



# Security Incident Response Procedure





## Table of Contents

1	Introduction.....	3
2	Incident Definition.....	4
3	Incident Classification.....	5
4	How to Respond to a Security Incident .....	7
5	Forensic Investigation Guidelines .....	9
	Appendix A: Incident Response Report .....	11
	Appendix B: PCI Data Security Standards.....	14



## 1 Introduction

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 Risk Management, Asia Pacific will be vitally important to the protection of your company's key information.

In the event of a security incident, Visa members and their agents or merchants must take immediate action to investigate the incident, limit the exposure of Visa account and transaction information, notify Visa, and report investigation findings.

This document is intended for Visa members and entities that handle Visa account and transaction information, and includes:

- (a) Merchants: face to face (retail), Mail Order/Telephone Order (MOTO) and e-Commerce
- (b) Service Providers
- (c) Internet Payment Service Providers (IPSP)

It contains all the relevant information and 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.<sup>1</sup>

---

<sup>1</sup> Visa International Operating Regulations, Volume 1, Section 2.1.E.1

## 2 Incident Definition

Before any discussion on the obligations of a compromised entity, it is important to establish the definition of a security incident. According to CERT/CC<sup>2</sup>, a security incident can have the following definitions:

- (a) violation of an explicit or implied security policy;
- (b) attempts (either failed or successful) to gain unauthorized access to a system or its data;
- (c) unwanted disruption or denial of services;
- (d) the unauthorized use of a system for the processing or storage of data; and/or
- (e) changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

In the context of this document, the term “security policy” in the first definition refers to the 12 requirements under the Payment Card Industry (PCI) Data Security Standards (Refer to Appendix B). All Visa members, and their agents or merchants must comply with these standards to protect Visa account and transaction information effectively.

To help merchants meet the PCI data security requirements, Visa has developed the Account Information Security (AIS) program. For more information on AIS, members/merchants can access the following website <http://www.visa-asia.com/ap/sea/merchants/riskmgmt/ais.shtml>.

---

<sup>2</sup> The CERT Coordination Centre (CERT/CC) at <http://www.cert.org>

### 3 Incident Classification

A security incident can be classified under the following categories:

#### Malicious Code Attacks

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

The following are some examples of malicious code attacks:

- (a) Worms or viruses rapidly spreading through emails (e.g. I Love You, Melissa Virus);
- (b) Spying codes (e.g. Caligula Virus, Marker Virus, Groov Virus);
- (c) Remotely controlled codes (e.g. Back Orifice, NetBus); and
- (d) Coordinated attack codes (e.g. Trinoo, Tribe Flood Network (TFN)).

#### Denial-of-Service (“DoS”)

DoS attacks refer to the use of specific tools by intruders to cause networks and/or computers to cease operating effectively or to erase critical programs running on the system. Currently, distributed DoS attacks are becoming prominent where a team of intruders located in various geographical locations launches simultaneous attacks on a victim host. It is generally difficult to trace the source of distributed DoS attacks as perpetrators could launch the attack through multiple different gateways before reaching the victim host. In a DoS attack, DNS, web and mail servers are the most likely targets.

While a DoS attack may not be a direct cause of account compromise, it may however be a warning signal for future attacks.

Some examples of DoS attacks are:

- (a) Email related DoS (e.g. mail SPAM, mail bombs);
- (b) Service related DoS (e.g. Slammer Worm, Chargen DoS); and
- (c) Network jamming DoS (e.g. SYN flood DoS, 'Ping of Death' DoS, Smurf DoS).

### **Unauthorized Access / Theft**

Unauthorized access ranges from the unauthorized usage of log-on credentials to the tampering of files and directories stored on a system or storage media. It could also entail access to additional computer systems through an unauthorized “sniffer” program or device planted to capture confidential information traversing the network. Most e-commerce merchants use Secure Socket Layer (SSL) to protect web transactions over the internet. SSL provides server authentication, data encryption and message integrity. Without SSL, most web transactions, including credit card transactions, would travel across the internet in the clear, and would be susceptible to network sniffing i.e. the information could be copied, modified or deleted.

