



# What To Do if Compromised

Visa USA

Fraud Investigations and  
Incident Management Procedures



## Table of Contents

Introduction .....	1
Security Breach Reporting .....	2
Steps and Requirements for Compromised Entities .....	3
Steps and Requirements for Acquirers .....	5
Account Data Format .....	7
Initial Investigation Request .....	8
Compromised Account Management System (CAMS) .....	10
Forensic Investigation Guidelines .....	14
Appendix A: Incident Report Template .....	16
Appendix B: List of Supporting Documents .....	20
Appendix C: Glossary of Terms .....	22

## 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 USA 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 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 members. 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.<sup>1</sup>

---

<sup>1</sup> *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.*

## Security Breach Reporting

---

The *Visa U.S.A. Inc. Operating Regulations*, the *Plus System Operating Regulations*, and the *Interlink Network Operating Regulations*, require that members comply with the Visa USA 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. Members 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 member must permit Visa USA, or an independent third party acceptable to Visa, to verify this ability by conducting a subsequent security review.

If Visa determines that a member 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.<sup>2</sup>

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

---

<sup>2</sup> *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 Visa CISP Data Security Standard 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.

### 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.

**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 USA Fraud Investigations and Incident Management group immediately at (650) 432-2978.
- Your local office of the United States Secret Service.

- 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 *Account Data Format* section on page 7 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.

## Steps and Requirements for Acquirers

### Notification

- 1. Immediately report to Visa the suspected or confirmed loss or theft of Visa cardholder data.** Members must contact the Visa USA Fraud Investigations and Incident Management group immediately at (650) 432-2978 or [usfraudcontrol@visa.com](mailto:usfraudcontrol@visa.com).
- 2. Within 48 hours, advise Visa whether the entity was in compliance with the Visa USA CISP PCI Data Security Standard and, if applicable, the 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 3 business days.** The information provided will help Visa understand the potential exposure and assist entities in containing the incident.

#### FOR MORE INFORMATION

To find out more about conducting an initial investigation, see the *Initial Investigation Request* section on page 8 of this guide.

### Independent Forensic Investigation

If Visa deems necessary, an independent forensic investigation must be conducted by a Qualified Incident Response Company (QIRC). In this case, it is the member's responsibility to ensure that a forensic investigation is conducted by a QIRC.

- 4. Upon receipt of an initial independent forensic investigation notification from Visa, members must:**
  - **Identify the QIRC within 5 business days.**
  - **Ensure that the QIRC is engaged or the contract is signed within 10 business days.**
  - **QIRC must be onsite to conduct a forensic investigation within 5 business days from contract agreement.**

If the compromised entity is not willing to engage a QIRC, the member must engage the company directly. Visa, however, has the right to engage a QIRC to perform a forensic investigation as it deems appropriate, and will assess all investigative costs to the member in addition to any fine that may be applicable.

- 5. If there is a suspected PIN compromise, ensure that an approved PIN security assessor is engaged or the contract is signed by within 10 business days.**
- 6. A PIN security assessor must be onsite to conduct a PIN security review within 5 business days from contract agreement.**

#### KEY POINT TO REMEMBER

The entity must have the assessor evaluate whether the entity complies with each of the 32 PCI PIN Security Requirements, available on [www.visa.com/pin](http://www.visa.com/pin).

#### KEY POINT TO REMEMBER

An approved QIRC may perform a PIN security review as long as the company has the appropriate skill set. This will be determined by Visa.

7. Provide a preliminary forensic report to Visa within 5 business days from the onsite review.
8. Provide a final forensic report to Visa within 10 business days from the completion of the review.

---

 PIN Security

9. If there is a suspected PIN compromise, provide a PIN security report within 10 business days from the onsite review.

---

 Account Numbers

10. Upload at-risk account numbers to Visa's Compromised Account Management System (CAMS).
11. By using CAMS, provide the at-risk account numbers to Visa within 10 business days of the request from Visa or from the receipt of the preliminary forensic report.

**FOR MORE INFORMATION**

For CAMS account access and upload procedures, see the Compromised Account Management System (CAMS) section on page 10 of this guide.

