

# Updated Account Data Compromise Recovery (ADCR)

## Frequently Asked Questions

---

### Background/ General Information

**Q: What is the Account Data Compromise Recovery process?**

A: The Account Data Compromise (ADCR) process allows issuers to recover a portion of their magnetic-stripe (POS 90) counterfeit fraud losses and operating expenses when a Payment Card Industry (PCI) Data Security Standard (DSS) violation could have allowed a compromise of full magnetic-stripe track data.

**Q: Why did Visa® create this process?**

A: The ADCR process was created to replace the compliance-filing process with a more efficient and cost-effective means of assigning liability associated with magnetic-stripe data storage events<sup>1</sup>. The compliance process was manually intensive, extremely complex, and only addressed member's transaction losses. In contrast, ADCR calculates recovery amounts on an aggregated basis and does not require issuers to file compliance claims at the individual transaction level. It also allows issuers to recover a portion of their operating expenses. ADCR's improved efficiency enables issuers to re-focus staff on the prevention of fraud. Acquirers benefit by having an improved ability to forecast financial liability for an event.

**Q: How do issuers know when account numbers have been placed at risk?**

A: Issuers are notified of account numbers placed at risk due to a compromise event via Compromised Account Management System (CAMS) alerts. Issuers receiving these alerts should take whatever action is necessary to minimize losses and protect their cardholders. When account numbers are placed at risk, all Visa stakeholders must work together to minimize fraud losses. CAMS alerts provide issuers an opportunity to play their part.

---

### Expanded ADCR Operating Regulations

**Q: What changed with the announcement on January 22, 2008 indicating that Visa Operating Regulations have been revised to expand the Account Data Compromise Recovery (ADCR) process?**

A: The *Visa U.S.A. Inc. Operating Regulations* have been changed to expand the scope of the ADCR process to include violations of the Payment Card Industry Data Security Standard (PCI DSS) requirements that could allow a compromise of full magnetic-stripe data.

**Q: Why did Visa make this change?**

A: Prior to this change, the scope of the ADCR process was limited to magnetic-stripe storage violations. Advances in technology now allow criminals to obtain magnetic-stripe data from a merchant during the course of a transaction, even if the merchant is not storing the data. For example, in recent cases criminals have exploited PCI

---

<sup>1</sup> The scope of ADCR was recently expanded to include full magnetic-stripe data compromises in which a PCI DSS violation could have allowed the compromise. Consequently, the scope is no longer limited to events involving magnetic-stripe data storage.

DSS violations to breach a merchant's network and place a data capture program, or "sniffer", on the network to capture in-flight transaction data. With this change, if a PCI DSS violation could have allowed a compromise of full magnetic-stripe data, the violation will be eligible for ADCR, provided all other ADCR eligibility requirements are met.

**Q: How does this change benefit financial institutions?**

A: The change benefits issuers and acquirers because recovery for compromises that would otherwise have been handled under compliance will now be handled under the more streamlined and cost-effective ADCR process.

**Q: When did the expanded ADCR Operating Regulations become effective?**

A: Beginning with qualifying Compromised Account Management System (CAMS) events that occur on or after January 22, 2008. Accordingly, Compliance cases related to CAMS events that occurred prior to January 22, 2008, involving PCI DSS violations must be filed no later than April 20, 2008.

**Q: Will compliance apply for CAMS alerts issued after the expanded ADCR Operating Regulations became effective?**

A: No. The existing compliance process for recovery of losses associated with violations of the *Visa U.S.A. Inc. Operating Regulations* involving non-compliance with PCI DSS requirements that could allow a compromise of magnetic-stripe data has been replaced with the ADCR process for CAMS alerts issued on or after January 22, 2008. Compliance rights are no longer available for disputes relating to such CAMS alerts issued on or after January 22, 2008.

**Q: Are cases that do not involve a PCI DSS violation potentially eligible for ADCR?**

A: No. To qualify for ADCR there must be a PCI DSS violation that could have allowed a full magnetic-stripe data compromise to occur.

