



What To Do If Compromised

Visa Inc. Fraud Control and Investigations Procedures

Version 3.0 (Global)

Effective May 2011

Visa Public



Table of Contents

Introduction	1
Identifying and Detecting Security Breaches	2
Attack Vectors	3
SQL Injection Attacks	3
Improperly Segmented Network Environment	3
Malicious Code Attacks	3
Insecure Remote Access	4
Insecure Wireless	5
Steps and Requirements for Compromised Entities	6
Steps and Requirements for Visa Clients (Acquirers and Issuers)	8
Notification	8
Preliminary Investigation	8
Independent Forensic Investigation	8
PIN Security	9
Account Numbers	9
PCI DSS Compliance	10
Requirements for Account Data Requests	11
Account Data Format	11
Account Data Upload	12
Compromised Account Management System (CAMS)	13

Introduction

What constitutes a security incident? The answer to this question is crucial to any organization looking to minimize the impact an incident might have on its business operations.

In general, incidents may be defined as deliberate electronic attacks on 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 will determine 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 to Visa.¹

The *What To Do If Compromised* guide is intended for Visa clients (i.e., acquirers and issuers), merchants, agents, and third-party service providers. It contains step-by-step instructions on how to respond to a security incident and provides specific time frames for the delivery of information or reports outlining actions taken by Visa, its clients, and its agents.

In addition to the general instructions provided here, Visa may also require an investigation that includes, but is not limited to, access to premises and all pertinent records including copies of analysis.

¹ *Visa International Operating Regulations*, General Investigation Responsibilities, ID #7123,, Prevention of Loss or Theft of Information, ID #5605, Additional Investigation, ID #7124. See Appendix J for more information on Visa International Operating Regulations.

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 certain signs that tend to appear when a security breach has occurred:

- Unknown or unexpected outgoing Internet network traffic from the payment card environment
- Presence of unexpected IP addresses or routing
- Unknown or unexpected network traffic from store to headquarter locations
- Unknown or unexpected services and applications configured to launch automatically on system boot
- Unknown files, software and devices installed on systems
- Unexplained modification or deletion of data
- Anti-virus programs malfunctioning or becoming disabled for unknown reasons
- Excessive failed login attempts in system authentication and event logs
- Vendor or third-party connections made to the cardholder environment without prior consent and/or a trouble ticket
- SQL Injection attempts or strange code in web server logs
- Authentication event log modifications (i.e., unexplained event logs are being deleted)
- Suspicious after-hours file system activity (i.e., user login or after-hours activity to Point-of-Sale (POS) server)
- Presence of a rootkit, which hides certain files and processes in, for example, Explorer, the Task Manager, and other tools or commands
- Systems rebooting or shutting down for unknown reasons
- Unexpected file lengths, sizes or dates, especially for system files
- Unexplained new user accounts
- Presence of archived/compressed files in system directories
- Variances in log chronology or timestamps
- If you are running Microsoft®, check Windows® registry settings for hidden malicious code. (**Note:** Make sure you back up your registry keys before making any changes and consult with Microsoft Help and Support).

Attack Vectors

The following are examples of attack vectors that hackers use to gain unauthorized access to organization's systems and steal sensitive information, such as payment card data and passwords.

SQL Injection Attacks

SQL injection is a technique used to exploit Web-based applications that use client-supplied data in SQL queries. SQL injection attacks can occur as a result of unpatched Web servers, improperly designed applications (i.e., incorrectly filtered escape characters or error-type handling) or poorly configured Web and database servers.

The SQL attack methods most recently detected were targeted against Websites and Web applications that were improperly designed or resided on unpatched systems, making them susceptible to attack. These latest SQL injection attacks pose serious additional risks to cardholder data stored or transmitted within systems (e.g., Microsoft and UNIX-based) and networks connected to the affected environment.

Improperly Segmented Network Environment

Payment card account information has been compromised at organizations that lack proper network segmentation. This attack method originates on the Internet, resulting in penetration to the organization's payment card environment and often leading to costly remediation efforts and increased fraud attacks. Such compromises can often be prevented if the organization's networks are properly segmented, limiting intruders to non-sensitive parts of the network that do not contain payment card information.