---

 Containment/  
Remediation

12. Ensure that the compromised entity has contained the incident and has implemented security recommendations provided by the QIRC, including any non-compliance with the PCI PIN Security Requirements.
13. If the entity is retaining full-track data, CVV2, and/or PIN blocks, ensure that the entity has removed the data. This also includes any historical data.
14. Validate that full-track data, CVV2, and/or PIN blocks are no longer being stored on any systems. Even though this is the member's responsibility, Visa requires that the validation be performed by the QIRC.
15. Submit an action plan to Visa within 5 business days after receiving the final forensic report. As required by Visa, members must provide an action plan with implementation dates related to findings identified by the QIRC. A revised action plan must be provided to Visa, as needed.
16. Monitor and confirm that the compromised entity has implemented the action plan.

---

 PCI Compliance

17. Ensure that the compromised entity has taken steps necessary to prevent future loss or theft of account information, consistent with the Visa USA CISP PCI Security Standard and the PCI PIN Security Requirements.
18. To comply with the Visa USA CISP PCI Security Standard and PCI PIN Security Requirements, engage an approved qualified security assessor to perform a PCI Security Audit, or complete a self-assessment questionnaire and remote vulnerability scan. Visa will determine the appropriate course of action required.

**FOR MORE INFORMATION**

Please visit the PCI Security Standards Council website ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)) for details on the PCI program requirements. For more information on PCI PIN security requirements, go to [www.visa.com/pin](http://www.visa.com/pin).

---

 Regulatory Compliance

19. In the event of a "large-scale" or "high-profile" suspected account data compromise, notify your banking regulator as soon as possible.

## Account Data Format

In the event of a compromise, Visa requires that **at risk** accounts be uploaded to the Visa Compromised Account Management System (CAMS). The account data must be **authorization data only**, and the data submission must be a fixed width or delimited text file. When uploading to CAMS, the user must provide a description of data being uploaded. For example:

- Timeframe of accounts
- Data elements at risk:
  - PAN
  - Expiration date
  - Track 1 or 2
  - CVV2
  - Other cardholder information, such as billing address, e-mail addresses, etc.
- Name of compromised entity
- Name of Visa investigator handling the incident

**FOR MORE INFORMATION**

For further details about CAMS access, see the CAMS section starting on page 10 of this guide.

At a minimum, the following data elements must be uploaded. **Special circumstances may require additional transaction data from the compromised entity and Visa member. Visa will provide the requirements to the member as needed.**

For:	Provide these data elements: (This is on a case-by-case basis. In some instances, not all data elements may be required)
<b>Card-Not-Present Events</b>	Plaintext, comma delimited file with <b>account numbers</b> only.
<b>Card-Present Events</b>	Plaintext, comma delimited file with the following: <ul style="list-style-type: none"> <li>• Credit accounts signature (include transaction details below)</li> <li>• Debit accounts signature (to include transaction details below)</li> <li>• Debit accounts used with a PIN (to include transaction details below). Separate files must be provided for:                             <ul style="list-style-type: none"> <li>- Interlink transactions</li> <li>- Plus transactions</li> </ul> </li> <li>• Key-entered accounts (to include transaction details below). Transaction details are defined as:                             <ul style="list-style-type: none"> <li>- Account number</li> <li>- POS entry mode</li> <li>- Transaction date</li> <li>- Card Acceptor ID</li> <li>- Amount of transaction</li> <li>- Response code</li> <li>- Merchant Category Code (MCC)</li> </ul> </li> </ul>

## Initial Investigation Request

Upon notification of a suspected account data compromise, Visa will request that the acquirer initiate a preliminary investigation of any entity involved in a potential track data, CVV2, and/or PIN block compromise. The initial investigation will assist Visa in understanding the compromised entity's network environment.