Internal compromise continues to be the most common and most damaging method of stealing sensitive information. Organized crime groups now actively recruit employees of organizations that process high volumes of account information to steal account and transaction information.

The following list includes some examples of unauthorized access:

- (a) Employees stealing confidential information;
- (b) System access by using user IDs belonging to ex-employees;
- (c) Unauthorized access by using user IDs that have administrative access rights;
- (d) System access by using special purpose IDs that are no longer required or use weak passwords; and
- (e) Unauthorized access by exploiting vulnerability in the company’s information systems, routers or firewalls.

### **Network reconnaissance probes**

The objective of performing reconnaissance probes against a company is to gather information on its network infrastructure. A probe can consist of two natures - host discovery and service ports discovery. Host discovery will determine all active systems in a network, which includes performing Operating System (“OS”) fingerprinting. Port discovery will gather information on the services running on the systems.

While a network probe attack may not result in an account compromise, it may however be a warning signal for future attacks.

There are many tools available on the internet for performing these probes such the following examples:

- (a) Host discovery (e.g. Ping sweep, directed broadcast pings, SYN-FIN scans), and
- (b) Service port discovery (e.g. TCP port scan, UDP port scan).

## 4 How to Respond to a Security Incident

Members, merchants and service providers are required to comply with the PCI Data Security Standards (PCI DSS). As part of these requirements, in the event a data compromise is suspected or confirmed, the compromised entity has certain specific obligations. Entities that suspect or have confirmed that a compromise of Visa account and transaction information has occurred must take the following actions:

### 1. Immediately contain and limit the exposure.

Prevent the further loss of data by conducting a thorough investigation of the suspected or confirmed loss or theft of account and transaction information within the first 24 hours of the matter arising. To preserve evidence and facilitate the investigation:

- Do not access or alter compromised systems (i.e. do not log on at all to the machine and change passwords, do not log on as ROOT);
- Do not turn off the compromised associated hardware machines. Instead, isolate compromised systems from the network (i.e. unplug cable);
- Preserve logs and electronic evidence;
- Keep a record of all actions taken;
- If using a wireless network, change the SSID on the AP and other machines that may be using this connection with the exception of any systems believed to be compromised; and
- Be on “high” alert and monitor all systems with Visa account and transaction information.

### 2. Alert all necessary parties immediately.

Be sure to contact:

- All internal response teams and internal information security groups
- Merchant acquiring bank
- Visa AP Risk Management

Tel: +65 6437 5862 or +65 6437 5873 (during business hours) or  
+65 9630 7672 (after hours)

Fax: +65 6437 5801

Email: [APInvestigations@visa.com](mailto:APInvestigations@visa.com)



- The relevant law enforcement authority. As a matter of policy, Visa will encourage the compromised entity to notify local law enforcement of the security breach. In the event that the compromised entity or its associated member fails to involve law enforcement, notification will be up to the discretion of Visa AP Risk Management.

**3. Provide the compromised Visa and Plus account numbers to your merchant acquiring bank within 24 hours.**

All potentially compromised accounts must be provided and transmitted as instructed by your merchant bank and Visa AP Risk Management. Visa will distribute the compromised account numbers to the affected issuers and ensure the confidentiality of entity and non-public information. It is critical that ALL compromised account numbers are provided.

**4. Provide Visa AP Risk Management with an Incident Response Report document to your merchant bank within the first three business days of the initial report or compromise identification.**

See Appendix A for the report template

**5. Complete an independent computer forensics review and complete a compliance questionnaire and vulnerability scan, as instructed by Visa.**

## 5 Forensic Investigation Guidelines

A compromised entity or the Visa member must engage a Qualified Security Assessor (QSA) to perform a forensic investigation. The following actions are included as part of the forensic investigation:

### 1. 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
  - Cardholder name
  - Cardholder address
  - All data exported by intruder
  - The time frame of account numbers stored and compromised;

*Note:* If applicable, the forensic team must run a packet-sniffer on the compromised entity's network.

