

PCI DSS Incident Response Template

Mastercard Specific Steps

VISA Specific Steps

American Express Specific Steps

MasterCard Specific Steps:

- Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100.
- Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail, to compromised_account_team@mastercard.com.
- Provide the MasterCard Merchant Fraud Control Department with the complete list of all known compromised account numbers.
- Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).
- Provide weekly written status reports to MasterCard, addressing open questions and issues, until the audit is complete to the satisfaction of MasterCard.
- Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
- Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.
- Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:
- Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs
- Distribute the account number data to its respective issuers.

Visa U.S.A. Specific Steps:

Steps and Requirements for Compromised Entities

Immediately contain and limit the exposure.

- To prevent further loss of data, conduct a thorough investigation of the suspected or confirmed loss or theft of account information within 24 hours of the compromise. To facilitate the investigation:
 - Do not access or alter compromised systems (i.e., don't log on at all to the machine and change passwords, do not log in as ROOT).* 1
 - Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug cable).
 - Preserve logs and electronic evidence.
 - Log all actions taken.
 - If using a wireless network, change Service Set Identifier (SSID) on the access point and other machines that may be using this connection (with the exception of any systems believed to be compromised).
 - Be on HIGH alert and monitor all Visa systems.
-

Alert all necessary parties, including:

- Internal information security group and Incident Response Team, if applicable
- Legal department
- Merchant bank
- Visa Fraud Control Group at (650) 432-2978
- Local FBI Office U.S. Secret Service – if Visa payment data is compromised

Provide the compromised Visa account to Visa Fraud Control Group at (650) 432-2978 within 24 hours.

- Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to Issuers and ensure the confidentiality of entity and non-public information.

Requirements for Compromised Entities

- All merchant banks must:
- Within 48 hours of the reported compromise, proof of Cardholder Information Security Program compliance must be provided to Visa.
- Provide an incident report document to Visa within four business days of the reported compromise
- Depending on the level of risk and data elements obtained the following must be completed within four days of the reported compromise:
- Undergo an independent forensic review
- A compliance questionnaire and vulnerability scan upon Visa's discretion

Steps for Merchant Banks

1. Contact Visa USA Fraud Control Group immediately at (650)432-2978
2. Participate in all discussions with compromised entity and Visa USA
3. Engage in a Visa approved security assessor to perform the forensic investigation
4. Obtain information about compromise from the entity
5. Determine if compromise has been contained
6. Determine if an independent security firm has been engaged by the entity
7. Provide the number of compromised Visa accounts to Visa Fraud Control Group within 24 hours
8. Inform Visa of investigation status within 48 hours
9. Complete steps necessary to bring entity into compliance with CISP according to timeframes described in "What to do if Compromised"
10. Ensure that entity has taken steps necessary to prevent future loss or theft of account information, consistent with the requirements of the Visa USA Cardholder Information Security Program

American Express Specific Steps:

- Within 24 hours of an account compromise event, notify American Express Merchant Services at (800) 528-5200.
- Prepare a detailed written statement of fact about the account compromise including the contributing circumstances.
- Prepare a list of all known compromised account numbers.
- Obtain additional specific requirements from American Express.