



Bankcard Merchant Programs

What they are and how to prevent your merchants from flagging the programs

By Jeffrey D. De Petro

Ah, the dreaded credit card companies' merchant programs. Or at least that is the perception. We think we understand them, but how do we keep merchants off the radar screen? In short, by understanding the programs and having the appropriate monitoring tools in place to identify the key indicators that lead to merchants' flagging the various programs.

Visa and MasterCard, as well as the other card brands, set standards all merchants must follow. When a merchant violates these standards, it could be subject to fines. If the merchant does not cease the prohibited practices, the acquirer may be forced to close the account. There are processing rule violations and there are program violations that result from excessive negative activity patterns found by the card brands' monitoring programs. Jeff Rosenblatt, COO of EVO Merchant Services, stated, "Although these types of monitoring programs may be perceived as a nuisance, they are actually a necessary tool in helping to reduce fraud and chargebacks. More importantly, they help to control negative merchant processing that does damage to the portfolio and raises liability."

Processing Rules Violations

Merchant processing violations commonly reported include:

- Setting minimum or maximum transaction amounts;
- Adding extra fees to cover processing costs;
- Requesting identification from customers;
- Not honoring all credit cards; or
- Not truncating the credit card number or the expiration date.

Processing rule violations are usually

reported by a consumer directly to the credit card company, which, in turn, notifies the member bank and requests that the merchant cease the prohibited practice. If the merchant complies, the credit card company is notified. If not, the merchant may be subject to penalties, including account closure.

Excessive Activity and Excessive Fraud Violations

Card company tracking programs look for excessive fraud and excessive chargebacks. MasterCard's programs include the Global Merchant Audit Program (GMAP), which identifies merchants with a high degree of fraud or counterfeit activity, and the Excessive Chargeback Program (ECP), which identifies merchants with excessive chargeback activity.

following occurring within one calendar month:

- At least three fraudulent transactions;
- A cumulative total of at least \$2,000 in fraudulent transactions;
- A minimum fraud-to-sales ratio of 1 percent within one calendar month.

Once identified by this program, MasterCard classifies the merchant into one of three tiers:

- Tier 1. A MasterCard fraud-to-sales ratio minimum of 1 percent and not exceeding 3.99 percent
- Tier 2. A MasterCard fraud-to-sales ratio minimum of 4 percent and not exceeding 6.99 percent
- Tier 3. A MasterCard fraud-to-sales ratio minimum of 7 percent.

If the merchant flags as Tier 1, the notification is for informational pur-



"Education and prevention is the name of the game."

– Jeffrey D. De Petro, vice president, EVO Merchant Services

Visa's programs include the Risk Identification Service (RIS), which is a merchant-level fraud monitoring program, and the Merchant Chargeback Monitoring Program (MCMP), which identifies merchants with excessive chargeback activity.

MasterCard's excessive fraud monitoring program, GMAP, was developed to identify and educate merchants who have a high degree of fraud or counterfeit activity. Using a rolling six months of data, GMAP identifies MasterCard merchants who have, at a minimum, all of the

poses only. If the merchant flags as Tier 2, the merchant must undergo training on fraud control procedures. If the merchant flags as Tier 3, either the merchant must be terminated or the acquirer must accept the chargeback liability. The Tier 3 identification also adds the merchant to MATCH for violation of MasterCard audit program thresholds, if the account is closed.

Visa's merchant fraud monitoring program, RIS, was revamped in April to provide a streamlined identification and remediation strategy. RIS identifies

merchants with excessive fraud and allows for a 90-day workout period, followed by a six-month penalty phase. Merchants are flagged if they exceed thresholds based on merchant category code (MCC) and fraud type. RIS Online uses a 10-month remediation timeline. The acquirer is first notified when the merchant exceeds program parameters. If a merchant continues in violation after the first notification, it enters a 90-day workout period. During this time, the merchant and acquirer must develop and implement fraud-reduction strategies. If a merchant is unsuccessful in reducing the fraud below the thresholds, it will enter into the fee period. The fee period includes monthly assessments that increase as the merchant continues to flag through the program. If a merchant fails to reduce its fraud, it might not be allowed to accept Visa transactions. "Nobody wins when fraud occurs. By identifying merchants who exceed fraud thresholds, RIS Online provides acquirers with the opportunity to address emerging threats to the payments system," says Visa.

