What To Do if Compromised

Visa Fraud Investigations and Incident Management Procedures

December 2007

Table of Contents

Introduction

What constitutes a security incident? The answer to this question is crucial to any organization looking to minimizing the impact an incident might have on its business operations. 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 to the payment system. 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 Inc., will be vitally important to the protection of your company's key information.

In the event of a security incident, Visa clients and their agents must take immediate action to investigate the incident, limit the exposure of cardholder data, notify Visa, and report investigation findings.

This *What To Do If Compromised* guide is intended for Visa clients. It 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; *Plus System Inc., Bylaws and Operating Regulations,* Section 1.19.; and the *Interlink Inc., Bylaws and Network Operating Regulations, Section 1.5.C.*

Identifying and Detecting Security Breaches

It is often difficult to detect when a system has been attacked or an intrusion has taken place. Distinguishing normal events from those that are related to an attack or intrusion is a critical part of maintaining a secure payment processing environment. Security breaches come in many different forms, and while detecting them may be challenging, there are several signs that you have been the victim of a security breach:

- Unknown or unexpected outgoing Internet network traffic from the cardholder environment
- Presence of unexpected IP addresses on store and wireless networks
- Unknown or unexpected network traffic from store to headquarter locations
- Unknown or unexpected services and applications configured to launch automatically on system boot
- Anti-virus programs malfunctioning or becoming disabled for unknown reasons
- Failed login attempts in system authentication and event logs
- Vendor or third-party connections to the cardholder environment without prior consent and/or a trouble ticket
- SQL Injection attempts in web server event logs
- Authentication event log modifications (i.e. unexplained event logs being deleted)
- Suspicious after-hours file system activity (i.e. user login or activity to POS server after-hours)
- Presence of .zip, .rar, .tar, and other types of unidentified compressed files containing cardholder data

Security Breach Reporting

The *Visa U.S.A. Inc. Operating Regulations,* the *Plus System Operating Regulations*, and the *Interlink Network Operating Regulations,* require that clients comply with the Visa Cardholder Information Security Program (CISP) by immediately reporting a security breach and the suspected or confirmed loss or theft of any material or records that contain cardholder data. Clients must, upon completion of the investigation, demonstrate their ability and their agents' ability to prevent future loss or theft of transaction information consistent with the CISP requirements. The client must permit Visa Inc., or an independent third party acceptable to Visa, to verify this ability by conducting a subsequent security review.

If Visa determines that a client or its agent 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]

An acquirer that fails to comply with the requirements is subject to fines and penalties.

[2] *Visa U.S.A. Inc. Operating Regulations,* Volume 1, Section 2.3.F.5; *Plus System Inc., Bylaws and Operating Regulations*, Section 1.19.; and the *Interlink Inc., Bylaws and Network Operating Regulations,* Section 1.5.C.

Steps and Requirements for Compromised Entities

Entities that have experienced a suspected or confirmed security breach must take prompt action to help prevent additional exposure of cardholder data and ensure compliance with the PCI Data Security Standards and Payment Card Industry (PCI) PIN Security 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 preserve evidence and 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 systems with cardholder data.
2. **Alert all necessary parties immediately.** Be sure to contact:
   - Your internal information security group and incident response team.
   - Your merchant bank.
   - If you do not know the exact name and/or contact information for your merchant bank, notify the Visa Fraud Investigations and Incident Management group immediately at (650) 432-2978.
   - Your local office of the United States Secret Service.

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 onsite immediately to help identify security deficiencies and control exposure. The forensic information collected by the team is often used as evidence to prosecute criminals.

3. **Provide all compromised Visa, Interlink, and Plus accounts to your merchant bank within 10 business days.** All potentially compromised accounts must be provided and transmitted as instructed by your merchant bank and Visa Investigations and Incident Management group. Visa will distribute the compromised Visa account numbers to Issuers and ensure the confidentiality of entity and non-public information.

FOR MORE INFORMATION

To find out more about data transaction requirements, see the *Requirements for Account Data Requests* section on page 8 of this guide.

4. **Within 3 business days of the reported compromise, provide an *Incident Response Report* document to your merchant bank.** (See Appendix A for the report template.)

Note: Visa, in consultation with your merchant bank, will determine whether or not an independent forensic investigation will be initiated on the compromised entity.

Forensic Investigation Guidelines

A Visa client must ensure that a Qualified Incident Response Assessor (QIRA) is engaged to perform a forensic investigation.