Network segmentation is a concept that refers to the practice of splitting a network into functional segments and implementing an access control mechanism between each of the boundaries. The most common example of network segmentation is the separation between the Internet and an internal network using a firewall/router.

Malicious Code Attacks

Malicious codes or malware can be programs such as viruses, worms, Trojan applications, and scripts used by intruders to gain privileged access and capture passwords or other confidential information (e.g., user account information). Malicious code attacks are usually difficult to detect because certain viruses can be designed to modify their own signatures after inflicting a system and before spreading to another. Some malicious codes can also modify audit logs to hide unauthorized activities.

In recent investigations, Visa has identified malicious codes designed to capture payment card data. These are examples of malicious code attacks:

- **Malware that allows interactive command shell or backdoor.** This type of malware allows an intruder to run commands to the compromised system. In some cases, the malware is hard-coded with the intruder's Internet Protocol (IP) address.
- **Packet sniffers.** Packet sniffing is the practice of using computer software or hardware to intercept and log traffic passing over a computer network. A packet sniffer, also known as a network analyzer or protocol analyzer, captures and interprets a stream or block of data (referred to as a "packet") traveling over a network.

Packet sniffers are typically used in conjunction with malicious software or malware. Once intruders gain entry into a critical system using backdoor programs or deploying rootkits, the sniffer programs are installed, making the malware more difficult to detect. Intruders can then "sniff" packets between network users and collect sensitive information such as usernames, passwords, payment card data or Social Security numbers. Once a critical system or network is compromised, sniffers are used to eavesdrop or spy on network users and activity. This combination of tools makes this attack scheme effective in compromising systems and networks.

- **Key logger malware.** Key logging is a method of capturing and recording keystrokes. There are key logger applications that are commercially available and are used by organizations to troubleshoot problems within computer systems. Visa Investigations reveal that there are key logger applications that are developed by intruders to capture payment card data and/or users credentials, such as passwords. The key logger captures information in real time and sends it directly to the intruder over the Internet. Additionally, newer advances provide the ability to intermittently capture screenshots from the key logged computer.

Key logger malware are widely available via the Internet and can be installed on virtually any operating system. Key loggers, like most malware, are distributed as part of a Trojan horse or virus, sent via e-mail (as an attachment or by clicking to an infected web link or site) or, in the worst case, installed by a hacker with direct access to a victim's computer.

Insecure Remote Access

Many Point-of Sale (POS) and ATM vendors, resellers, and integrators have introduced remote access management products into the environments of organizations that they support. A variety of remote access solutions exists, ranging from command-line based (e.g., SSH, Telnet) to visually-driven packages (e.g., pcAnywhere, Virtual Network Computing, Remote Desktop). The use of remote management products comes with an inherent level of risk that may create a virtual backdoor on your system. The exploitation of improperly

configured and unpatched remote management software tools is the method of attack most frequently used by hackers against POS payment systems. An improperly configured system can be vulnerable in the following ways:

- Remote access ports and services always listening from the Internet.
- Use of default password or no password.
- Lack of two-factor authentication.
- Lack of a properly configured firewall.
- Disabled logging mechanisms eliminate insight into system access activity and signs of intrusion.

Insecure Wireless

The adoption of wireless technology is on the rise among participants in the payment industry; particularly merchant retailers, many of whom use wireless technology for inventory systems or check-out efficiency (e.g., “line busting,” ringing up customers while they are in line). Wireless technologies have unique vulnerabilities; organizations must carefully evaluate the need for such technology and understand the risks, as well as the security requirements, before deploying wireless systems.

Following are some of the common methods used to attack wireless networks. These methods are widely documented on the Internet, complete with downloadable software and instructions.

- **Eavesdropping** — An attacker can gain access to a wireless network just by “listening” to traffic. Radio transmissions can be freely and easily intercepted by nearby devices or laptops. The sender or intended receiver has no means of knowing whether the transmission has been intercepted.
- **Rogue Access** — If a wireless Local Area Network (LAN) is part of an enterprise network, a compromise of the LAN may lead to the compromise of the enterprise network. An attacker with a rogue access point can fool a mobile station into authenticating with the rogue access point, thereby gaining access to the mobile station. This is known as a “trust problem,” and the only protection against it is an efficient access-authentication mechanism.
- **Denial of Service (DOS)** — Due to the nature of radio transmission, wireless LANs are vulnerable to denial-of-service attacks and radio interference. Such attacks can be used to disrupt business operations or to gather additional information for use in initiating another type of attack.
- **Man-in-the-Middle (MITM)** — Packet spoofing and impersonation, whereby traffic is intercepted midstream then redirected by an unauthorized individual for malicious purposes, are also valid threats.