**Q: In ADCR qualified cases where a PCI DSS violation occurred, will Visa provide information to the acquirer(s) proving that the violation resulted in a full magnetic-stripe data compromise?**

A: Visa will provide information from the forensics investigation or other sources indicating that one or more violations occurred that could have allowed the full magnetic-stripe compromise to occur. While Visa will not be required to provide specific proof that the compromise was a direct result of a violation, a determination will be made based upon the preponderance of evidence, including statistical analysis in addition to forensic findings.

**Q: Will "sniffing"<sup>2</sup> cases now be eligible for ADCR?**

A: If a PCI DSS violation could have allowed a sniffing-related full magnetic-stripe compromise to occur, and assuming it meets all other eligibility conditions, it will be eligible for ADCR.

---

<sup>2</sup> In some cases, intruders place a data capture program known as a "sniffer" on the compromised entities' networks. The sniffer intercepts data traveling over the networks, including wireless networks.

**Q: Will skimming cases be eligible for ADCR?**

A: If a PCI DSS violation could have allowed a skimming-related full magnetic-stripe compromise to occur, and assuming it meets all other eligibility conditions, it will be eligible for ADCR.

---

**Issuer ADCR  
Eligibility and  
Participation**

**Q: What must issuers do in order to participate in the ADCR process?**

A: ADCR participation is determined at the Business ID (BID) Level. To participate in ADCR, issuers must register each BID to receive CAMS alerts. In addition, to be eligible for recovery of a portion of their operating expenses, issuers must enroll each BID in the Operating Expense Recovery process.

**Q: How do issuers register to receive CAMS alerts?**

A: To receive CAMS alerts issuers must submit an e-mail to [CAMS@visa.com](mailto:CAMS@visa.com) and request a CAMS alert registration form. This form includes instructions for registering BIDs for CAMS.

**Q: How do issuers enroll in the Operating Expense Recovery process?**

A: Enrollment for participation in the Operating Expense Recovery process is done at the BID level. Issuers that license BINs must complete and submit the Account Data Compromise Recovery Process Operating Expense Recovery Enrollment Form for each of their BIDs. The enrollment form is available on Visa Online (VOL) at [www.us.visaonline.com/us\\_riskmgmt/adcr](http://www.us.visaonline.com/us_riskmgmt/adcr). If you do not have access to VOL, visit [www.vol enroll.com](http://www.vol enroll.com) to sign up. *You can also request a copy of the enrollment form by sending an e-mail to [eSupport@visa.com](mailto:eSupport@visa.com).*

**Q: What is the cost to enroll in ADCR?**

There are no enrollment fees.

**Q: Why is Visa imposing an administration fee to issuers?**

A: ADCR replaced the cumbersome compliance process, where both a filing fee (\$150) and a review fee (\$250) were assessed when Visa ruled on each case. With ADCR, the manually intensive process of preparing and responding to cases is now handled by Visa resulting in significant cost savings for issuers. The minimal ADCR administration fee replaces all of the fees that would otherwise have been payable on potentially hundreds of compliance cases. The ADCR fee helps to offset Visa's cost for administering the process.

**Q: Are the administrative fees netted on a monthly basis?**

A: Each qualifying CAMS event will have a separate credit. All credits issued, whether for recovery of counterfeit fraud losses or operating expenses will be distributed on a monthly basis and each credit will be net of the appropriate administration fee.

**Q: Does an issuer have to experience magnetic-stripe (POS 90) counterfeit fraud in order to qualify for operating expense reimbursement?**

A: No. Analysis of the magnetic-stripe (POS 90) counterfeit fraud will be considered in determining whether an event is eligible for operating expense recovery, however it is not a minimum requirement.

**Q: Why is ADCR limited to CAMS events with 10,000 accounts or greater?**

A: Since the ADCR process requires a significant amount of administration, Visa needed to establish a minimum number of account numbers so the process would not be applied to small events involving relatively small amounts of fraud.

**Q: What can an issuer do if the amount of account numbers in a CAMS event is less than 10,000 or if the fraud falls outside of the defined 13 month window? Will there be an alternative process available?**

A: No. If the compromise event does not meet the ADCR eligibility requirements, there is no alternative process available. In those situations, the fraud is the issuer's responsibility.

