What To Do If Compromised

Visa Fraud Control and Investigations Procedures

December 2008
Version 1.0 (U.S.)

Table of Contents

Introduction

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

In general, incidents may be defined as deliberate electronic attacks on communications or information processing systems. Whether initiated by a disgruntled employee, a malicious competitor, or a misguided hacker, deliberate attacks often cause damage and disruption to the payment system. How you respond to and handle an attack on your company's information systems will determine how well you will be able to control the costs and consequences that could result. For these reasons, the extent to which you prepare for security incidents, and work with Visa Inc., will be vitally important to the protection of your company's key information.

In the event of a security incident, Visa clients and their agents must take immediate action to investigate the incident, limit the exposure of cardholder data, notify Visa, and report investigation findings to Visa.[1]

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

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

[1] *Visa U.S.A. Inc. Operating Regulations*—Section 2.3.F.3, Loss or Theft of Account or Transaction Information; Section 2.3.F.4, Investigations; and Section 2.3, General Security Requirements. *Visa U.S.A. Plus System, Inc. Bylaws and Operating Regulations*—Section 1.19, Customer Information Security Program; *Visa U.S.A. Interlink Network, Inc. Bylaws and Operating Regulations*—Section 2.4, Investigation of Merchants; Section 2.6, Cardholder Information Security Program; Section 2.8, Loss or Theft of Account Information. *Visa U.S.A. Inc. Operating Regulations* are available at *www.visa.com*.

Identifying and Detecting Security Breaches

It is often difficult to detect when a system has been attacked or an intrusion has taken place. Distinguishing normal events from those that are related to an attack or intrusion is a critical part of maintaining a secure payment processing environment.

Security breaches come in many different forms and, while detecting them may be challenging, there are certain signs that tend to appear when a security breach has occurred:

- Unknown or unexpected outgoing Internet network traffic from the payment card environment
- Presence of unexpected IP addresses on store and wireless networks
- Unknown or unexpected network traffic from store to headquarter locations
- Unknown or unexpected services and applications configured to launch automatically on system boot
- Unknown files, software and devices installed on systems
- Anti-virus programs malfunctioning or becoming disabled for unknown reasons
- 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 in web server event 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 .zip, .rar, .tar, and other types of unidentified compressed files containing cardholder data
- 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
- If you are running Microsoft, check Windows registry settings for hidden malicious code. (**Note:** Make sure you back up your registry keys before making any changes and consult with Microsoft Help and Support).

Attack Vectors

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

SQL Injection Attacks

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

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

Improperly Segmented Network Environment

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

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

Malicious Code Attacks

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

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

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

  Packet sniffers are typically used in conjunction with malicious software or malware. Once intruders gain entry into a critical system using backdoor programs or deploying rootkits, the sniffer programs are installed, making the malware more difficult to detect. Intruders can then "sniff" packets between network users and collect sensitive information such as usernames, passwords, payment card data or Social Security numbers. Once a critical system or network is compromised, sniffers are used to eavesdrop or spy on network users and activity. This combination of tools makes this attack scheme effective in compromising systems and networks.
- **Key logger malware.** Key logging is a method of capturing and recording keystrokes. There are key logger applications that are commercially available and are used by organizations to troubleshoot problems within computer systems. Visa Investigations reveal that there are key logger applications that are developed by intruders to capture payment card data and/or users credentials, such as passwords. The key logger captures information in real time and sends it directly to the intruder over the Internet. Additionally, newer advances provide the ability to intermittently capture screenshots from the key logged computer.

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

Insecure Remote Access

Many Point-of Sale ("POS") 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:

- Failure to regularly update or patch a system can render the system vulnerable to exploits that defeat the security mechanisms built into the product.
- Lack of encryption or weak encryption algorithms can lead to the disclosure of access credentials.
- Use of default passwords can provide easy access to unauthorized individuals.
- Disabled logging mechanisms eliminate insight into system access activity and signs of intrusion.

Insecure Wireless

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

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

- **Eavesdropping** — An attacker can gain access to a wireless network just by "listening" to traffic. Radio transmissions can be freely and easily intercepted by nearby devices or laptops. The sender or intended receiver has no means of knowing whether the transmission has been intercepted.

- **Rogue Access** — If a wireless Local Area Network (LAN) is part of an enterprise network, a compromise of the LAN may lead to the compromise of the enterprise network. An attacker with a rogue access point can fool a mobile station into authenticating with the rogue access point, thereby gaining access to the mobile station. This is known as a "trust problem," and the only protection against it is an efficient access-authentication mechanism.
- **Denial of Service (DOS)** — Due to the nature of radio transmission, wireless LANs are vulnerable to denial-of-service attacks and radio interference. Such attacks can be used to disrupt business operations or to gather additional information for use in initiating another type of attack.
- **Man-in-the-Middle (MITM)** — Packet spoofing and impersonation, whereby traffic is intercepted midstream then redirected by an unauthorized individual for malicious purposes, are also valid threats.

