What To Do If Compromised

Visa Inc. Fraud Investigation Procedures

Version 4.0 (Global)
Effective September 2013
Visa Public

Table of Contents

Introduction

Identification, containment, and remediation of any electronic security incident are crucial to any organization looking to minimize the impact a data breach will have on its business operations.

In general, an electronic data breach occurs when an entity suffers a deliberate electronic attack on its communications or information processing and/or storage systems. Whether initiated by a disgruntled employee, a malicious competitor, or a hacker, deliberate attacks often cause damage and disruption to the payment system. Advance preparation on how to respond to an attack on your company's information systems may allow you to control resulting costs and consequences. Additionally, close collaboration with payment system providers, including, Visa Inc., is vitally important to the protection of your company's key information and any card holder information.

In the event of a data breach, in addition to complying with any applicable laws and regulations, Visa clients or members and their agents must take immediate action to contain the incident, notify payment system partners including Visa, and investigate the incident, which may include retaining an independent PCI Forensic Investigator (PFI).[1]

The *What To Do If Compromised* guide was prepared for Visa clients or members, merchants, agents, and third-party service providers. It contains step-by-step instructions on how to respond to a data breach and provides specific time frames for the delivery of information or reports.[2]

[1] *Visa International Operating Regulations*, Member Investigation of Suspected Fraud, ID #7123, Prevention of Loss or Theft of Information, ID #5605, Additional Investigation, ID #7124.

[2] 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, ID #7124.

Identifying and Detecting A Data Breach

Hackers are becoming increasingly sophisticated and it may be difficult to detect a data breach. However, distinguishing normal events from those that are related to a data breach is a critical part of maintaining a secure payment processing environment.

Data 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 headquarters 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 or unknown encrypted 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.
- **Memory parser malware.** This type of malware targets payment card data being processed in the clear in random access memory (RAM). The malware is configured to hook into a payment application binary responsible for processing payment transactions and extracts the systems memory for full track data. As compliance with the PCI DSS expands, POS systems are increasingly eliminating the practice of storing prohibited data to system disks, thereby preventing attackers from readily obtaining stored data. The use of memory parser malware that parses data from volatile memory suggests attackers have successfully adapted their techniques to obtain payment data not written to POS system disks. This method of data extraction is of particular concern, since unencrypted data is commonly written to volatile memory during the transaction process.

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 for Compromised Entities

Entities that have experienced a suspected or confirmed security breach should 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 data exposure and minimize data loss. Prevent any further loss of data by conducting a thorough investigation. Compromised entities should consult with their internal incident response team.
2. 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 the 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 all evidence and logs (i.e., original evidence, security events, web, database, firewall, etc.)
   - Document all actions taken, including dates and individuals involved.
   - 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).
   - Block suspicious IPs from inbound and outbound traffic.
   - Be on high alert and monitor traffic on all systems with cardholder data.
3. 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.

Notification Following a Security Breach or Compromise of a PCI PTS Approved Devices

In the event that there is a potential compromise of a PCI SSC PTS Approved PIN-Entry device (PED), the compromised entity must inform the PED vendor of the PED compromise. Clients or members must inform the vendor of all relevant information including:

- The number and location of actual products affected
- The number of compromised accounts
- Details of any compromised keys
- Any reports detailing the security breach or compromise
- Any report or evaluations performed to investigate the security breach or compromise

Vendors that manufacture PCI PTS Approved PEDs are required to inform the PCI SSC with this information so that the PCI SSC can evaluate the severity of the compromise and take appropriate actions, including PED delisting.

For a list of PCI PTS approved devices, please go to *www.pcisecuritystandards.org*.

4. The compromised entity also should consider what notification to law enforcement is required or otherwise appropriate. If you would like assistance in contacting the appropriate law enforcement agency, contact the Visa Incident Response Manager.
5. 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 in place an Incident Response Team to assist with forensic investigations. In the event of a compromise, Visa will work with the compromised entity and assist with coordination of a team of forensic specialists to go onsite immediately to help identify security deficiencies and control exposure. The forensic information collected by this team may be used as evidence to prosecute criminals.