**Q: Does the 10,000 account minimum apply per financial institution or per event?**

A: There must be a minimum of 10,000 Visa account numbers in the event overall, not per financial institution.

**Q: How will issuers be notified that a CAMS alert qualifies for participation in ADCR?**

A: Once Visa makes a final decision that an event qualifies for ADCR, all impacted members will be notified via the ADCR Event Qualification Status Report on Visa Online. The report is updated twice a month. Please note that in a best case scenario, that determination will be approximately three to four months after the date of the CAMS alert. This is because Visa must first make a preliminary determination of eligibility, then provide the acquirer 30 days to appeal. At the end of the appeal timeframe, Visa then evaluates all information before making a final decision.

---

**Transaction  
Recovery  
Qualification**

**Q: What transactions qualify for recovery?**

- A: The following qualification requirements must be met in order for transactions to qualify for recovery:
- Transactions must be reported properly through the Visa Fraud Reporting System
  - Transactions must be reported as a full magnetic-stripe read transactions (POS Entry Mode of 90)
  - Transactions must be reported as counterfeit (Fraud Type 4)
  - Transactions must fall within the 13 month event window
    - Up to 12 months prior to CAMS alert date
    - And one month post CAMS alert date
  - Transactions with account numbers not involved in a prior compromise event within the 12 months prior to the event

**Q: What is meant by event window?**

A: For magnetic-stripe (POS 90) counterfeit fraud transactions to qualify for recovery for a specific compromise event, their transaction dates must fall within the start and end date established for each compromise event. This timeframe is called an event window. Each compromise event that qualifies for participation in the ADCR process has its own event window. The event window is based on the date of the related CAMS alert and can be up to 12 months prior to the CAMS alert date and one month after the CAMS alert date.

Examples:

1. CAMS alert is sent on January 1, 2007. The forensic study indicates the compromise occurred on September 15, 2005. The event window would start on January 1, 2006 and end January 31, 2007,
2. CAMS alert is sent on January 1, 2007. The forensic study indicates that the compromise occurred on June 1, 2006. The event window would start on June 1, 2006 and end on January 31, 2007.

**Q: How does Visa know the fraud is tied to a specific CAMS event?**

A: An event qualifies for ADCR based on Visa's analysis of the forensic reports, information provided by issuers, information provided by the acquirer/merchant involved in the compromise event and analysis of fraud reporting. Additionally, account numbers that were involved in a prior event within the previous 12 months are excluded. Only the remaining account numbers that incurred magnetic-stripe (POS 90) counterfeit fraud losses are eligible for the fraud recovery component of ADCR.

**Q: How do chargebacks affect a member's recovery?**

A: There are very few chargeback rights associated with magnetic-stripe (POS 90) counterfeit transactions. Given that liability is calculated at an aggregate basis for incremental fraud only, Visa is not accounting for chargebacks at this time. Visa will continue to monitor the activity to evaluate whether it makes sense to change this policy in the future.

---

**Operating  
Expense  
Recovery**

**Q: Why are issuers only receiving operating expense recovery on 80 percent of the account numbers at risk?**

A: The Operating Expense Recovery process provides some relief for accounts that had to be "worked" once a CAMS alert is issued. At the time of a CAMS alert, many account numbers on the alert are no longer active. They have already been closed, reissued, are expired, blocked, etc. Therefore there are no, or very little, incremental operating expenses that are incurred on these inactive accounts. A member survey reflected that 80 percent of account numbers on CAMS alerts are actually worked.

**Q: When must an issuer enroll to participate in the Operating Expense Recovery process for an event?**

A: Enrollment must occur prior to the date of the CAMS alert for the event.

Example: The enrollment date occurs on January 15, 2007. A qualifying CAMS alert occurs on January 30, 2007. If your financial institution has account numbers listed in the CAMS alert, your institution would be considered for operating expense recovery if all other participation criteria are met. If, given the same enrollment date, a CAMS alert occurred on January 13, 2007 your financial institution would not be considered for recovery because the enrollment occurred after the alert date.