For more information on additional attack vectors and mitigation strategies, please visit www.visa.com/cisp, under “Alerts, Bulletins and Webinars.”

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 Payment Card Industry Data Security Standard (PCI DSS), PCI Payment Application Data Security Standard (PA-DSS), and PCI PIN Security Requirements.

1. Immediately contain and limit the exposure. Minimize data loss. Prevent the further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information. Compromised entities should consult with their internal incident response team. To preserve evidence and facilitate the investigation:
 - Do not access or alter compromised system(s) (i.e., don't log on at all to the compromised system(s) and change passwords; do not log in as ROOT). Visa highly recommends compromised system not be used to avoid losing critical volatile data.
 - Do not turn the compromised system(s) off. Instead, isolate compromised systems(s) from the network (i.e., unplug network cable).
 - Preserve evidence and logs (i.e., original evidence, security events, web, database, firewall, etc.)
 - Document all actions taken.
 - If using a wireless network, change the Service Set Identifier (SSID) on the wireless access point (WAP) and other systems that may be using this connection (with the exception of any systems believed to be compromised).
 - Be on **high** alert and monitor traffic on all systems with cardholder data.
2. Alert all necessary parties immediately:
 - Your internal incident response team and information security group.
 - If you are a merchant, contact your merchant bank.
 - If you do not know the name and/or contact information for your merchant bank, notify Visa Incident Response Manager immediately:
 - U.S. - (650) 432-2978 or usfraudcontrol@visa.com
 - Canada - (416) 860-3090 or CanadaInvestigations@visa.com
 - Latin America & Caribbean - (305) 328-1713 or lacrmac@visa.com
 - Asia Pacific and Central and Eastern Europe, Middle East and Africa (CEMEA) - VIFraudControl@visa.com

If you are a financial institution, contact the appropriate Visa region at the number or e-mail provided above.

3. Notify the appropriate law enforcement agency. Contact the Visa Incident Response Manager above for assistance in contacting local law enforcement agency.
4. Visa has developed a communication guideline in responding to a data breach for compromised entities. There are some good basic communications principles that can be applied to most data breach situations. This guideline is intended to provide some best-practice guidance for compromised entities on how to think about, prepare for and respond to data breaches. You can download a copy of the guideline here
http://usa.visa.com/download/merchants/cisp_responding_to_a_data_breach.pdf

Key Point to Remember

To minimize the impact of a cardholder information security breach, Visa has created an Incident Response Team to assist in forensic investigations. In the event of a compromise, Visa will work with the compromised entity and assist in coordinating a team of forensic specialists to go onsite immediately to help identify security deficiencies and control exposure. The forensic information collected by this team is often used as evidence to prosecute criminals.

5. The compromised entity should consult with its legal department to determine if notification laws are applicable.
6. Provide all compromised Visa, Interlink, and Plus accounts to the Visa acquiring bank or to Visa within ten (10) business days. Acquiring entities must provide all compromised Visa Account numbers regardless if the transaction went through another regional or national network. All accounts must indicate if the transaction was Visa, Interlink, Plus or other network ID must be provided. All potentially compromised accounts must be provided and transmitted as instructed by the Visa acquiring bank and Visa. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information. **Note:** If you are an issuer, provide foreign accounts or accounts from other financial institutions to Visa.
7. Within three (3) business days of the reported compromise, provide a written documentation to the Visa client or to Visa. If you are a financial institution, provide the Incident Report to Visa.
Note: If Visa deems necessary, an independent forensic investigation by a Payment Card Industry Forensic Investigator (PFI) will be initiated on the compromised entity.

Steps and Requirements for Visa Clients (Acquirers and Issuers)

-
- Notification**
1. Immediately report to Visa the suspected or confirmed loss or theft of Visa cardholder data. Clients must contact the Visa Risk Management group immediately at the appropriate Visa region.
 2. Within 48 hours, advise Visa whether the entity was in compliance with PCI DSS and, if applicable, PCI PA-DSS and PCI PIN Security requirements at the time of the incident. If so, provide appropriate proof.

