



What Every Merchant Should Know About The New Account Data Compromise Recovery Process



What Every Merchant Should Know About the New Account Data Compromise Recovery Process

Visa U.S.A. Inc. Operating Regulations state: A merchant or its agent must not retain or store the full contents of the magnetic stripe subsequent to an authorization of a transaction.

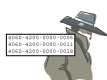
For the past two years, Visa and its members have struggled to recover disputes related to account compromises that have been linked to subsequent magnetic stripe-read counterfeit fraud. Visa's current compliance process provides issuers with a way to file a claim against an acquirer whose merchant allegedly stored the magnetic-stripe data. The process includes extensive research to identify the compromised entity, offers Visa members the ability to obtain copies of both the valid and fraudulent transactions, and allows for the submission of pre-compliance correspondence to settle a dispute before it escalates to a compliance claim for the amount of the fraudulent transactions. Although effective for small-scale cases, many members have reported that this process is too cumbersome and costly when thousands of accounts and fraudulent transactions are involved.

In an effort to replace the current compliance process with one that limits merchants' exposure and is cost-effective, efficient, and equitable for all parties involved, Visa has developed the Account Data Compromise Recovery (ADCR) process.

Visa's ADCR process, which becomes effective October 1, 2006, is used exclusively for magnetic-stripe data that has been determined as compromised. It limits counterfeit fraud liability for acquirers to a timeframe that is capped at 13 months, as compared to the current process where account exposure risk can extend up to the expiration date of the compromised cards. Additionally, ADCR allows the partial recovery of some operating expenses for issuers.

Mapping the ADCR Process from Start-to-Finish

ACCOUNT COMPROMISE AND SUBSEQUENT COUNTERFEIT FRAUD



Criminals **use a system or operational vulnerability to access** Merchant A's point-of-sale (POS) system with stored card data. They retrieve valid account information.



The stolen account information is downloaded to a computer, then encoded on counterfeit cards or re-encoded on lost/stolen cards.



The counterfeit cards (with seemingly valid data) are used at various merchant locations. Card issuers approve the transactions since no lost/stolen card or fraud has been reported at this point.

COMPROMISED ACCOUNT MANAGEMENT SYSTEM (CAMS)



Merchant A discovers the account compromise and immediately notifies their acquirer who uploads the stolen account numbers directly to CAMS.



Visa investigates and validates that an account compromise has occurred. Visa then sends a **CAMS** e-mail alert to affected issuers to notify them of the compromised accounts.



Affected issuers monitor, close, or block compromised accounts.

ADCR PROCESS



Visa determines whether the validated account compromise meets ADCR criteria.

- The full contents of any track of the magnetic stripe was stored after transaction authorization.
- The compromise involves 10,000 or more U.S. accounts.
- Incremental magnetic-stripe counterfeit fraud is attributed to the compromise.



Visa calculates and advises the acquirer of its **potential** ADCR financial liability, which includes a percentage of the magnetic stripe-read counterfeit fraud and partial operating expense liability amounts. Estimates are based on the projected magnetic stripe-read counterfeit fraud and account exposure risk expected during the compromise event window. The estimated liability allows acquirers to better forecast and plan for financial impact. The acquirer has 30 days to appeal the preliminary decision and provide documents to Visa for consideration.



If at the end of the issuer fraud-reporting window, it has been confirmed that an event meets ADCR criteria, Visa calculates the actual acquirer incremental counterfeit fraud and operating expense liability amounts due each participating issuer impacted by the compromise. **The calculation methodology is described on the next page.**



Visa notifies the acquirer and issuers of their respective liability or reimbursement amounts. Acquirers, at their discretion, determine when and how to notify a merchant about estimated and final liability amounts.

A **compromise event window** is defined as a 13-month maximum time period that can be up to 12 months prior to and one month past the CAMS alert date. Magnetic stripe-read counterfeit transactions must fall within the event window to qualify for recovery.