**Q: Will the enrollment process for Operating Expense recoveries ever expire?**

A: This is an open enrollment process. Issuers can sign up at any time and once enrolled will remain eligible for recovery until such time as the process is no longer supported.

**Q: The Operating Expense Recovery amount of \$1 does not cover issuer's true costs. Why is it so low?**

A: Issuer processes for responding to CAMS alerts vary widely. Some automatically reissue all or some of the account numbers listed. Some simply implement monitoring or enhance their current monitoring programs. Others use a combination of these approaches. Some do nothing. The current recovery amount of \$1 is a reasonable proxy for average issuer costs and may be reevaluated in the future.

---

**Acquirer  
Liability/Issuer  
Reimbursement  
Calculation**

**Q: What is Baseline Percentage?**

A: Baseline Percentage is the percentage of total fraud in the Visa system attributable to magnetic-stripe (POS 90) counterfeit fraud, excluding accounts in the event being evaluated. For example, if total Visa fraud during an event window, excluding accounts involved in the event, is \$100 million, and total magnetic-stripe counterfeit fraud, excluding the same accounts, is \$18 million, the Baseline Percentage will be 18% (\$18 million / \$100 million).

**Q: What is Baseline Fraud?**

A: Baseline Fraud is the amount of magnetic-stripe (POS 90) counterfeit fraud that would have been expected on the event account population if the compromise event had not occurred. In other words "business as usual". It is calculated by multiplying the Baseline Percentage by the total fraud for the event. For example, if the total fraud for an event is \$100,000 and the Baseline Percentage is 18%, Baseline Fraud will be \$18,000 (\$100,000 X .18).

**Q: What is Incremental Fraud?**

A: Incremental Fraud is the total magnetic-stripe (POS 90) counterfeit fraud for an event minus Baseline Fraud. It represents the fraud amount that exceeds the Baseline Fraud amount. For example, if the total magnetic-stripe counterfeit fraud for an event is \$50,000 and the Baseline Fraud amount is \$18,000, the Incremental Fraud amount will be \$32,000 (\$50,000 - \$18,000).

**Q: Will the baseline calculation and the incremental calculation be published per event, and if so, where?**

A: Yes. The baseline and incremental calculations will be included in the reporting that is provided to all impacted members.

**Q: When calculating the baseline percentage, will any other compromise events be removed to reach the final percentage?**

A: The baseline percentage is the percentage of total fraud in the Visa system attributable to magnetic-stripe (POS 90) counterfeit fraud. Only accounts in the event being evaluated are excluded.

---

## ADCR Liability CAP Guideline

**Q: What is the ADCR liability cap guideline?**

A: As an interpretation of the Catastrophic Loss<sup>3</sup> section in the *Visa U.S.A. Inc. Operating Regulations*, Visa has established a guideline to cap ADCR liability between two percent and five percent of the affected entity's annual Visa sales volume. The specific cap percentage to be used within this range will be determined at Visa's discretion, based on criteria such as the merchant's Payment Card Industry (PCI)/Cardholder Information Security Program (CISP)<sup>4</sup> level.

**Q: Why did Visa introduce the liability cap guideline?**

A: Visa has established this guideline to fairly balance the needs of Visa stakeholders, guard against negative impacts to the payment system and ensure continued broad acceptance of Visa products.

**Q: When does the cap guideline apply?**

A: Application of the cap guideline will be contingent upon full cooperation of the affected acquirers, merchants and any related agents. For example, cooperating with the compromise investigation, providing information within requested timeframes and demonstrating satisfactory progress toward remediation of PCI/CISP violations).

**Q: How much does the cap guideline typically reduce liability for a compromised merchant?**

A: This depends on the magnitude of the total calculated ADCR liability relative to the merchant's annual Visa sales volume. In a case with a relatively high calculated liability amount and a relatively small annual Visa sales amount, the cap amount might be a small percentage of the calculated amount. In a case where the calculated amount is less than the cap amount, the cap will not reduce liability at all.