6. The compromised entity should consult with its legal department to determine if laws mandating customer notification are applicable.

7. 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.

   Important Note: In the event that the compromised entity believes that an electronic data breach does not result in any vulnerability of card holder data, Visa reserves the right to require the compromised entity or its Acquirer provide evidence that no card holder data was vulnerable.

8. Within three (3) business days of the reported compromise, provide a written documentation to the Visa client or to Visa. See Appendix A. 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 or Members (Acquirers and Issuers)

Visa clients or members must conduct a thorough investigation of a suspected or confirmed theft of Visa cardholder data involving their own network environment or their merchants or agents.

Notification

1. Immediately report to the Visa Risk Management group if there is any suspected or confirmed unauthorized access to any Visa cardholder data.
2. Within 48 hours, provide Visa with any evidence of status of compliance with PCI DSS and, if applicable, PCI PA-DSS and PCI PIN Security requirements at the time of the incident.

Preliminary Investigation

3. Perform an initial investigation and provide written documentation of any findings or conclusions to Visa within three (3) business days. The information will help Visa understand potential exposure to assist with containing the incident. Documentation must include any steps taken to contain the incident.

For More Information

To find out more about conducting an initial investigation, see *Appendix A: Initial Investigation Request* on page 17.

Independent Forensic Investigation

At Visa's discretion, an independent forensic investigation must be conducted by a Payment Card Industry Forensic Investigator (PFI). A PFI investigation is required on compromised entities that fall under the following categories:

- Self-reported data security breach affecting payment cards
- Suspected data breach: multiple Common Point of Purchases (CPPs) from different issuers
- Suspected data breach based on a single CPP with >25 accounts and/or > $25K in fraud
  - Merchant Fraud Conversion Rate (MCR) supports CPP
- Law enforcement or other credible source reports a data security breach affecting payment cards

The following small merchants will be required to undergo either alternative forensic or a combination of onsite and alternative forensic investigation by a PFI:

Small merchant with annual Visa transaction volume > 201K - 1M	Combination of onsite and alternative forensic investigation
Small merchant with annual Visa transaction volume of > 50K - 200K	Alternative forensic investigation

For more information on alternative forensic investigation, go to *https://www.pcisecuritystandards.org/documents/PFI_Program_Guide.pdf*

Onsite Forensic: Visa may require an onsite forensic for any merchant that has not contained the initial event (this may be determined through additional CPP reports and/or data analysis).

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 or members 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/members 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 or member in addition to any fine that may be applicable.

Key Point to Remember

The entity must have the PFI evaluate whether it is in compliance 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 of completion of the review.

   Note: Visa has the right to reject the forensic 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 of completion of 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. The final report must include a description of 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 not stored on any systems. Although this is generally the client or member's responsibility, following a data breach, Visa requires that the validation be performed by the PFI.
13. Submit a remediation plan that includes remediation dates responsive to the PFI findings to Visa within five (5) business days of receipt of the final forensic report.

    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*.

    Note: In the event the compromised entity had a PCI DSS audit performed by a QSA and suffered a data breach, Visa will require that the entity engage another QSA to perform the PCI DSS audit.

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 data breach, any "at risk" account numbers, including both international and domestic accounts, must be provided to Visa through Visa's Compromised Account Management System (CAMS).

Where appropriate, Visa may require the entity to provide accounts via a CD using encryption software such as PGP[3] or Winzip[4] with 256-AES encryption and strong password. The following guidelines must be followed when providing accounts to Visa:

Account Data Format

The account data must include **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:

  4xxxxxxxxxxxxxx,0801

Key Point to Remember
Clients or members must comply with any request for additional data.

1. Submitted data of the same type 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

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

[4] 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 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.