Forensic Investigations must be conducted using the following scope and methodology:

- QIRA will assess compromised entity's computing environment to identify relevant sources of electronic evidence
  - Assess all external connectivity points within each location involved
  - Assess network access controls between compromised system(s) and adjacent and surrounding networks
- Acquire electronic evidence from compromised entity's host and network-based systems
  - Forensic evidence acquisition must be conducted onsite at the compromised entity's premises
  - If circumstances do not permit onsite evidence acquisition, notification to Visa Fraud Investigations is required
- Forensically examine electronic evidence to find cardholder data and establish an understanding of how a compromise may have occurred
- Verify cardholder data is no longer at risk and/or has been removed from the environment
- Present forensic investigation findings to all parties involved in the incident

KEY POINT TO REMEMBER

Visa reserves the right to engage the team.

The following actions are 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:
  - Full magnetic-stripe data (e.g., Track 1 and 2)
  - PIN blocks
  - CVV2
  - Account number
  - Expiration date

  - Other sensitive data elements (e.g., SSN, DOB)
  - Cardholder name
  - Cardholder address
- All data exported by intruder
- The timeframe of account numbers stored and compromised

Note: If applicable, the forensic team must 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 the 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 Track 1 and Track 2 data, CVV2, and/or PIN block storage.** Examine all potential locations—including payment application—to determine if CVV2, Track 1, and Track 2 data, and/or PIN blocks are stored, whether encrypted or unencrypted (e.g., in production or backup databases or tables used in development, application logs, transaction logs, trouble-shooting or exception files, stage or testing environment data on software engineers' machines, etc.).

❒ **If full-track data, CVV2, and/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 external and internal vulnerability scan.**

Appendix A: Incident Report Template

This appendix section contains the content and format standards that must be followed when completing the *Incident Response Report.*

The *Incident Response Report* can be completed by the compromised entity or the independent forensic investigator. Once completed, the report must be distributed to Visa, the client and the compromised entity. Visa will classify the report as "Visa Secret."[3]

[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, client banks, business partners, and/or the Brand.

Incident Report Template

I. Executive Summary:

Include the following:

- Date of when forensic company was engaged
- Date(s) when forensic investigation began
- Location(s) visited or reviewed
- A brief summary of the environment reviewed (Details should be documented under the Findings section.)
- If identified, list cause of intrusion
- Date(s) of intrusion
- List suspected cause of intrusion
- Specification as to whether or not the compromise has been contained
- Type of account information at risk:
  - Track 1 and Track 2
  - PIN blocks
  - CVV2
  - Account number
  - Expiration date
  - Cardholder name
  - Cardholder address
  - Number of accounts at risk
  - Timeframe of accounts at risk

(See a sample of Incident Dashboard on the following page)

II. Background

- Brief summary of compromised entity company:
  - Type of company
  - Number of locations
  - Parent company (if applicable)

Incident Dashboard

CLIENT	Level <1, 2, 3 or 4> Merchant <or Service Provider>
Compromise Identification Date	
Method of Identification	☐ Self Detection ☐ CPP
Date of Engagement	
Date of Onsite	
Type of Environment	☐ eCommerce ☐Brick & Mortar ☐SP
Type of Data	☐ Cardholder Name ☐ Cardholder Address ☐ PAN ☐ Expiry ☐ CVV2/CVC2/CID ☐ Track Data ☐ Encrypted PINs
Type of Track Data	☐ Track 1 ☐ Track 2
Brand Exposure	☐ VISA ☐ MC ☐ DISC ☐ AMEX ☐ JCB
Number of Cards in Live System Space	[Include breakdown by card brand type]
Number of Cards in Unallocated Space	[Include breakdown by card brand type]
Logs that provided evidence: ☐ Firewall Logs ☐ Intrusion Detection Systems ☐ Database Queries ☐ FTP Server Logs ☐ System Login Records ☐ Web Server Logs	☐ File-Integrity Monitoring Output ☐ Transaction Logs ☐ Remote Access Logs ☐ Wireless Connection Logs ☐ Anti-Virus Logs ☐ Security Event Logs ☐ File Creation/Access Date
Suspected Cause Summary:	
[INSERT BRIEF CASE SUMMARY. DETAILED FINDINGS SHOULD BE INCLUDED ON THE FINDINGS SECTION OF THE REPORT.]	
Date of Intrusion	
Duration of Intrusion	
Data Exported by Intruder	☐ Yes ☐ No ☐ Unknown
Law Enforcement Notified	☐ Local ☐ USSS ☐ FBI ☐ Other

III. PCI Status

Based on findings identified on the forensic investigation, indicate the compliance status for each of the twelve basic requirements under the CISP PCI Data Security Standard.

