



Ten Smart Ways to Deal with an Account Compromise... *and still protect your customers and bottom line*

You've just received an e-mail from Visa's Compromised Account Management System (CAMS) alerting you that some of your accounts are at risk. Now what? Should you immediately block and reissue all of the compromised accounts...and perhaps unnecessarily disrupt or inconvenience your customers? How about daily monitoring—do you have the capacity and resources to keep an eye out for any suspicious activity? Or should you do nothing at all and just keep your fingers crossed that it will all blow over?

All of these are possible approaches to an all too common problem for today's card issuer. The good news is there are some practical (and tactical) ways to go about dealing with an account number compromise. **Here are ten best practices to consider when trying to determine your best course of action.**

- 1 Evaluate your situation.** Find out how many of the compromised accounts are still active. If there are some non-active accounts, determine how many of them have been closed due to fraud.
 - If you have closed accounts that were involved in fraud, you should look to see if the fraud pattern on the closed accounts matches up with the circumstances or fraud pattern described in the CAMS alert message. For example, if the CAMS alert describes a fraud pattern of full magnetic-stripe counterfeit taking place, you should determine if your fraud patterns are similar. If the fraud alert describes a compromise involving only account numbers and expiration dates, you may be looking for card-not-present fraud patterns. If you detect similar fraud patterns you may want to consider blocking and reissuing cards for the affected "active" accounts using these best practices as a guide. Fraud patterns matching the kind of data elements compromised are often tell-tale signs that someone has already obtained some of your accounts and has used them. So, the other accounts may be exposed as well.
 - If you haven't seen any signs of fraud that you believe could be linked to the reported account compromise incident, apply the remaining best practices accordingly. You need to keep in mind that it is often difficult to determine if the hacker was able to retrieve all of the exposed account numbers, including those from your institution.
- 2 Narrow down the high-risk possibilities.** For incidents involving the compromise of full track data, find out if any of the accounts were reissued after the compromise date. If so, you may not need to consider these accounts as "high-risk", since they would have been reissued with a different Card Verification Value (CVV) and expiration date.
- 3 Check for upcoming expirations.** Of the affected accounts, determine how many of them will be expiring in the next 30 to 180 days. Consider moving up the reissue on those accounts.
- 4 Stay one step ahead of fraud exposure.** Examine the possibility of you or your processor monitoring the compromised accounts using a fraud management system.
- 5 Do a fraud exposure reality check.** Take into consideration the number of cards affected, daily spending limits on cards, and the likelihood that fraud may occur. Also, assess the likelihood that the fraud will take place in the card-not-present environment, which may give you chargeback rights for fraudulent transactions. Know your normal fraud rates. How do these accounts measure against your normal fraud rates. Are they higher or lower. Higher than normal fraud rates may require you to examine all options including cost and reissue.
- 6 Notify your dispute area of the compromise.** This way, if they begin to get dispute calls on the affected accounts, appropriate action can be taken immediately.
- 7 Know your insurance rights and liabilities.** If you are a credit union and have counterfeit fraud insurance coverage, you may need to review your coverage with your carrier and discuss the impact of not blocking and reissuing new cards.
- 8 Pay attention to Visa follow-up notices.** Visa will continue to monitor compromised accounts through its internal system and will notify you if any unusual activity is detected. This doesn't mean that you should discontinue monitoring these accounts.
- 9 Keep Visa in the loop.** Always let Visa know if you have experienced fraud that you would consider related to a compromise incident, or if you begin experiencing fraud on any of the compromised accounts.
- 10 Think before you list.** If you do block and reissue compromised accounts, carefully assess the cost/benefit of listing these accounts on the Visa Card Recovery Bulletin. Given the "per card" costs involved to list accounts with fraudulent activity on the Visa Recovery Bulletin, this service should be used prudently. You, of course, want to minimize the risk of continued losses, but in the end is it worth the expense of doing so?

Ten Smart Ways to Deal with an Account Compromise... and still protect your customers and bottom line

Other Visa Resources Available to Help Issuers Better Manage Risk

Visa offers a number of risk management materials as part of its Member education program. Current publications include:



Visa Issuer Risk Management Guide

VBS 06.30.04

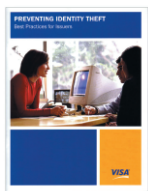
Comprehensive in scope, this guide brings together current best practices for improving Issuer profitability through proper credit and debit card fraud prevention.



Visa Check Card Risk Management Strategies

VBS 02.05.04

This guide summarizes the key risk issues faced by Visa check card Issuers and offers a complete set of operating practices and strategies for effective risk management.



Preventing Identity Theft Issuer Best Practices

VBS 08.01.03

This essential resource highlights a set of best practices that issuing financial institutions can use to strengthen their application validation, account maintenance, and ongoing identity theft fraud activity monitoring processes.



Visa U.S.A. Information Security Programs and Initiatives - VBS 06.01.04

This four-page brochure presents a general overview of the multiple information security programs and initiatives currently implemented by Visa.

All of these resources are available to Members in a downloadable PDF format via the Visa Business School Online Learning Center at www.us.visaonline.com. They are also available in print and can be ordered through the Visa Fulfillment Center at 1-800-235-3580.

Key Terms At A Glance

- **Card-Not-Present Environment** - A merchant, market, or sales environment where transactions occur without a valid Visa card being present. Card-not-present is used to refer to mail order/telephone order merchants and sales environments, as well as the Internet.
- **Card Verification Value (CVV)** - A unique three-digit "check number" encoded on the magnetic-stripe of all valid cards. The number is calculated by applying an algorithm (a mathematical formula) to the stripe encoded account information and is verified online at the same time a transaction is authorized.
- **Card Verification Value 2 (CVV2)** - A unique three digit "check number" indent printed on the signature panel of all valid cards. The number is calculated by applying an algorithm, and is used by mail order/ telephone order and Internet merchants to verify the user.
- **Compromised Account Management System (CAMS)** - A secure and efficient way for Acquirers, merchants, and law enforcement agencies to upload compromised and stolen/recovered accounts directly to Visa. As this information is received by CAMS, e-mail alert messages are automatically sent to registered Issuer users to notify them of the compromised and stolen/recovered accounts.
- **Key-Entered Fraud** - The use of key-entered transactions for depositing fraudulent sales transaction receipts.
- **Mag-Stripe** - A strip of magnetic tape on the back of all bankcards. The stripe is encoded with cardholder account information as specified in the *Visa U.S.A. Inc. Operating Regulations*. On a valid card, the account information on the magnetic-stripe matches similar embossed information on the front of the card.
- **Visa Card Recovery Bulletin** - An international printed list of lost/stolen, counterfeit, and other cards that Issuers have listed for pickup. The Card Recovery Bulletin is only printed in countries outside the United States.

How To Contact Us

Visa Fraud Control

Phone: 650 432-2978

Fax: 650 432-2945



© 2004 Visa U.S.A. Inc.
VBS 07.15.04