---

<sup>3</sup> Section 4.1.G of Volume II of *Visa U.S.A. Inc. Operating Regulations - Catastrophic Loss*  
*If an account compromise event is deemed catastrophic, Visa U.S.A. reserves the right to implement an alternative process.*

<sup>4</sup> The PCI/CISP defines four levels of merchants based on Visa transaction volume and other criteria.

---

**Acquirer  
Liability and  
Issuer  
Reimbursement  
Notification**

**Q: How will members be notified of their respective liability or reimbursement amounts?**

A: After the close of the event window and when the fraud reporting period has elapsed, Visa will calculate each member's respective liability or reimbursement amount and send the results via e-mail. Issuers will receive an *Account Data Compromise Recovery - Issuer Recovery Statement*. Acquirers will receive an *Account Data Compromise Recovery - Acquirer Liability Statement*.

**Q: Will acquirers receive any pre-notification that a compromise event has occurred that potentially qualifies for participation in the Account Data Compromise Recovery (ADCR) process?**

A: Yes. After a CAMS alert has been issued and Visa makes the preliminary determination that a compromise event will qualify for participation in ADCR, Visa will e-mail the acquirer the *Account Data Compromise Recovery Process - Acquirer Liability Estimation*. This communication will include a Qualification Summary indicating why Visa has preliminarily determined that the event will qualify for ADCR. It will also provide an estimate of the amount of liability for both the magnetic-stripe (POS 90) counterfeit fraud losses and the operating expenses.

**Q: Are acquirers allowed to share with the merchant the Qualification Summary document received from Visa with the preliminary determination of ADCR qualification?**

A: Yes. The Qualification Summary can be shared with the compromised merchant as part of the management of your programs and services. You must indicate to the merchant that the Qualification Summary is confidential and proprietary information that may not be shared or discussed with anyone not related to the case.

**Q: Will the acquirer be given an opportunity to appeal the decision?**

A: Yes. Upon receipt of the pre-notification, acquirers will have 30 days, from the date on the notice to submit an appeal to Visa and provide any information or documentation they have. Visa will consider the acquirer's appeal when making the final determination of whether the event qualifies for participation in ADCR. Once that decision is made it is final and there are no additional appeal rights.

**Q: Who will receive these statements by e-mail?**

A: Issuer statements will be e-mailed to both the Primary Center Manager and Fraud Manager(s) using the e-mail addresses currently available in Visa's corporate database, or to the designee provided through the Operating Expense Recovery enrollment process. Acquirer statements will be e-mailed to both the Primary Center Manager and Fraud Manager(s) using the e-mail address currently available in Visa's corporate data base.

**Q: Who should members contact to update ADCR notification contact names and e-mail addresses?**

A: Send an e-mail request to [USMembercontacts@visa.com](mailto:USMembercontacts@visa.com) or contact Franchise Communications at (650) 432-7064.

---

## BID/BIN Logistics

**Q: Some Visa members sponsor other issuers and receive CAMS alerts on their behalf. Do these issuers need to register for CAMS themselves or are sponsoring members able to do it on their behalf?**

A: CAMS alert registration and ADCR enrollment is done at the BID level. Only institutions that license their own BINs can register for CAMS.

**Q: If a processor or credit union league is registered to receive CAMS alerts on behalf of issuer BIDs, are those issuers considered CAMS participants?**

A: An employee of the member BID that licenses their own BIN must register to receive CAMS alerts in order to qualify for participation in the ADCR process. The same is true for enrollment for partial recovery of operating expenses. An employee of the member BID must enroll in the Operating Expense Recovery process.

**Q: Must each BID register to receive CAMS alerts, or only the parent BID?**

A: Each member BID that licenses issuing BINs must register to receive CAMS alerts.

---

## Event Window Timeframe Issues

**Q: If issuers experience a significant spike in magnetic-stripe (POS 90) counterfeit fraud after the event window has passed, will the original Baseline for the event be re-evaluated?**

A: Once the event window is closed, there will not be any adjustments made to the Baseline. One of the guiding principles of the ADCR process is to place a cap on the liability for which the acquirer is held liable. Issuers are encouraged to follow best practices and monitor and control fraud or re-issue accounts that are impacted by these events.