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

Steps and Requirements for Compromised Entities

Entities that have experienced a suspected or confirmed security breach must take prompt action to help prevent additional exposure of cardholder data and ensure compliance with the Payment Card Industry Data Security Standard (PCI DSS), PCI Payment Application Data Security Standard (PA-DSS)[2], and PCI PIN Security Requirements[3].

1. Immediately contain and limit the exposure. Minimize data loss. Prevent the further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information. Compromised entities should consult with their internal incident response team. To preserve evidence and facilitate the investigation:
   - Do not access or alter compromised system(s) (i.e., don't log on at all to the compromised system(s) and change passwords; do not log in as ROOT).
   - Do not turn the compromised system(s) off. Instead, isolate compromised systems(s) from the network (i.e., unplug network cable).
   - Preserve logs (i.e., security events, web, database, firewall, etc.)
   - Log all actions taken.
   - If using a wireless network, change the Service Set Identifier (SSID) on the wireless access point (WAP) and other systems that may be using this connection (with the exception of any systems believed to be compromised).
   - Be on "high" alert and monitor traffic on all systems with cardholder data.

[2] *Visa U.S.A. Inc. Operating Regulations*—Section 2.1.E.3, Loss or Theft of Account or Transaction Information; Section 2.1.E.4, Investigations; and Section 2.3, General Security Requirements. *Visa U.S.A. Plus System, Inc. Operating Regulations*—Section 1.19, Customer Information Security Program. *Visa U.S.A. Interlink Network, Inc. Operating Regulations*—Section 2.4, Investigation of Merchants; Section 2.6, Cardholder Information Security Program; Section 2.8, Loss or Theft of Account Information. Visa Operating Regulations are available at *www.visa.com*.

[3] By submitting a Transaction through Interchange, an Acquirer warrants that required safeguards, as specified in the *PIN Management Requirements* documents, are protecting the Issuer's PIN. The Acquirer agrees to indemnify and hold harmless the Issuer for all Claims and Liabilities resulting from the Acquirer's breach of this warranty. *Visa U.S.A. Operating Regulations*—Section 1.16.B.45. *Visa U.S.A.Interlink Network, Inc. Bylaws and Operating Regulations*—Section 1.10.D.1. *Visa U.S.A. Plus System, Inc. Bylaws and Operating Regulations*—Section 1.10.C.

2. Alert all necessary parties immediately:
   - Your internal incident response team and information security group.
   - If you are a merchant, contact your merchant bank.
   - If you do not know the name and/or contact information for your merchant bank, notify Visa Incident Response Manager immediately:
     - U.S. – (650) 432-2978 or usfraudcontrol@visa.com
     - Canada – (416) 860-3090 or CanadaInvestigations@visa.com
     - Latin America & Caribbean – (305) 328-1713 or lacrmac@visa.com
     - Asia Pacific – (65) 96307672 or APInvestigations@visa.com
     - CEMEA – +44 (0) 207-225-8600 or *CEMEAFraudControl@visa.com*

     If you are a financial institution, contact the appropriate Visa region at the number provided above.
3. Notify the appropriate law enforcement agency. (See *Appendix J*, on page 59, for United States Secret Service Electronic Crimes Task Force contact information in your area.)

KEY POINT TO REMEMBER

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

4. The compromised entity should consult with its legal department to determine if state notification laws are applicable.
5. Provide all compromised Visa, Interlink, and Plus accounts to the Visa acquiring bank or to Visa within ten (10) business days. 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.

6. Within three (3) business days of the reported compromise, provide an Incident Report to the Visa client or to Visa. (See *Appendix C,* on page 28, for the Incident Report template.) If you are a financial institution, provide the Incident Report to Visa.

   Note: If Visa deems necessary, an independent forensic investigation by a Visa-approved Qualified Incident Response Assessor (QIRA) will be initiated on the compromised entity. This policy applies to compromised financial institutions.

Steps and Requirements for Visa Clients (Acquirers and Issuers)

Notification

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

Preliminary Investigation

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

FOR MORE INFORMATION

To find out more about conducting an initial investigation, see *Appendix A: Initial Investigation Request* on page 19.

Independent Forensic Investigation

If Visa deems necessary, an independent forensic investigation must be conducted by a QIRA.

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

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

KEY POINT TO REMEMBER

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

5. If there is a suspected PIN compromise, the QIRA will perform a PIN security and key management investigation and a PCI PIN security assessment.
6. Provide a preliminary forensic report to Visa within five (5) business days from the onsite review. *The QIRA or the compromised entity can work with the appropriate region in the event that the preliminary report is delayed.*
7. Provide a final forensic report to Visa within ten (10) business days from the completion of the review.

PIN Security

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

Account Numbers

9. Provide "at risk" account numbers to Visa within ten (10) business days from the date that Visa requests the account numbers.