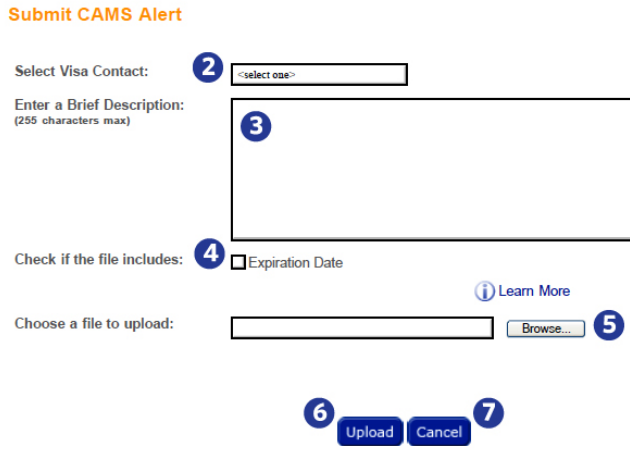
Compromised Account Management System (CAMS)

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 *gvol.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.



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 event.
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.

Appendix A: Initial Investigation Request

Upon notification of a suspected account data compromise, the Visa client or member must initiate a preliminary investigation of their systems or of their merchants and agents involved in a potential track data, CVV2, and/or PIN compromise and share the findings with Visa. [VIOR IDs #7123 and #7124.] Note this is not a PFI preliminary report. The initial investigation will assist Visa in understanding the compromised entity's network environment.

To comply with Visa's initial investigation requirement, the Visa client or member must provide the following information:

Key Point to Remember

The information required below is applicable to suspected/confirmed compromised entities such as Visa clients or members, merchants, processors, or third-party service providers.

Entity Information

Description	Response
Name of entity	
Is entity a direct-connect to Visa?	
If entity is a merchant, provide the Merchant Category Code (MCC)	
Acquirer BIN	
Entity PCI DSS Level (e.g., Level 1-4)	
Entity PCI DSS Compliance Status (If compliant, please provide proof of PCI DSS compliance documentation.)	
Was entity compliant at the time of the breach?	
Has entity provided a PCI DSS remediation plan? If so, please provide details of the plan.	
Approximate number of transactions/accounts handled per year	
1. ATM	
2. POS PIN/Debit	
3. Credit	
If merchant, is entity corporate-owned or an individual franchise?	
If merchant, does entity have other locations? If so, please provide a list of locations, the name of the payment application, and version information.	

Network/Host Information

Description	Response
Is there Internet connectivity?	
Is there wireless connectivity?	
Does entity utilize a high-speed connection (e.g., cable modem, DSL)	
Is there remote access connectivity? If so, who has remote access?	
Is remote access always on or is it enabled upon request?	
What type of remote access software is used?	
Is the terminal PC-based or is it connected to a PC-based environment?	
Has entity noticed any abnormal activity on its systems?	
Is the entity retaining full track data, CVV2 or encrypted PIN blocks?	
How long is the data stored on the system(s)?	
Have there been any recent changes to the network and host such as: ▪ Upgrade to the payment application ▪ Installation of a firewall ▪ Installation of anti-virus program ▪ Changes to remote access connectivity	
Provide a transaction flow for credit and debit, as well as remote access to the network. The data flow must include: ▪ Installation of anti-virus program ▪ Cardholder data sent to a central corporate server or data center ▪ Upstream connection to third-party service providers ▪ Connection to entity bank/acquirer ▪ Remote access connection by third-party service providers or internal staff	

Third-Party Connectivity

Description	Response
Does the entity send transactions to a processor(s)? If so, who is the processor(s)?	
Name of payment application vendor	
Name of reseller, if applicable	
Is the entity hosted? If so, who is the hosting provider?	