PCI Data Security Standard		
Requirements	In Place	Not in Place
Build and Maintain a Secure Network		
Requirement 1: Install and maintain a firewall configuration to protect cardholder data		
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters		
Protect Cardholder Data		
Requirement 3: Protect stored cardholder data		
Requirement 4: Encrypt transmission of cardholder data across open, public networks		
Maintain a Vulnerability Management Program		
Requirement 5: Use and regularly update anti-virus software		
Requirement 6: Develop and maintain secure systems and applications		
Implement Strong Access Control Measures		
Requirement 7: Restrict access to cardholder data by business need-to-know		
Requirement 8: Assign a unique ID to each person with computer access		
Requirement 9: Restrict physical access to cardholder data		
Regularly Monitor and Test Networks		
Requirement 10: Track and monitor all access to network resources and cardholder data		
Requirement 11: Regularly test security systems and processes		
Maintain an Information Security Policy		
Requirement 12: Maintain a policy that addresses information security		

IV: Network Infrastructure Overview

Provide a diagram of the network that includes the following:

- Cardholder data sent to central corporate server or data center
- Upstream connections to third-party processors
- Connections to Visa client bank networks
- Remote access connections by third-party vendors or internal staff
- Inbound/outbound network connectivity
- Network security controls and components (network security zones, firewalls, etc.)
- Clearly identify all infrastructure components implemented or modified after the timeframe of the compromise

VI: Findings

- Provide specifics on firewall, infrastructure, host, and personnel findings
- Identify any and all changes made to compromised entity's computing environment after the identification of a compromise
  - Provide specific dates of network, system, or Point of Sale (POS) changes
  - Include any and all forensic evidence supporting changes made to networks, systems, and POS components
- Identify any data accessed by unauthorized parties
- Identify any data exported by unauthorized parties
- Identify any evidence of data deletion from systems involved in a compromise
- If applicable, identify any deleted data recovered through forensic file recovery methods
- Identify any third-party payment applications, including product version
- Provide a timeline of incident events

Appendix B: List of Supporting Documents

This appendix section includes a list of the documents you need to perform the Visa CISP and PCI PIN Security compliance validation steps outlined in this guide.

List of Supporting Documents

The following documents can be downloaded at *www.visa.com/cisp* and *www.visa.com/pin.*

- **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 entities 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 Standards.
- **PCI Self-Assessment Questionnaire** – The PCI Self-Assessment Questionnaire (SAQ) is an important validation tool that is primarily used by smaller merchants and service providers to demonstrate compliance to the PCI DSS. Responses must address any system(s) or system component(s) involved in processing, storing, or transmitting Visa cardholder data. For any answers where N/A is marked, a brief explanation should be attached.
- **PCI Security Scanning Procedures** – Procedures and guidelines for conducting network security scans for entities and third-party service providers who are scanning their infrastructures to demonstrate CISP compliance.
- **PCI PIN Security Requirements** (*www.visa.com/pin*)
- **Visa PIN Security Program Auditor's Guide** (*www.visa.com/pin*)

Appendix C: Glossary of Terms

Acquirer	Financial institution that enters into agreements with merchants to accept Visa cards as payment for goods and services. Commonly referred to as the merchant bank.
Agent	Any contractor, including third-party processors and servicers, whether a client or non-client, engaged by a client to provide services or act on its behalf in connection with the Visa payment services.
At Risk Accounts	Refers to accounts that were included in a suspected or confirmed compromised data file.
Authentication	The process of verifying the true origin or nature of the sender and/or the integrity of the text of a message.
Authorization	A process by which an issuer approves a transaction for a specified amount with a merchant.
Bank Identification Number (BIN)	Bank identification number. A unique number assigned by the bankcard association to its members. On a cardholder's account number, the BIN appears as the first six digits. Visa BINs begin with a "4."
Card Authorization Acceptor ID	Information found in the authorization message (Field 42) from a legitimate transaction at the Acceptor ID CPP identified merchant.
Card-Not-Present	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-Present	A merchant, market, or sales environment where a transaction can be completed only if both a valid Visa card and cardholder are present and the sale is processed by an individual representing the merchant or acquirer. Card-present transactions include face-to-face retail sales and cash disbursements.
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 Visa fraud prevention system used in card-not-present transactions to ensure that the card is valid. The CVV2 is the three-digit value that is printed on the back of all Visa cards. Card-not-present merchants ask the customer for the CVV2 and submit it as part of their authorization request. For information security purposes, merchants are prohibited from storing CVV2 data.
Cardholder	The person or entity whose name is embossed on the face of a card or encoded on the magnetic stripe.

