



Cardholder Information Security
Program (CISP)

What To Do If Compromised

Prepared by Visa USA 11/14/05





Table of Contents

Introduction	1
Security Breach Reporting	2
Steps and Requirements for Compromised Entities	3
Forensic Investigation Guidelines	4
Appendix A – Incident Report Template	5
Appendix B – List of Supporting Documents	7

Introduction

Recognizing what constitutes a security incident is crucial to minimizing the impact an incident might have on your organization. In general, incidents may be defined as deliberate electronic attacks on the communications or information processing systems. Whether initiated by a disgruntled employee, a malicious competitor or a misguided hacker, deliberate attacks often cause damage and disruption equal to or greater than any natural disaster. How you respond to and handle an attack on your company's information systems determines how well you will be able to control the costs and consequences that could result. For these reasons, the extent to which you prepare for security incidents and work with Visa USA will be vitally important to the protection of your company's key information.

In the event of a security incident, merchants or agents must take immediate action to investigate the incident, limit the exposure of cardholder data, notify their Merchant Bank and Visa, and report investigation findings. This "What To Do If Compromised" guide contains step-by-step instructions on how to respond to a security incident. In addition to the general instructions provided here, Visa may also require an investigation that includes, but is not limited to, providing access to premises and all pertinent records, including copies of analysis.¹

¹ *Visa U.S.A. Inc. Operating Regulations*, Volume 1, Section 2.3.F.4.b

Security Breach Reporting

In the event of a security breach, the **Visa U.S.A. Inc. Operating Regulations** require Members to immediately report the breach and the suspected or confirmed loss or theft of any material or records that contain cardholder data. Members must, upon completion of the investigation, demonstrate their ability or their merchants' or agents' ability to prevent future loss or theft of transaction information consistent with the CISP requirements. Visa USA, or an independent third party acceptable to Visa, must verify this ability by conducting a subsequent security review.

If Visa determines that an entity has been deficient or negligent in securely maintaining account information or reporting or investigating the loss of this information, Visa may require immediate corrective action.²

If a merchant or its agent does not comply with the security requirements or fails to rectify a security issue, Visa may:

- Fine the Member institution,
- Impose restrictions on the merchant or its agent, or
- Permanently prohibit the merchant or its agent from participating in Visa programs.

² Visa U.S.A. Inc. *Operating Regulations*, Volume 1, Section 2.3.F.5

Steps and Requirements for Compromised Entities

Merchants and service providers that have experienced a suspected or confirmed security breach must take prompt action to help prevent additional damage and adhere to CISP requirements.

1. **Immediately contain and limit the exposure.** Prevent the further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information. 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).
 - 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 SSID on the AP 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.
2. **Alert all necessary parties immediately.** Be sure to contact:
 - Your internal information security group and incident response team.
 - Your merchant bank.
 - The Visa Fraud Control Group immediately at (650) 432-2978.
 - Your local office of the Secret Service.
3. **Provide all compromised Visa accounts to Visa Fraud Control Group within 24 hours.** All potentially compromised accounts must be provided and transmitted as instructed by the Visa Fraud Control Group. Visa will distribute the compromised Visa account numbers to Issuers and ensure the confidentiality of entity and non-public information.
4. **Within four business days of the reported compromise:**
 - Provide an *Incident Response Report* document to Visa. (See Appendix A for report template.)
 - Depending on the level of risk and data elements obtained, undergo an independent forensic review and perform a compliance questionnaire and vulnerability scan upon Visa's discretion.

Key Point to Remember

To minimize the impact of a cardholder information security breach, Visa has put together an Incident Response Team to assist in forensic investigations. In the event of a compromise, Visa will coordinate a team of forensic specialists to go on-site immediately to help identify security deficiencies and control exposure. The forensic information collected by the team is often used as evidence to prosecute criminals.

Forensic Investigation Guidelines

In the event of a compromise, Visa USA or the acquiring Visa Member will engage an independent security firm to perform a forensic investigation on compromised entities.