**To comply with Visa's initial investigation request, the acquirer must provide the following information:**

- Name of Entity
- Bank Identification Number (BIN)
- Entity ID
- Card Acceptor Identifier (CAID)
- Date when compromised entity began processing with member
- Date when compromised entity stopped processing with member (if applicable)
- An assessment and description of the entity's network environment:
  - Is there Internet connectivity?
  - Is there wireless connectivity?
  - Is there a third-party (reseller or POS vendor) remote connectivity?
  - What type of remote control program is used and how is it configured?
  - Is the terminal PC-based or connected to a PC-based environment?
  - Any abnormal activity on entity's network (e.g., viruses, Trojans, or high CPU utilization)?
- Documentation depicting the transaction data flow for credit and debit, as well as access to the network. The data flow must include:
  - Cardholder data sent to central corporate server or data center
  - Upstream connection to third-party processor
  - Connection to member
  - Remote access connection by third-party vendors or internal staff
- Entity's CISP/PCI PIN Security compliance status. The acquirer must include appropriate documentation (e.g., audit report, vulnerability scan, and completed questionnaire)

- ❑ Disclosure as to whether or not the entity is retaining full-track data or CVV2
- ❑ If the entity accepts PIN-based transactions, disclosure as to whether or not the entity is retaining encrypted PIN blocks
- ❑ Name and version of POS/ATM application:
  - Is the POS/ATM application PABP-compliant?
  - What is the date when the entity first used the POS/ATM application?
- ❑ If the entity is using a third-party reseller, disclosure of the reseller name and contact information
- ❑ If entity has more than one location, a list of all locations operated by the compromised entity. For each location, include the name and version of the POS/ATM application

**FOR MORE INFORMATION**

For a list of PABP-compliant payment applications, visit [www.visa.com/cisp](http://www.visa.com/cisp).

## Compromised Account Management System (CAMS)

### CAMS Enrollment

The *Compromised Account Management System (CAMS)* was developed by Visa to securely distribute and obtain **at risk** Visa account numbers. To obtain access to Visa CAMS, entities must first:

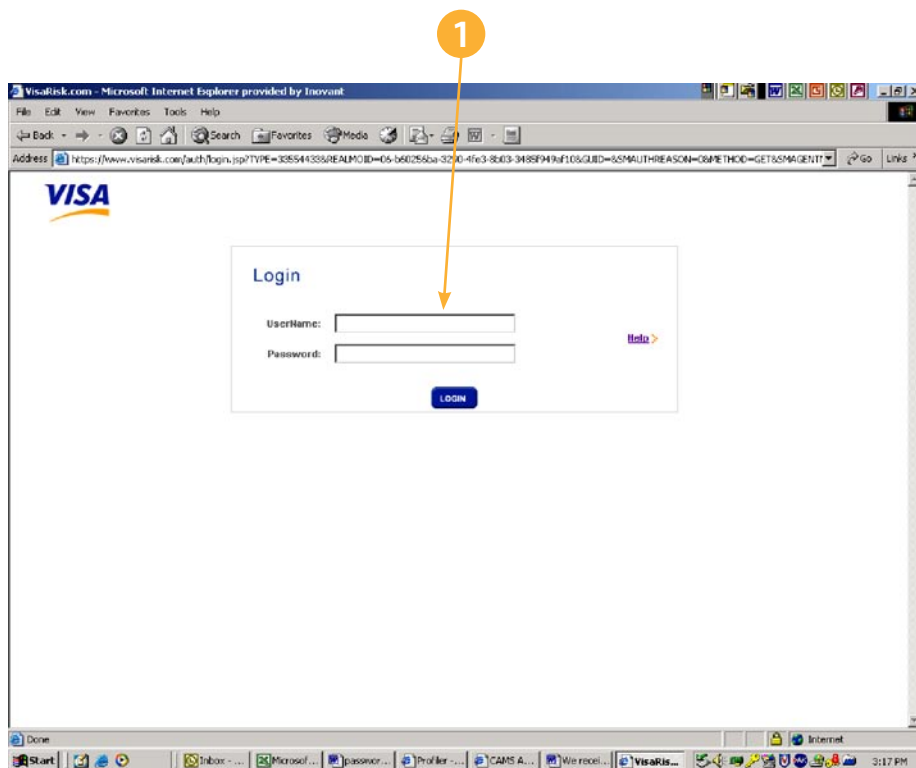
- Contact Visa Investigations and Incident Management by e-mail at [cams@visa.com](mailto:cams@visa.com).
- Complete the CAMS enrollment form.
- Send the completed form back to Visa.