Cardholder Data	All identifiable personal data about the cardholder and relationship to the client (e.g., account number, expiration date, data provided by the client, other electronic data gathered by the merchant/agent). This term also accounts for other personal insights gathered about the cardholder such as address, telephone number, etc.
Client	An organization which is a member of Visa and which issues cards and/or signs merchants.
Compromise	In cryptography, the breaching of secrecy and/or security. A violation of the security of a system such that an unauthorized disclosure of sensitive information may have occurred. This includes the unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other keying material).
Compromised Account	Accounts downloaded by an intruder or found in criminal possession.
Compromised Account Management System (CAMS)	Via CAMS, acquirers, merchants, and law enforcement officers can safely 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.
Electronic Commerce (e-Commerce)	The purchase of goods and services over the Internet without a paper transaction between buyer and seller.
Entity	For payment and industry purposes, an entity is any organization that must be PCI compliant. Compliance is mandatory for any organization type and/or systems that stores, processes or transmits cardholder data. An entity could be an Acquirer, service provider, a merchant, or merchant's agent.
Encryption	An online data security method scrambling data so that it is difficult to interpret without a corresponding decryption key.
Full-Track Data	There are two tracks of data on a bankcard's magnetic-stripe: • **Track 1** is 79 characters in length. It is alpha-numeric and contains the account number, the cardholder name, and the additional data listed. • **Track 2** is the most widely read. It is 40 characters in length, and is strictly numeric. This track contains the account number, expiration date, the secure code, and discretionary institution data.
Hacker	A person who deliberately logs on to other computers by circumventing the log-on security system. This is sometimes done to steal valuable information or to cause damage that might be irreparable.

Magnetic Stripe (Mag Stripe)	A strip of magnetic tape on the back of all bankcards. The magnetic stripe is encoded with identifying 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.
Merchant	A principal or entity entering into a card acceptance agreement with a Visa client financial institution.
Merchant Bank	See "Acquirer."
Payment Card Industry (PCI) Data Security Standard	A set of requirements established by the Payment Card Industry to protect cardholder data. These requirements apply to all members, merchants, and service providers that store, process, or transmit cardholder data.
Payment Card Industry (PCI) PIN Security Requirements	A comprehensive set of measures for the safe transmission and processing of cardholder PINs during ATM and (POS) PIN-entry device (PED) transactions. All participants in the payment processing chain that manage cardholder PINs and encryption keys must be in full compliance with the *PCI PIN Security Requirements* This document can be downloaded from the PIN website at *www.visa.com/pin*
Personal Identification Number (PIN)	An alphabetic and/or numeric code which may be used as a means of cardholder identification.
Qualified CISP Incident Response Assessor List	Visa-approved security vendors to perform forensic investigations in the event of a security incident.
Qualified Data Security Company (QDSC)	A security company that has been qualified by PCI SSC to perform a PCI Data Security Assessment according to the PCI Security Audit Procedures. Please visit the *PCI Security Standards Council* website (*www.pcisecuritystandards.org*) for details on the PCI program requirements.
Third-Party Processor	A service provider organization that is acting as the agent of a client to provide authorization, clearing, or settlement services for merchants and members.
Third-Party Servicer	A service provider organization that is not a client of Visa and is not directly connected to VisaNet, but provides the following services to the client: • Response processing for Visa program solicitations • Transaction processing, including gateways • Data capture • Other administrative functions, such as chargeback processing, risk/security reporting, and customer service

Visa Cardholder Information Security Program (CISP)	A Visa program that establishes data security standards, procedures, and tools for all entities—merchants, service providers, issuers, and merchant banks—that store Visa cardholder account information. CISP compliance is mandatory. CISP requirements prohibit merchants and service providers from storing the full contents of any magnetic stripe, CVV2, or PIN block data. For more information regarding CISP, visit *www.visa.com/cisp.*
VisaNet	The data processing systems, networks and operations that are used to support and deliver authorization services, exception file services, clearing and settlement services and any other services.