If Confirmed Breach, Please Provide the Following

Description	Response
How was the incident identified?	
How did the compromise take place? 1. List vulnerabilities that allowed the compromise to take place 2. Details of hacker's activity 3. List malicious IPs 4. List malware information	
Did entity notify law enforcement? If so, which agency and when notified?	
Has the compromise been contained? If so, how?	
How many Visa cards were compromised (as defined by this guide)?	
Was the entity storing any cardholder data, including any of the fields below? If so, please indicate the type of data that was stored. ▪ Primary Account Number (PAN) ▪ Any portion of PAN ▪ Expiration Date ▪ Full Track 1 ▪ Full Track 2 ▪ CVV2 ▪ Cardholder Name ▪ Social Security Number ▪ Date of Birth	
What data elements were compromised and/or exposed? ▪ PAN ▪ Expiration Date ▪ Full Track 1 ▪ Full Track 2 ▪ CVV2 ▪ Cardholder Name ▪ Cardholder Address ▪ Social Security Number	

List of Payment Applications and PIN Entry Device (PED) in Use

Description	Response
Payment application and version information	
Is this a corporate-mandated payment application and version?	
PCI PIN Transaction Security: PIN Entry Device (PED) information, if applicable. Include the name of the PED firmware version. Visit *www.pcisecuritystandards.org/pin* for a list of PCI-approved PIN entry devices.	
Shopping cart and version information	
Are the payment applications in use PCI PA-DSS compliant? Visit *https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php* for a list of PA-DSS compliant payment applications.	
Is entity using a compliant PED? Visit *www.pcisecuritystandards.org/pin* for a list of compliant PEDs.	
Are any of the Attended POS PEDs in use neither Pre-PCI or PCI Approved? Visa set global mandates that all attended POS PEDs that were neither Pre-PCI or PCI approved must be removed from production by July 2010. Review the Visa General PED FAQ for Visa Mandates for compliant PED usage: *http://usa.visa.com/download/merchants/cisp-pin-entry-device-faq.pdf*	

Potential Skimming/PED Tampering

Description	Response
Can entity trace legitimate transactions to a single employee, device, or lane(s)?	
Did entity have any employees who were employed for a short period of time?	
Did other employees notice suspicious behavior of the new employee (e.g., eager to handle all credit card transactions)?	
Is there any video surveillance and has it been reviewed?	
Can all PEDs be accounted for at all times?	
Are any of the POS PEDs in use listed on the June 2010 Security Alert available at: *http://usa.visa.com/download/merchants/bulletin_compromised_ped_listing_mandatory_sunset_dates.pdf*	

Other Information

Description	Response
Has entity received complaints regarding fraudulent transactions from their customers?	
Has entity been contacted by law enforcement regarding fraudulent transactions?	
Can law enforcement provide intelligence that skimming groups are active in the area?	

Appendix B: Forensic Investigation Guideline

A Visa client/member or compromised entity must engage a Payment Card Industry Forensic Investigator (PFI) to perform a forensic investigation. Visa will **NOT** accept forensic reports from non-approved forensic companies. It is the Visa client or member's responsibility to ensure their merchant or agent engage a PFI to perform a PFI forensic investigation. [VIOR IDs #7123 and #7124.Cite?] Visa has the right to engage a PFI to perform a further forensic investigation as it deems appropriate, and will assess all investigative costs to the appropriate Visa client, in addition to any assessment that may be applicable. PFIs are required to release forensic reports and findings to Visa. All PFIs must utilize Payment Card Industry reporting templates.

Note: For a list of PFIs, please go to: *https://www.pcisecuritystandards.org/approved_companies_providers/pci_forensic_investigator.php.*

Note: Visa has the right to reject the report if it does not meet the PFI requirements. PFIs are required to address with Visa, the acquirer, and the compromised entity any discrepancies before finalizing the report.