Excessive Chargeback Programs

MasterCard's chargeback monitoring program, ECP, puts the burden of monitoring and reporting to acquiring banks. Each month, the acquirer is responsible for calculating the chargeback-to-transaction ratio (CTR) in basis points for each of its merchants. The CTR is the number of chargebacks the merchant location receives in a calendar month, divided by the number of sales transactions received from the merchant in the preceding month.

If a merchant has a CTR in excess of 50 basis points and at least 50 chargebacks in a calendar month, MasterCard considers it a Chargeback Monitored Merchant (CMM). If in each consecutive calendar month a merchant has a CTR of at least 100 basis points and a minimum of 50 chargebacks, the merchant is considered an Excessive Chargeback Merchant (ECM). The merchant maintains the designation of

ECM until the CTR is below 100 basis points for two consecutive months. Each month, the acquirer must submit a CMM report for each of its merchants that qualified as a CMM for the previous calendar month, no later than 45 days from the end of the month. Within 30 days of the end of the second trigger month, and on a monthly basis, the acquirer must submit an ECM report for each of its merchants that qualify as an ECM for two consecutive months. The ECP program timeframes and fee assessment are based on a tiered structure that increases until the situation is resolved.

Visa's chargeback monitoring program, MCMP, monitors the total volume of interchange transactions and chargebacks for each merchant location and identifies those who exceed Visa's chargeback activity thresholds. "The MCMP has been very effective in reducing member operating costs by enabling acquirers to quickly respond to merchants with excessive levels of chargebacks," says Visa. A merchant must meet or exceed each of the following parameters during a single month to violate the program.

- 100 or more Visa interchange transactions;
- 100 or more Visa chargebacks; and
- 1 percent or higher ratio of overall Visa chargebacks to Visa interchange transactions.

If this happens, Visa notifies the acquirer and assesses applicable penalties. The timeframes and penalties are based on a tiered structure. Fines for chargeback activity may continue to be assessed to the acquirer for all trailing chargeback activity that occurs up to 120 calendar days after transaction processing has ceased or as equivalent to the penalties being assessed to the acquirer at the time the transaction processing ceased. If the merchant continues to meet or exceed the thresholds beyond the program timeframes, or if the merchant demonstrates a critical level of chargeback-to-interchange volume at any time during a given month, Visa may require the acquirer to terminate the merchant agreement.

Education and Prevention

Education and prevention is critical. Merchants should be educated in the correct way to accept and process credit card payments, and also trained in ways to identify fraud and to limit, if not eliminate, questionable transactions. Educating a merchant is an ongoing process that should be done at every point of contact with the merchant. Each acquiring organization should have an internal training strategy that keeps its personnel well trained on the specific card brand rules, as well as tactics to maximize the value of each merchant interaction. All personnel should take advantage of each contact with merchants to reinforce the need to stay within the rules.

Fraud prevention is a continuous process. Monitoring tools and identifiers can be built into any risk monitoring system to serve as an early warning detection system. Risk investigators should show merchants what they can do to protect themselves.

Pre-notifications and early warning monitoring tools provide time to correct the problem prior to the merchant's flagging one of the monitoring programs. If a merchant should flag a program, conduct your own investigation as to why the merchant flagged, take steps to rectify the problem, and work closely with merchants to identify problems of which they might not be aware.

Understanding these card company programs and the value they bring to protecting your portfolio will help you recognize them as yet another tool in helping to manage merchant risk. The programs are here to stay, and everyone should take the opportunity to understand the them, educate their merchants and have prevention strategies in place. Implementing these practices will lead to a happier and more prosperous processing merchant. **TT**

Jeffrey D. De Petro is vice president for EVO Merchant Services and is the vice chair of the ETA Risk and Fraud Management Committee. He can be reached at jdepetro@goevo.com.