**Entities will be contacted with a user ID and password.**

### CAMS Access

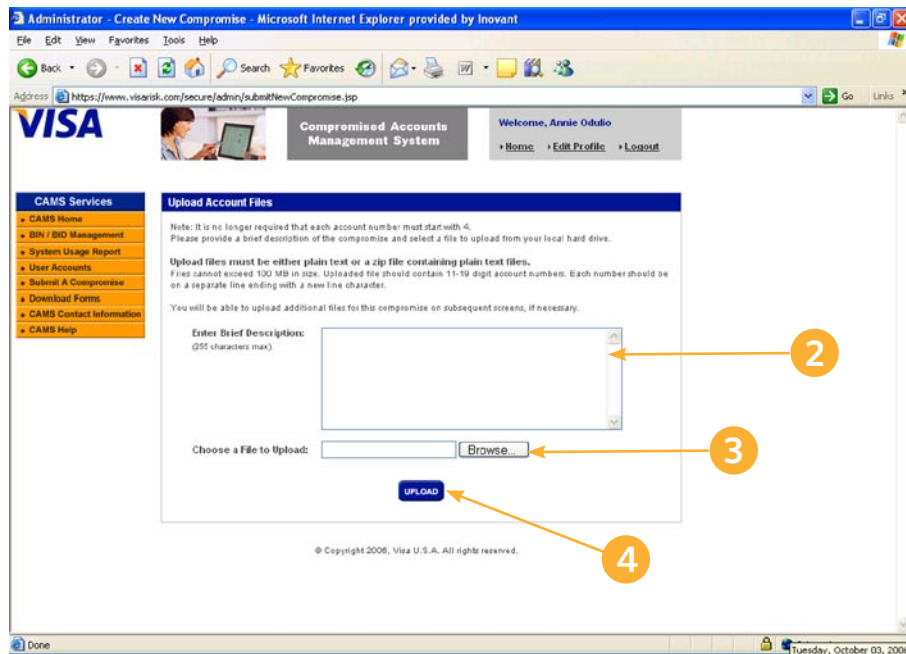
Once you receive your user ID and password from Visa, follow the steps below to access CAMS at [www.visarisk.com](http://www.visarisk.com)

1. At the Login screen, enter your user name and password. Click "LOGIN"



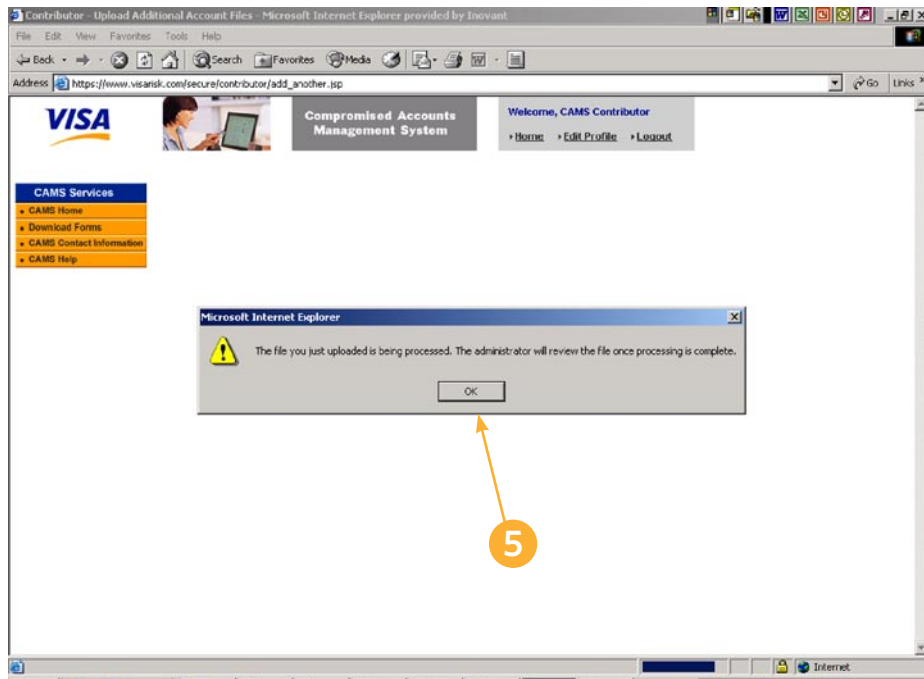
**The CAMS Upload Account Files screen will appear.**

- CAMS Upload
2. Type in a brief description of the compromise.
  3. Choose the file to be uploaded to CAMS. It must be in text format and saved with a txt extension. Word or Note Pad is recommended.
  4. Click UPLOAD. The file will be immediately uploaded to CAMS. Visa receives an e-mail alert whenever a file is uploaded to CAMS.