For more information on the forensic investigation guideline, please refer to the document labeled *PCI Forensic Investigator (PFI) Program Guide, Annex A* available at: *https://www.pcisecuritystandards.org/security_standards/documents.php?view=&association=PFI&language=*

Appendix C: PFI Report Templates

The following templates can be downloaded at:
https://www.pcisecuritystandards.org/security_standards/documents.php?view=&association=PFI&language=

- Preliminary Report Template
- Final Report Template
- PIN Security Report Template

Appendix D: List of Supporting Documents

The following documents can be downloaded at *www.visa.com/cisp*, *www.visa.com/pinsecurity*, *www.visa.com/pin*, *www.pcisecuritystandards.org*

- Payment Card Industry Forensic Investigator (PFI) List – List of forensic companies qualified to perform a PCI forensic investigation on compromised entities and reporting templates.
- Qualified Security Assessor (QSA) – List of assessors qualified to perform PCI assessments for those entities requiring onsite validation of PCI compliance.
- PCI Data Security Standard (PCI DSS) – Detailed security requirements to which Visa clients or members, merchants, and service providers must adhere to ensure the protection of cardholder data.
- PCI Self-Assessment Questionnaire (SAQ) – The PCI SAQ is an important validation tool 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. **Note:** 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 compliance to the PCI DSS.
- Acquiring institutions and agents involved with PIN transaction processing must comply with the security requirements and guidelines specified in the PIN Security documents that can be downloaded from *www.visa.com/pinsecurity*.
- PCI PIN Security Requirements (visit *www.visa.com/pinsecurity*).
- Visa PIN Security Program Auditor's Guide (visit *www.visa.com/pinsecurity*).
- Issuer PIN Security Guidelines available at: *http://usa.visa.com/download/merchants/visa-issuer-pin-security-guideline.pdf*

Appendix E: Glossary of Terms

802.11	IEEE 802.11 is a set of standards for wireless local area network (WLAN) computer communication, developed by the IEEE LAN/MAN Standards Committee (IEEE 802) in the 5 GHz and 2.4 GHz public spectrum bands.
Account Information Security Program (AIS)	See Visa Cardholder Information Security Program (CISP)
Acquirer	Financial institution that enters into agreements with merchants to accept Visa products as payment for goods and services. Also 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 Visa payment services.
At Risk Accounts	See Compromised Account.
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.
Backdoor	A method of bypassing normal authentication and obtaining access to plaintext information while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice), or could be a modification to an existing program or hardware device.
Bank Identification Number (BIN)	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 the number "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 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 that 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 the relationship to the client. Cardholder Data includes but is not limited to name, address, account number or portion of an account number, expiration date, full track 1 and/or 2 data, PIN, mag stripe data, and CVV2.
Client	An financial institution that issues cards and/or signs merchants to accept Visa products; it is subject to the terms of the Visa International Operating Regulations as a result of its relationship with Visa.
Common Point of Purchase (CPP)	Refers to the location of a legitimate transaction (usually a purchase or cash advance transaction) common to a number of accounts involved in a subsequent fraudulent transaction. The CPP entity would be investigated to determine if it was a point of compromise.
Compromise	Process where any third party obtains improper access to data systems.
Compromised Account	Any account made vulnerable to possible exfiltration as a result of a data security breach.
Compromised Account Management System (CAMS)	Used by financial institutions, merchants and law enforcement officers to safely upload compromised and stolen/recovered accounts directly to and from Visa. Information uploaded to CAMS is automatically sent via an e-mail alert to registered issuer users to provide notification of any vulnerable, compromised, and stolen/recovered accounts.
Cryptographic Key	A parameter used in conjunction with a cryptographic algorithm that determines: ▪ The transformation of plaintext data into ciphertext data ▪ The transformation of ciphertext data into plaintext data ▪ A digital signature computed from data ▪ The verification of a digital signature computed from data ▪ An authentication code computed from data or ▪ An exchange agreement of a shared secret