**Q: How will Visa determine liability if two events occur within close proximity?**

A: In the event that a compromise event occurs within 30 days of another event, the liability for both the magnetic-stripe (POS 90) counterfeit fraud losses and operating expenses will be equally shared between the compromised parties for common account numbers.

---

## Calculation Credit/Debit Settlement

**Q: Will issuers need to do anything in order to collect the recovery amount noted on their issuer Account Data Compromise Recovery Statement?**

A: No. Visa will process these credits through the Global Member Billing Solution; also known as Integrated Billing.

**Q: Do acquirers need to process credits to each issuer qualified to receive recovery for either magnetic-stripe (POS 90) counterfeit fraud or operating expenses?**

A: No. Visa will process these credits through the Global Member Billing Solution; formerly known as Integrated Billing.

**Q: When can members expect to receive their credits and debits?**

A: The processing of issuers' and the acquirer's respective liability or reimbursement amounts is determined by the date of the related CAMS alert. The entire process including determining event qualification, appeal (if any), calculation of liability, billing the acquirer, and crediting the issuer will take approximately seven months following the date of CAMS. However, depending on the complexities of determining event qualification and the volume of cases overall at any given time, the process could take longer. Qualified, non-qualified and pending cases are posted on the ADCR page on Visa Online.

**Q: Under what circumstances would an issuer not receive a fraud loss payout?**

A: Issuers would not receive recovery of magnetic-stripe (POS 90) counterfeit fraud losses for the following reasons:

- The compromise event did not qualify for participation in the ADCR process
- Magnetic-stripe (POS 90) counterfeit fraud transactions are not properly fraud reported as counterfeit (Fraud Type 4) within 90 days of the transaction processing date
- The compromise event had less than 10,000 account numbers
- The net recovery amount is less than \$25
- The issuer was not registered to receive CAMS alerts
- The total amount of magnetic-stripe (POS 90) counterfeit fraud was not above normal levels
- Visa is unable to collect liability from the acquirer

**Q: If an issuer BID or BIN is transferred during the event window, who will receive any payment due?**

A: Visa will pay (through GMBS) the member of record at the time of the calculation.

**Q: If an acquirer BID or BIN is transferred during the event window, who will be liable for the losses?**

A: Visa will bill (through GMBS) the member of record at the time of the calculation.

**Q: Why is it that issuers will not receive recovery amounts that are under \$25?**

A: It is cost prohibitive to administer small recovery amounts.

**Q: If members are receiving CAMS alerts on behalf of sponsored issuers, will they also receive the sponsored issuers' reimbursement statements, and will they be expected to deliver these statements?**

A: If the member who receives the CAMS alerts is the licensee of the BIN, then yes, they will also receive the statements for the issuers they sponsor. It is also the responsibility of the BIN licensee to manage the delivery of the information to the issuer financial institution that they sponsor.

**Q: Why does it take so long to recover the magnetic-stripe (POS 90) counterfeit fraud losses?**

A: After the 13th month of the event window has elapsed, issuers need to be given the opportunity to submit their fraud reports. The *Visa U.S.A. Inc. Operating Regulations* provide issuers 90 days from the transaction's central processing date to report fraudulent transaction activity to Visa.

**Q: Will the payout include the specific CAMS alert number?**

A: Yes. The billing line item detail from the Global Member Billing Solution will include the CAMS alert number associated with the event under the Special Description header along with one of the following descriptions:

Issuers:

- Compromise Counterfeit Recovery
- Compromise Ops Exp Recovery

Acquirers:

- Compromise Counterfeit Collections
- Compromise Ops Exp Collections

**Q: How are payout amounts segregated when there are multiple members sponsored using the same BID?**

A: Payouts will always be made at the BID level to the BIN Licensee. For BIDs who share issuing BIN(s) with one or more sponsored members, a supplemental report will be made available to the contact person identified during the ADCR enrollment process. The supplemental report will have breakouts for the accounts of each sponsored member as determined by the account ranges of record on the date the payout is calculated.