How Visa Determines . . . Acquirer Incremental Counterfeit Fraud Liability

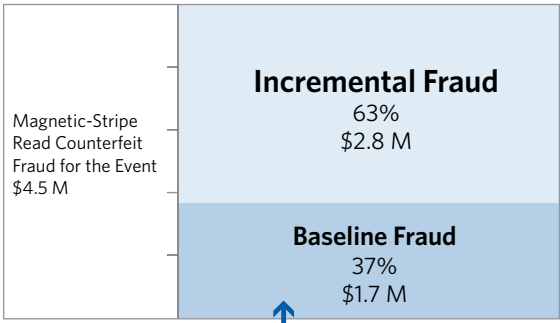
Under the ADCR process, Visa first determines the acquirer’s magnetic stripe-read counterfeit fraud liability attributable to improper magnetic-stripe data storage by calculating the amount of magnetic stripe-read counterfeit fraud that would have taken place in the Visa system during the 13-month event window if the account compromise had never happened. This “baseline” establishes the expected level of fraud for which an acquirer is not responsible. Visa then subtracts the baseline from the actual amount of magnetic stripe-read counterfeit fraud that occurred during the event window. The result is an “incremental fraud” assessment of the acquirer’s liability. This is the fraud that is above normal and therefore attributable to the magnetic-stripe data exposure. Additionally, any account number that was in a prior magnetic-stripe compromise event within the prior 12 months is excluded.

Issuers participating* in the ADCR process can recoup \$1 per eligible account involved in the compromise to partially cover operating expenses, such as card re-issuance and increased customer service calls. Any account number in a prior magnetic-stripe compromise event within the prior 12 months is excluded.

Acquirers are only liable for up to 80 percent of the total number of accounts involved in a magnetic-stripe data compromise. The remaining 20 percent represents the approximate percentage of accounts that will require little or no work by the issuers. In other words, these are account numbers that expired or were closed, reissued, or blocked prior to the time they appeared on a CAMS alert.

**Issuers must enroll in the Operating Expense Recovery process and be receiving Visa’s CAMS alerts in order to receive reimbursement.*

HYPOTHETICAL EXAMPLE



Acquirer is not responsible for Baseline Fraud

EXAMPLE: Acquirer Counterfeit Fraud Liability Calculation	AMOUNT
Actual magnetic stripe-read counterfeit fraud for event window	\$4,500,000
Baseline magnetic stripe-read counterfeit fraud (37%)	(\$1,665,000)
Net magnetic stripe-read counterfeit fraud liability amount (63%) (Incremental fraud)	\$2,835,000

Visa Compromised Account Management System (CAMS) offers a secure and efficient way for acquirers, merchants, law enforcement agencies, and issuers to transmit compromised and stolen/recovered account data to and from Visa through an encrypted site. Via CAMS, acquirers, merchants, and law enforcement officers can upload compromised and stolen/recovered account numbers directly to Visa. E-mail alerts are automatically sent through CAMS to registered issuers to notify them of account numbers that have been placed at risk. Issuers are allowed to access the account numbers in CAMS.



Reduce Your Risk Exposure and Liability

Merchants who store magnetic-stripe data provide criminals with an attractive and vulnerable platform from which to steal sensitive cardholder information. As the very nature of magnetic-stripe data theft continues to evolve, so does the need for merchants to proactively strengthen their security controls and greatly reduce their exposure to account compromise risk.

Avoid Magnetic-Stripe Data Storage Violations

- **Be CISP-compliant.** Work with your acquirer to understand your information security role and what's required of you and your service provider(s) in regard to CISP compliance. For more information about Visa CISP, visit www.visa.com/cisp.
- **Do not store magnetic-stripe data after transaction authorization.** The full contents of track data, which is read from the magnetic stripe, must not be retained on any system after a transaction is authorized. **If held in a CISP-compliant manner, the account number, expiration date, and name are the only elements of track data that may be retained.**
- **Evaluate your current/pending payment applications.** Do a thorough review of all payment applications to ensure non-storage of magnetic-stripe data. Confirm the security of your payment applications using *Payment Application Best Practices (PABP)*, which can be downloaded from the CISP web site at www.visa.com/cisp. This site also lists all software vendors whose payment applications have been validated by a Visa-approved security assessor.
- **Immediately report an account compromise.** If you suspect an account compromise, alert all necessary parties of a suspected or confirmed security breach immediately. Provide all compromised Visa account numbers to your acquirer bank within 24 hours. Remember, the sooner you report an account compromise, the sooner you close the window of opportunity for counterfeited fraud and limit your exposure.
- **Know your liability for data security problems.** Many merchant/acquirer contracts explicitly hold merchants liable for losses resulting from compromised card data if the merchant (and/or service provider) lacked adequate data security.

In the end, an ounce of prevention can go a long way, since any costs that merchants spend up front to protect magnetic-stripe data are probably going to be far less than what they could wind up paying in total liability for account compromises.

Visa merchants and service providers who store, process, or transmit cardholder data must comply with Visa's Cardholder Information Security Program (CISP) requirements.



© 2006 Visa U.S.A. Inc. VRM 07.07.06