### 2. Perform incident validation and assessment:

- Establish how the 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; and
- Determine if compromise has been contained.



**3. Check for Track 1 and Track 2 data, CVV2 and/or PIN block storage.**

Examine all potential locations, including payment applications, 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, troubleshooting or exception files, stage or testing environment data on software engineers' machines, etc.).

**4. If full track data, CVV2, and/or PIN blocks are stored by a payment application, identify the vendor name, product name, and version number.**

**5. If applicable, review VisaNet endpoint security and determine risk.**

**6. Preserve all potential electronic evidence on a platform suitable for review and analysis by a court of law if needed.**

**7. Perform external and internal vulnerability scans.**



## Appendix A: Incident Response Report

INCIDENT RESPONSE REPORT		
Date Updated:	Incident no.:	
<b>1. Contact information for this Incident</b>		
Name:	Organization:	Title:
Address:		
Office/Cell Phone:	Email:	Fax no.:
<b>2. Physical location of affected computer/network:</b>		
(Include building number, shop number, and barcode information, if available):		
<b>3. Period that Incident occurred:</b>		
From (mm/dd/yy):	Till (mm/dd/yy):	
Time (hh:mm:ss am/pm/Time Zone):	Time (hh:mm:ss am/pm/Time Zone):	
<b>4. Incident Assessment:</b>		
Describe the incident.		
How was the incident discovered? Please elaborate:		
Damage or observations resulting from incident.		
Are there any actions taken to contain the incident? Please elaborate. Include any dates of completion.		



<b>5. Impact assessment:</b>
How many card accounts have been compromised:
Which banks/organizations issued the affected accounts?
Type of account information at risk. Please elaborate on the sensitivity of the data lost. <ul style="list-style-type: none"><li>- Track 1 and Track 2</li><li>- PIN blocks</li><li>- CVV2</li><li>- Account number</li><li>- Expiration Date</li><li>- Cardholder name</li><li>- Cardholder address</li><li>- Number of accounts at risk</li><li>- Timeframe of accounts at risk</li></ul>
<b>6. Apparent or suspected source of compromise:</b>
<b>7. Network Infrastructure Overview</b>
Provide a diagram of the network that includes the following: <ul style="list-style-type: none"><li>- Cardholder data sent to central corporate server or data center</li><li>- Upstream connection to third-party processor</li><li>- Connection to member</li><li>- Remote access connection by third-party vendors of internal</li></ul>
<b>8. Information Sharing:</b>
With whom this information has been shared outside of the Company (do not leave blank and check all that apply): <ul style="list-style-type: none"><li><input type="checkbox"/> Acquiring Bank</li><li><input type="checkbox"/> Law Enforcement Agency</li><li><input type="checkbox"/> Forensic Specialists</li><li><input type="checkbox"/> Others (Specify):</li><li><input type="checkbox"/> No Sharing is Authorized</li></ul>



**9. Additional Information:**

If this incident is related to a previously reported incident, include any previously assigned incident number for reference:



## Appendix B: PCI Data Security Standards

Requirements
<b>Build and Maintain a Secure Network</b> 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
<b>Protect Cardholder Data</b> Requirement 3: Protect stored cardholder data Requirement 4: Encrypt transmission of cardholder data across open, public networks
<b>Maintain a Vulnerability Management Program</b> Requirement 5: Use and regularly update anti-virus software Requirement 6: Develop and maintain secure systems and applications
<b>Implement Strong Access Control Measures</b> 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
<b>Regularly Monitor and Test Networks</b> Requirement 10: Track and monitor all access to network resources and cardholder data Requirement 11: Regularly test security systems and processes
<b>Maintain an Information Security Policy</b> Requirement 12: Maintain a policy that addresses information security