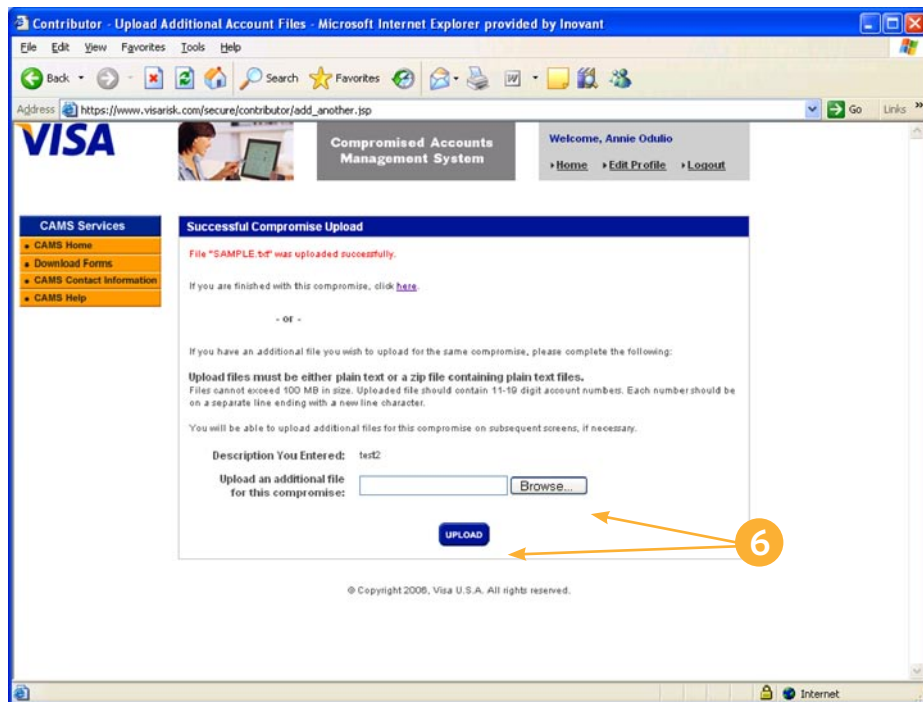
A message box will appear on screen telling you that the file is being uploaded.

5. Click **OK** to accept file upload message.



A notice will appear on screen confirming that the file was uploaded. It will also provide you with an option to upload another file—that is part of the same compromise – or to log out.

6. Upload an additional file and check upload if necessary, or log out.



If you have any questions or problems, please contact Visa by e-mail at [cams@visa.com](mailto:cams@visa.com).

## Forensic Investigation Guidelines

A compromised entity or the Visa member must engage a Qualified Incident Response Company (QIRC) to perform a forensic investigation. **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
  - 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.

### KEY POINT TO REMEMBER

Visa reserves the right to engage the team.

- 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, troubleshooting 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 member and the compromised entity. Visa will classify the report as "Visa Secret."<sup>3</sup>

---

<sup>3</sup> 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.

## Incident Report Template

---

### I. Executive Summary:

Include the following:

- Date of when forensic company was engaged
- Date(s) of forensic investigation
- 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

### II. Background

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

### 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
<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		

#### 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 connection to third-party processor
- Connection to member
- Remote access connection by third-party vendors of internal staff

**V. Investigative Procedures**

Include forensic tools used during investigation.

**VI. Findings**

- Provide specifics on firewall, infrastructure, host, and personnel findings.
- Identify any data exported by intruder.
- 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**

Identify actions made to contain the incident. Include any dates of completion.

