Info Sheet

BRAM and VIRP Basics

Learn about rules Mastercard and Visa have created to protect card brands and consumers from illegal and/or brand-damaging activity.

What are BRAM and VIRP, and what do they cover?

The Mastercard **Business Risk Assessment and Mitigation** (BRAM) Program and the **Visa Integrity Risk Program** (VIRP) – formerly the Global Brand Protection Program (GBPP) – are designed to protect card brands and consumers from illegal and/or brand-damaging activity. These programs impose fines on acquiring banks for any detected processing of fraud, illegal activity, or activity that may pose regulatory or reputational risk. Examples of such damaging activity include the illegal sale of prescription drugs or counterfeit merchandise, illegal or miscoded gambling, child exploitation or banned pornography, and websites used for fraud or transaction laundering. This is by no means an exhaustive list, but it illustrates the important role these programs play in keeping the payments ecosystem a safer place for consumers.

How do these programs work?

The card brands have a variety of ways of detecting transactions that they consider "brand-damaging." Some detection appears to be proactive on the card brands' part, while in other cases, external stakeholders such as law enforcement agencies, rights holders, or card brand investigators submit a complaint about a merchant. After identifying the merchant account and acquiring bank, the card brand will notify the acquiring bank of the noncompliant behavior and require a timely response that will include taking action against the offending merchant. Acquirers or payment processors then take action against the merchant, which may constitute account termination, a warning, or other remedial steps.

What happens to violative merchants?

In some cases, the merchant is (or should be) added to the **Member Alert to Control High-Risk** (MATCH) list, a database of merchants whose accounts were terminated within the preceding five years. When an acquirer considers signing a merchant, MATCH can help the acquirer assess whether the merchant was terminated by another acquirer and under what circumstances. This information may affect the decision whether to acquire this merchant and, if a decision is made to acquire, whether to implement specific action or conditions with respect to acquiring.

How do I adhere to BRAM and VIRP guidelines?

Acquirers must properly classify high-risk merchants and ensure that their merchants are not processing illegal or brand-damaging transactions. Part of this involves accurate MCC classifications. Card brands hold broad authority to levy noncompliance assessments, and may require acquirers to implement risk reduction measures or even prohibit them from acquiring any type of high-risk merchant. We encourage acquirers to proactively investigate suspected violative behavior and provide card brands with timely, detailed information about incidents that arise.

How much can fines be? Who is subject to fines? How are fines/penalties assessed?

The amount of fines varies by card brand. In general, Mastercard's fines are potentially higher – well into the six figures per transaction. However, if the acquirer is using LegitScript or another Merchant Monitoring Solutions Provider (MMSP), there is fine mitigation of up to 75% to 100%. Visa has no such mitigation program, but the fines are typically in the five-figure range per transaction. The magnitude of noncompliance assessments varies depending on the severity of the violation and other factors, potentially reaching hundreds of thousands of dollars or more. Furthermore, fines are often compounded if the merchant in question is a repeat offender or the acquirer failed to comply with card brand standards or other legal requirements. Failure to properly terminate an account can result in additional fines.

How do I know if a product or service violates BRAM and/or VIRP policy?

These programs' guidelines for restricted activities are regularly updated (see the links below). If a merchant is offering a product or service that is illegal in the buyer's or seller's jurisdiction, then the resulting transaction is virtually guaranteed to be noncompliant with BRAM and VIRP standards. You can partner with a registered **Merchant Monitoring Service Provider** (MMSP) like LegitScript to monitor your merchant portfolio, detect transaction launderers, and identify other risky behavior.

Partner with a registered Merchant Monitoring Service Provider like LegitScript to monitor your merchant portfolio, detect transaction launderers, and identify other risky behavior.

Additional Information

- On **BRAM** and Mastercard, see: https://www.mastercard.us/en-us/business/overview/support/rules.html
- On **VIRP** and Visa, see: https://usa.visa.com/dam/VCOM/download/about-visa/visa-rules-public.pdf
- On **LegitScript Merchant Monitoring**, see: https://www.legitscript.com/merchant-monitoring

LegitScript: Making the Internet and Payment Ecosystems Safer and More Transparent – Now and for Future Generations

Contact Us
1-877-534-4879
legitscript.com/contact