptors wherever you can, as these can differ more often than you'd think.

- **Transparent Disclosures:** Offer clear, detailed customer terms and conditions, especially for subscription models. Be transparent about pricing, subscription terms, product or service details, and account setup instructions.

- **Proactive Communication:** Establish a communication timeline to set expectations around renewals, charges, and support.

- **Multi-Channel Support:** Provide customers with multiple service contact options (phone, email, chat) and respond promptly to inquiries.

- **Proactive Resolutions:** Address known issues early to prevent chargebacks and disputes, ensuring a smoother customer experience.

5

Analyze Your Chargeback Reason Codes

- **Fraud-Related Codes:** High fraud chargebacks may indicate a need for stronger fraud prevention tools such as 3-D Secure, AVS, or CVV checks.
- **Service-Related Codes:** Review the customer experience to ensure product descriptions, delivery, and customer support meet customer expectations. One effective way to gain insight is by ordering and returning your own product, allowing you to experience the process firsthand, just like your customers do.
- **Authorization-Related Codes:** Regularly verify all transactions are properly authorized to prevent authorization-related chargebacks.
- **Recurring Billing Codes:** If these make up a large percentage of your disputes, make it easier for customers to manage subscriptions and clarify recurring billing terms.

6 Track Dispute Data & Reconcile Consistently

- **Consolidate and Analyze Data:** Incorporate Customer Relationship Management (CRM) metadata with payments data to track fraud sources and chargeback causes.
- **Identify Patterns:** Benchmark key metrics and look for accelerating changes so you can spot emerging issues.
- **Monitor Mitigation Levels:** Refine your strategies as data changes. Elevated RDR and CDRN activity may highlight potential underlying risks.
- **Reconcile Resolved Disputes:** Deduct resolved disputes from TC40 data to maintain an accurate VAMP ratio.

Key Takeaway:

Start preparing now! VAMP will increase the focus on fraud and dispute metrics, and taking action early ensures your business is ready to maintain compliance and optimize performance under the new guidelines.

Book a free consult with our advisor today

Book Now