**VIII. Recommendations**

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

## Appendix B: List of Supporting Documents

---

This appendix section includes a list of the documents you need to perform the Visa USA 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](http://www.visa.com/cisp) and [www.visa.com/pin](http://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 Visa USA CISP PCI Data Security Standard.
- **PCI Self-Assessment Questionnaire** – Must be completed by Level 2 and 3 entities, 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 entities and third-party service providers who are scanning their infrastructures to demonstrate CISP compliance.
- **PCI PIN Security Requirements** ([www.visa.com/pin](http://www.visa.com/pin))
- **Visa PIN Security Program Auditor's Guide** ([www.visa.com/pin](http://www.visa.com/pin))

## Appendix C: Glossary of Terms

<b>Acquirer</b>	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.
<b>Agent</b>	Any contractor, including third-party processors and servicers, whether a member or non-member, engaged by a member to provide services or act on its behalf in connection with the Visa payment services.
<b>Authentication</b>	The process of verifying the true origin or nature of the sender and/or the integrity of the text of a message.
<b>Authorization</b>	A process by which an issuer approves a transaction for a specified amount with a merchant.
<b>Bank Identification Number (BIN)</b>	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."
<b>Card Authorization Acceptor ID</b>	Information found in the authorization message (Field 42) from a legitimate transaction at the Acceptor ID CPP identified merchant.
<b>Card-Not-Present</b>	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.
<b>Card-Present</b>	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.
<b>Card Verification Value (CVV)</b>	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.
<b>Card Verification Value 2 (CVV2)</b>	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.
<b>Cardholder</b>	The person or entity whose name is embossed on the face of a card or encoded on the magnetic stripe.

<b>Cardholder Data</b>	All identifiable personal data about the cardholder and relationship to the member (e.g., account number, expiration date, data provided by the member, 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.
<b>Compromise</b>	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).
<b>Compromised Account Management System (CAMS)</b>	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.
<b>Electronic Commerce (e-Commerce)</b>	The purchase of goods and services over the Internet without a paper transaction between buyer and seller.
<b>Entity</b>	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.
<b>Encryption</b>	An online data security method scrambling data so that it is difficult to interpret without a corresponding decryption key.
<b>Full-Track Data</b>	There are two tracks of data on a bankcard's magnetic-stripe: <ul style="list-style-type: none"> <li>▪ <b>Track 1</b> is 79 characters in length. It is alpha-numeric and contains the account number, the cardholder name, and the additional data listed.</li> <li>▪ <b>Track 2</b> 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.</li> </ul>
<b>Hacker</b>	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.
<b>Magnetic Stripe (Mag Stripe)</b>	A strip of magnetic tape on the back of all bankcards. The magnetic stripe is encoded with identifying account information as specified in the <i>Visa U.S.A. Operating Regulations</i> . On a valid card, the account information on the magnetic stripe matches similar embossed information on the front of the card.

<b>Member</b>	An organization which is a member of Visa and which issues cards and/or signs merchants.
<b>Merchant</b>	A principal or entity entering into a card acceptance agreement with a Visa member financial institution.
<b>Merchant Bank</b>	See “Acquirer.”
<b>Payment Card Industry (PCI) Data Security Standard</b>	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.
<b>Payment Card Industry (PCI) PIN Security Requirements</b>	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 <i>PCI PIN Security Requirements</i> . This document can be downloaded from the PIN website at <a href="http://www.visa.com/pin">www.visa.com/pin</a> .
<b>Personal Identification Number (PIN)</b>	An alphabetic and/or numeric code which may be used as a means of cardholder identification.
<b>Qualified Data Security Company (QDSC)</b>	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 <i>PCI Security Standards Council</i> website ( <a href="http://www.pcisecuritystandards.org">www.pcisecuritystandards.org</a> ) for details on the PCI program requirements.
<b>Third-Party Processor</b>	A service provider organization that is acting as the agent of a member to provide authorization, clearing, or settlement services for merchants and members.
<b>Third-Party Servicer</b>	A service provider organization that is not a member of Visa and is not directly connected to VisaNet, but provides the following services to the member: <ul style="list-style-type: none"> <li>▪ Response processing for Visa program solicitations</li> <li>▪ Transaction processing, including gateways</li> <li>▪ Data capture</li> <li>▪ Other administrative functions, such as chargeback processing, risk/security reporting, and customer service</li> </ul>
<b>Visa Cardholder Information Security Program (CISP)</b>	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 <a href="http://www.visa.com/cisp">www.visa.com/cisp</a> .
<b>VisaNet</b>	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.