The following actions will be included as part of the forensic investigation:

- **Determine cardholder information at risk.** This includes:
 - Number of accounts at risk, identify those stored and compromised on all test, development, and production systems
 - Type of account information at risk:
 - Account number
 - Expiration date
 - Cardholder name
 - Cardholder address
 - CVV2
 - Full magnetic stripe data (e.g., Track 1 and 2)
 - PIN blocks
 - Identify any data exported by intruder
 - Provide timeframe of account numbers stored and compromised
 - If applicable, forensic team to run a packet-sniffer on compromised entity's network
- **Perform incident validation and assessment:**
 - Establish how compromise occurred
 - Identify the source of compromise
 - Determine timeframe of compromise
 - Review entire network to identify all compromised or affected systems, considering the e-commerce, corporate, test, development, and production systems as well as VPN, modem, DSL and cable modem connections, and any third-party connections
 - Determine if compromise has been contained
- **Check for CVV2, Track 1 and Track 2 storage.** Examine all potential locations—including payment application—to determine if CVV2, Track 1, Track 2, or PIN blocks are stored, whether encrypted or unencrypted—e.g., in production or backup tables or databases, databases used in development, application logs, transaction logs, stage or testing environment data on software engineers' machines, etc.
- **If full track data, CVV2, or PIN blocks are stored by a payment application, identify the vendor name, product name and version number.**
- **If applicable, review VisaNet endpoint security and determine risk.**
- **Preserve all potential electronic evidence on a platform suitable for review and analysis by a court of law if needed.**
- **Perform remote vulnerability scan of entity's Internet facing site(s).**

Appendix A – Incident Report Template

The report content and format standards outlined below must be followed when completing the *Incident Response Report*. Once completed, the report must be distributed to Visa, Member and the compromised entity. Visa will classify the report as “Visa Secret.”³

I. Executive Summary:

- Provide overview of the incident
 - Include Risk Level (High, Medium, Low) during forensic analysis
 - Specify if compromise has been contained

II. Background

III. PCI Status

- Based on findings identified on the forensic investigation, list non-compliant PCI requirements

IV. Network Infrastructure Overview

- Include a diagram of the network

V. Investigative Procedures

- Include forensic tools used during investigation

VI. Findings

- Type of account information at risk:
 - ✓ Account number
 - ✓ Expiration date
 - ✓ Cardholder name
 - ✓ Cardholder address
 - ✓ CVV2
 - ✓ Track 1 and Track 2
 - ✓ PIN blocks
- Number of accounts at risk
- Timeframe of accounts at risk
- Timeframe of compromise and source of compromise

³ This classification applies to the most sensitive business information, which is intended for use within Visa. Its unauthorized disclosure could seriously and adversely impact Visa, its employees, member banks, business partners, and/or the Brand.

- Identify any data exported by intruder.
- Provide specifics on firewall, infrastructure, host, and personnel findings.
- If no hacker utilities/tools were found, explain how intrusion could occur.
- Identify any third-party payment application, including product version.

VII. Compromised Entity Action

VIII. Recommendations

IX. Contact(s) at entity and security assessor performing investigation

Appendix B – List of Supporting Documents

To perform the steps for CISP compliance validation described in this guide, you will need to download the following documents at www.visa.com/cisp.

- **Qualified Security Assessor List** – List of assessors qualified to perform CISP assessments for those entities requiring onsite validation of CISP compliance.
- **Qualified Incident Response Assessor List** – List of assessors qualified to perform incident response and forensic investigations for compromised entities.
- **PCI Data Security Standard** – Detailed security requirements, to which merchants and service providers must adhere to ensure the protection of cardholder data.
- **PCI Security Audit Procedures** – Detailed security requirements, guidelines and testing procedures to assist an independent third-party security firm verify that an entity is in compliance with the PCI Data Security Standard.
- **PCI Self-Assessment Questionnaire** – The Questionnaire must be completed by Level 2 and 3 merchants and Level 3 service providers as part of CISP compliance validation. Responses must address any system(s) or system component(s) involved in processing, storing, or transmitting Visa cardholder data.
- **PCI Security Scanning Procedures** – Procedures and guidelines for conducting network security scans for merchants and third party service providers who are scanning their infrastructures to demonstrate CISP compliance.