---

**Legal/Appeal Rights**

**Q: Are there any issuer appeal rights if they believe their amount to be inaccurate?**

A: No. Visa's decision is final. If you believe there is an error, you may want to consider reviewing your fraud reporting practices to ensure they align with *Visa U.S.A. Inc. Operating Regulations*. Only issuers that have properly reported magnetic-stripe (POS 90) counterfeit fraud (Fraud Type 4) transactions within 90 days of the transaction date, and whose transaction date falls within the event window, will be eligible for recovery. You may also want to validate that none of your fraud transactions were returned (rejected) by Visa due to failed Fraud Reporting System edits.

**Q: Does participation in the ADCR process prohibit me from pursuing any legal rights against an acquirer?**

A: Participation in the ADCR process does not relinquish any legal rights that may exist outside of the Visa system.

---

## ON-US Transactions

**Q: Will issuers receive recovery for “on-us” magnetic-stripe (POS 90) counterfeit fraud losses?**

A: No. While the vast majority of Visa transactions have historically been processed over VisaNet®, past “on-us” exceptions were granted to allow members the option of processing these transactions in-house, or through some means other than VisaNet. Effective May 15, 2005, the *Visa U.S.A. Inc. Operating Regulations* required that all US Visa transactions be authorized, cleared, and settled through VisaNet. This effectively ended “on-us” processing by members in all but a few exception cases.

---

## Fines

**Q: Will acquirers still be assessed fines for storing magnetic-stripe data or is this process replacing Visa fines?**

A: Existing Visa fines and penalties will continue to be assessed as outlined in the *Visa U.S.A. Inc. Operating Regulations*.

---

## Visa Fraud Reporting

**Q: Will Visa be monitoring the abuse of the fraud reporting process?**

A: Yes. Visa does monitor issuers’ fraud reporting.

**Q: Does the 13-month event window allow the 90-day timeframe for fraud reporting to be completed once a CAMS alert is communicated to issuers?**

A: Yes. The event window closes one month after the CAMS alert is sent. Issuers have 90 days after the event window closes to report fraud that occurred during the event window.

**Q: What happens when the customer reports the card lost and a member later discovers that the fraud is a result of a counterfeit card? Are members able to change this to the proper reporting within 90 days of the CPD in order to have this particular card qualify?**

A: As per Fraud Reporting System specification, members can update their fraud records to reflect new information on a fraud case. Fraud reporting changes to a different fraud type should be rare instances as these changes will greatly impact payout calculations. Visa will monitor these changes through its Fraud Reporting Compliance program. Additionally, any fraud reporting or maintenance completed 120 days after the CAMS alert date will not be reflected in the payout calculation.

**Q: What specific analysis is done on the fraud data? What can Visa do to prove to the acquirer that true counterfeit fraud occurred?**

A: Visa analyzes trends of magnetic-stripe (POS 90) counterfeit fraud for the accounts in the event and compares them to norms for the Visa system overall. The data used for all calculations is obtained from the Visa Fraud Reporting System.

**Q: What, specifically, does Visa do to determine if a merchant has been a common point of purchase?**

A: Common points of purchase can be identified from a variety of sources including the merchant, the acquirer, issuers, or Visa internal analysis. The Visa Fraud Control team will send a CAMS alert if it determines, based on all available information, that account numbers have been placed at risk. The ADCR process will only apply to a subset of CAMS alerts. See the Transaction Recovery Qualification section for more information.

**Q: If a member notifies a cardholder that his or her account has fraud on it and then at a later date that same account number shows up on a CAMS alert and it qualifies for ADCR, does the member have to report that fraud to Visa again?**

A: If the member properly reported the transaction to Visa as counterfeit (Type 4) and validated that the cardholder was in possession of their card at the time of the transaction, the fraud reporting to Visa will be captured by ADCR—no additional work is required.