Denial of Service (DoS)	Denial of Service (DoS) is a tool or program used by intruders to cause networks and/or computers to cease operating effectively or to erase critical programs running on the system.
Electronic Commerce (e-commerce)	The purchase of goods and services over the Internet without a paper transaction between buyer and seller.
Encryption	An online data security method that scrambles data so that it is difficult to interpret without a corresponding decryption key.
Event	Refers to an event of a known or suspected data compromise. It is used interchangeably with the term "incident".
Full-Track Data	There are two tracks of data on a bankcard's magnetic stripe: Track 1 is 79 characters in length. It is alphanumeric and contains the account number, the cardholder name, and the additional data listed on Track 2. 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, 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.
IEEE (Institute of Electrical and Electronics Engineers, Inc.)	The Institute of Electrical and Electronics Engineers, Inc., is an international non-profit, professional organization for the advancement of technology. More info at *www.ieee.org*.
Incident Response Managers	Visa staff designated by a regional office to coordinate response to incidents.
Issuer	A financial institution that issues Visa products.
Magnetic Stripe (Mag Stripe)	A strip of magnetic tape located on the back of all bankcards. The magnetic stripe is encoded with identifying account information as specified in the Visa International Operating Regulations. On a valid card, the account information on the magnetic stripe matches similar embossed information located on the front of the card.
Man-in-the-Middle (MITM)	A form of eavesdropping in which an attacker makes independent connections with the victims and relays messages between them, making the victims believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker.

MD5 Hash	The MD5 hash (also known as checksum) for a file is a 128-bit value, similar to taking a fingerprint of a file.
Merchant	An entity that enters into a card acceptance agreement with a Visa acquirer or processor.
Merchant Bank	See Acquirer.
Merchant Level	All merchants fall into one of four merchant levels based on Visa transaction volume over a 12-month period.
PAN	Primary Account Number.
Payment Card Industry Data Security Standard (PCI DSS)	A set of requirements established by the payment card industry to protect cardholder data. Through CISP, these requirements apply to all Visa clients or members, and their merchants and service providers that store, process, or transmit cardholder data. *https://www.pcisecuritystandards.org/*
Payment Card Industry (PCI) PIN Security Requirements	A comprehensive set of measures created for the safe transmission and processing of cardholder PINs during ATM and point-of sale (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/pinsecurity*.
PCI Security Standards Council (PCI SSC)	The PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including: the Data Security Standard (DSS), Payment Application Data Security Standard (PA-DSS), and Pin-Entry Device (PED) Requirements. For more information on PCI SSC, visit *www.pcisecuritystandards.org/*
PCI Forensic Investigator (PFI)	The PCI Forensic Investigator (PFI) program establishes and maintains rules and requirements regarding eligibility, selection and performance of companies that provide forensic investigation services to ensure PFIs meet PCI Security Standards. The PFI program aims to help simplify and expedite procedures for approving and engaging forensic investigators by: ▪ Providing a single set of requirements for forensic investigators upon which market participants may align ▪ Maintaining a list of Council-approved forensic investigators for compromised entities to choose from ▪ Providing guidance on how investigations are to be conducted and reported
Personal Identification Number (PIN)	An alphabetic and/or numeric code which may be used as a means of cardholder identification.

Point of Compromise (POC)	Refers to the location in the breached entity's system where account number data was obtained by unauthorized third parties.
Rootkit	A program designed to take administrative control of a computer system without authorization from the system's owners.
Secure Shell (SSH)	"Secure Shell" is a network protocol that allows data to be exchanged using a secure channel.
Service Set Identifier (SSID)	"Service Set Identifier" is the name used to identify the particular 802.11 wireless LAN to which a user wants to attach.
Telnet (Telecommunications Network)	A network protocol used on the Internet or on Local Area Network (LAN) connections.
Third-Party Processor	A service provider organization acting as the client's agent 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*. In other regions (Latin America, Asia Pacific Central Middle East Africa and Canada) this program is named the Account Information Security (AIS) Program
VisaNet	The data processing systems, networks and operations used to support and deliver authorization services, exception file services, clearing and settlement services and any other services.
WAP (Wireless Application Protocol)	An open international standard for application layer network communications in a wireless communication environment.

WAP or AP (Wireless Access Point)	A computer networking device that allows wireless communication devices to connect to a wireless network using Wi-Fi and related standards. The WAP usually connects to a wired network and can relay data between both wireless and wired devices (such as computers or printers) on the network.
WEP (Wired Equivalent Privacy)	An algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio and are more susceptible to eavesdropping than wired networks.