-
- Preliminary Investigation**
3. Perform an initial investigation and provide written documentation to Visa within three (3) business days. The information provided will help Visa understand the potential exposure and assist entities in containing the incident. Documentation must include the steps taken to contain the incident.

Independent Forensic Investigation

If Visa deems necessary, an independent forensic investigation must be conducted by a Payment Card Industry Forensic Investigator (PFI). Click here: https://www.pcisecuritystandards.org/approved_companies_providers/pci_forensic_investigator.php for a list of approved PFIs.

4. Upon receipt of an initial independent forensic investigation notification from Visa, clients must:
 - Identify the PFI within five (5) business days.
 - Ensure that the PFI is engaged (or the contract is signed) within ten (10) business days.
 - The PFI must be onsite to conduct a forensic investigation within five (5) business days from the date the contract agreement is signed.

The Visa client or compromised entity should engage the PFI directly. However, Visa, has the right to engage a PFI to perform a forensic investigation as it deems appropriate, and will assess all investigative costs to the client in addition to any fine that may be applicable.

Key Point to Remember

The entity must have the PFI evaluate whether the entity complies with each of the 32 PCI PIN Security Requirements, available on www.visa.com/pinsecurity.

5. If there is a suspected PIN compromise, the PFI will perform a PIN security and key management investigation and a PCI PIN security assessment.

Key Point to Remember

The PFI preliminary, final forensic reports and PIN security report templates can be downloaded at:
https://www.pcisecuritystandards.org/security_standards/documents.php?document=PFI_Program_Guide#PFI_Program_Guide.

6. Provide a preliminary forensic report to Visa within five (5) business days from the onsite review. *The PFI or the compromised entity can work with the appropriate region in the event that the preliminary report is delayed.*
7. Provide a final forensic report to Visa within ten (10) business days from the completion of the review.

Note: Visa has the right to review the forensic report and reject the report if it does not meet the PFI requirements.

PIN Security

8. If there is a suspected PIN compromise, provide a PIN security report within ten (10) business days from the onsite review. This report should also review PIN-related cryptographic keys to determine if the keys might have been compromised.

Account Numbers

9. Provide “at risk” account numbers (domestic and international) to Visa within ten (10) business days from the date that Visa requests the account numbers.
10. Ensure that the compromised entity has contained the incident and has implemented security recommendations provided by the PFI, including any non-compliance with the PCI PIN Security Requirements.
11. If the entity is retaining full-track data, CVV2, and/or PIN blocks, ensure that the entity has removed the data (this includes any historical data).
12. Validate that full-track data, CVV2, and/or PIN blocks are no longer being stored on any systems. Even though this is the client’s responsibility, Visa requires that the validation be performed by the PFI.
13. Submit a remediation plan to Visa within five (5) business days after receiving the final forensic report. As required by Visa, clients must provide a remediation plan with implementation dates related to findings identified by the PFI.
 A revised remediation plan must be provided to Visa, as needed.
14. Monitor and confirm that the compromised entity has implemented the action plan. Confirmation must be done by the PFI, or Qualified Security Assessor (QSA).

PCI DSS
Compliance

15. Ensure that the compromised entity achieves full PCI compliance by adhering to the PCI DSS, PCI PA-DSS and, if applicable, the PCI PIN Security Requirements. Compliance validation is required per *Visa International Operating Regulations*.

Key Point to Remember

Please visit www.pcisecuritystandards.org for more information on PCI DSS and the PCI PIN Entry Device Testing Program.

For more information on PCI PIN Security Requirements, please visit www.visa.com/pinsecurity.

Requirements for Account Data Requests

In the event of a compromise, Visa requires that “at risk” accounts be provided to Visa through Visa’s Compromised Account Management System (CAMS). It is important that the compromised entity or acquirer/processor provide both domestic and international accounts to Visa.

In some cases, Visa may require the entity to provide accounts via a CD using encryption software such as PGP² or Winzip³ with 256-AES encryption and strong password. The following guidelines must be followed when providing accounts to Visa:

Account Data Format

The account data provided must be **authorization** data only.