---

**Card-Not-Present and PIN Transaction Exclusions**

**Q: Why doesn't the ADCR process allow for the recovery of card-not-present transactions?**

A: ADCR replaced the compliance right that existed prior to October 1, 2006 covering a violation for storing magnetic-stripe data that resulted in a financial loss for an issuer. Since chargeback rights exist for card-not-present transactions, they are not included in this process.

**Q: Is there a similar recovery process for PIN-based transactions?**

A: Visa's compliance program currently includes recovery for Interlink and Plus PIN-based transactions. It is planned that ADCR will replace compliance as Visa's recovery program for Interlink and Plus transactions in the future once a sufficient history of fraud reporting data is available.

---

**International Transactions**

**Q: Are International fraud transactions resulting from a compromise of a US account number that was compromised at a US merchant included in the ADCR process?**

A: Yes. All magnetic-stripe (POS 90) counterfeit fraud transactions associated with an eligible compromise event in the US are included, regardless of where the fraud transaction occurred.

Q: Are International account numbers included in the ADCR process?

A: No. The ADCR process applies to US account numbers only. International account numbers are covered under the Data Compromise Recovery (DCR) solution. This program was introduced in October 2007 and is the international equivalent of ADCR. Please refer to the *Visa International Operating Regulations* for handling magnetic-stripe (POS 90) counterfeit losses from foreign issuers, or due to a compromise event that occurs outside of the US.

---

### **CAMS Alerts and Issuer Response**

**Q: Since issuers are only receiving recovery for magnetic-stripe (POS 90) counterfeit fraud transactions that occur up to 30 days after the related CAMS alert date, does Visa suggest closing all accounts that appear on a CAMS alert to avoid future losses?**

A: No. For most compromise events, a very small percentage of the account numbers involved in a compromise event, on average, actually experience magnetic-stripe (POS 90) counterfeit fraud. Therefore it may not be practical or a good business practice to automatically reissue all accounts. However, each event is unique and each issuer may have different experiences with each event. Therefore, issuers must make their own business decision as to when and if an account is closed based on their internal procedures and knowledge.

---

### **Contacts and Further Information**

**Q: Who should members contact if they have questions pertaining to the ADCR recovery processes?**

A: For general questions regarding the counterfeit fraud or operating expense recovery processes send an e-mail to [eSupport@visa.com](mailto:eSupport@visa.com).

For general questions regarding enrollment in the operating expense recovery process send an e-mail to [eSupport@visa.com](mailto:eSupport@visa.com).

**Q: Where can I learn more about the Visa Fraud Reporting System (FRS)?**

A: Refer to the *Visa Fraud Reporting System User's Guide*. You can also contact your Visa Account Executive or call (888) 847-2242 for a Visa subject matter expert.

---

### **Miscellaneous**

**Q: Why are repeat account numbers excluded?**

A: Repeat account numbers are excluded so that members are not paid twice for the same fraud.

**Q: What if a member's PIN processor doesn't support the fraud reporting process to BASE II on Plus and Interlink transactions?**

A: When ADCR becomes available for Plus and Interlink, fraud reporting will be required in order to participate.

**Q: Will Visa accept Fair Isaac or Star reporting for the PIN transactions?**

A: Fraud reporting must be done through the Visa system.

**Q: Will acquirers be able to upload compromised account numbers in CAMS in smaller batches to avoid the 10,000 account number requirement?**

A: No. Visa will aggregate those that are received within a short time of one another.

**Q: How can members confirm if they or their sponsored issuers are enrolled in CAMS?**

A: To find out whether a BID is enrolled in CAMS, members can submit an e-mail to [eSupport@visa.com](mailto:eSupport@visa.com) and provide the BID of the sponsoring member, or the BIN that is used by the associate member. Sponsoring members may request a CAMS alert registration form by sending an e-mail to the same address.

**Q: How do members import ADCR to processors who provide fraud recovery support?**

A: Processors need to properly submit fraud reports on behalf of the financial institutions they support. Visa will handle all other components of the process.

**Q: Can multiple people be designated to receive ADCR statements or access to CAMS alerts?**

A: Yes. Additional recipients (maximum of three) may also enroll to receive the ADCR statements or have access to CAMS alerts.