File submitted must be a plain-text, comma delimited file containing account numbers and expiration dates. For example:

- The card number, followed by a comma, followed by the expiration date in YYMM format:

4xxxxxxxxxxxxxxxx,0801

KEY POINT TO REMEMBER

Visa may require additional data for further fraud analysis and will inform the compromised entity and the Visa client if additional data is required.

1. Submitted data should be limited to **one** file. In cases where one file isn’t possible, make every effort to minimize total file counts. If multiple files are provided, all of them **MUST** be consistent (i.e., they **MUST** contain the same formatting and transaction details).
2. The following information must be provided in separate files and clearly labeled:
 - Signature and PIN-based transactions (Interlink and Plus)
 - Track and non-track data
 - Data sniffed/captured by the hacker
 - Data stored by the compromised entity
 - Data transferred out of the compromised entity’s network

² PGP (Pretty Good Privacy) is a computer program that provides cryptographic privacy and authentication. For more information on PGP, go to www.pgp.com.

³ WinZip is a data compression utility with the ability to compress using 256-AES encryption. For more information on WinZip, go to www.winzip.com.

Account Data Upload

When providing a file to Visa via Compromised Account Management System (CAMS) or copying to a CD, the user must provide a description of the data being uploaded or copied. For example:

1. Transaction date(s) of "at risk" accounts
2. Data elements at risk:
 - Primary Account Number (PAN)
 - Expiration date
 - Track 1 or 2
 - CVV2
 - PIN blocks
 - Other cardholder information, such as billing address, e-mail addresses, SSN, DOB, etc.
3. Name of compromised entity
4. Name of Visa investigator handling the incident

Key Point to Remember

Visa accounts copied to a CD or other removable media must be encrypted using PGP or Winzip with 256-AES encryption with strong password.

Compromised Account Management System (CAMS)

The Compromised Account Management System (CAMS) offers a secure and efficient way for acquirers, merchants, law enforcement agencies, and financial institutions to transmit compromised and recovered account data to and from Visa through an encrypted site. Using CAMS, acquirers, merchants, and law enforcement officers can upload potentially compromised and recovered accounts directly to Visa.

Subscribing financial institutions can access CAMS by logging on to www.us.visaonline.com and receive compromise alerts via e-mail regarding their accounts.

To Upload File(s):

1. Access the "Submit CAMS Alert" screen to upload your file data. At this screen, you must enter a description, indicate whether you are providing an expiration date, and select a file to upload from your hard drive.

Submit CAMS Alert

The screenshot shows the 'Submit CAMS Alert' form with the following elements and numbered callouts:

- 2**: A dropdown menu labeled 'Select Visa Contact:' with the text '<select one>'.
- 3**: A large text input field labeled 'Enter a Brief Description: (255 characters max)'.
- 4**: A checkbox labeled 'Check if the file includes: Expiration Date'.
- 5**: A 'Browse...' button next to a file input field labeled 'Choose a file to upload:'.
- 6**: An 'Upload' button.
- 7**: A 'Cancel' button.

There is also a 'Learn More' link with an information icon next to the 'Expiration Date' checkbox.

2. From the drop down menu, select your assigned Visa contact. **This field is required.**
3. Enter a brief description of the files you are uploading for the compromise.
4. If applicable, indicate whether the file includes an expiration date. (Indicating an account expiration date will help the issuer identify which accounts are good candidates for monitoring.)
5. Click "Browse" to select a file from your local hard drive.
 - Files must be either plain text or a .zip file containing plain text files.
 - Files cannot exceed 100 MB in size.
 - The uploaded file should contain 11-19 digit account numbers.

6. Click the "Upload" button to begin the file transfer process. *The progress box will display how much of the upload has been completed.*
7. To stop the file transfer, click the "**Cancel**" button at any time.

To Upload Additional File(s):

After a successful upload, the "Submit CAMS Alert" screen will reappear with a message that confirms that your upload has been completed successfully. You will also be asked if you would like to add another file to the same alert. If you add another file, please remember that you will only be allowed to submit one description for each alert; the first description that you submit will apply.

If an error occurs during the upload, an error message will appear and you will be asked to upload the file again. You should also receive an e-mail message describing the upload error.

In response, you can either resubmit the file or contact the CAMS Administrator at VisaRiskManager@visa.com or 1-800-439-9013 for assistance.