Containment/ Remediation

10. Ensure that the compromised entity has contained the incident and has implemented security recommendations provided by the QIRA, including any non-compliance with the PCI PIN Security Requirements.
11. If the entity is retaining full-track data, CVV2, and/or PIN blocks, ensure that the entity has removed the data (this includes any historical data).
12. Validate that full-track data, CVV2, and/or PIN blocks are no longer being stored on any systems. Even though this is the client's responsibility, Visa requires that the validation be performed by the QIRA.
13. Submit a remediation plan to Visa within five (5) business days after receiving the final forensic report. As required by Visa, clients must provide a remediation plan with implementation dates related to findings identified by the QIRA.

    A revised remediation plan must be provided to Visa, as needed.
14. Monitor and confirm that the compromised entity has implemented the action plan.

PCI DSS Compliance

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

KEY POINT TO REMEMBER

Please visit *www.pcisecuritystandards.org* for more information on PCI DSS and the PCI PIN Entry Device Testing Program. For more information on PCI PIN Security Requirements, please visit *www.visa.com/pinsecurity*.

Requirements for Account Data Requests

In the event of a compromise, Visa requires that "at risk" accounts be provided to Visa through Visa's Compromised Account Management System (CAMS).

In some cases, Visa may require the entity to provide accounts via a CD using encryption software such as PGP[4] or Winzip[5] with 256-AES encryption and strong password. The following guidelines must be followed when providing accounts to Visa:

Account Data Format

- The account data provided must be **authorization** data only.
- File submitted must be a plain-text, comma delimited file containing account numbers and expiration dates. For example:
  - The card number, followed by a comma, followed by the expiration date in YYMM format:

    4xxxxxxxxxxx1234,0801

KEY POINT TO REMEMBER

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

Please refer to *Appendix E* for information on the Advanced Account Data Format and Account Data File Layout.

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

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

[5] 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.

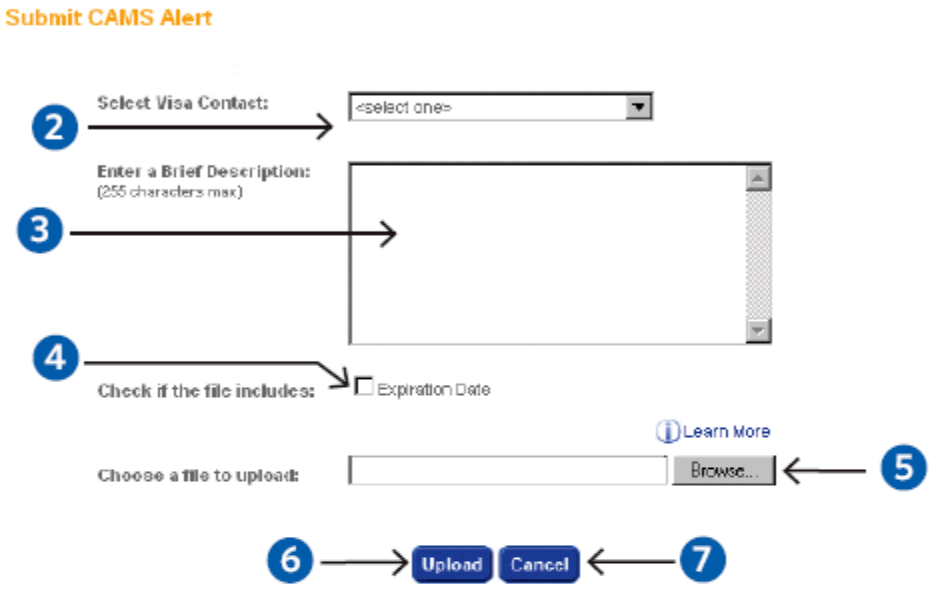
Compromised Account Management System (CAMS)

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

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

To Upload File(s):

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



2. From the drop down menu, select your assigned Visa contact. **This field is required.**
3. Enter a brief description of the files you are uploading for the compromise.
4. If applicable, indicate whether the file includes an expiration date. (Indicating an account expiration date will help the issuer identify which accounts are good candidates for monitoring.)

5. Click "Browse" to select a file from your local hard drive.
   - Files must be either plain text or a .zip file containing plain text files.
   - Files cannot exceed 100 MB in size.
   - The uploaded file should contain 11-19 digit account numbers.
6. Click the "Upload" button to begin the file transfer process. *The progress box will display how much of the upload has been completed.*
7. To stop the file transfer, click the "**Cancel**" button at any time.

To Upload Additional File(s):

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

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

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

Appendix A: Initial Investigation Request

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

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

KEY POINT TO REMEMBER

The information required below is applicable to suspected/confirmed compromised entities such as Visa clients, 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.)	
If merchant, date entity began processing with acquirer	
If merchant, date entity stopped processing with acquirer (if applicable)	
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: ▪ 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?	

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?	
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 *www.visa.com/PABP* 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.	

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 November 2007 Security Alert available at *www.visa.com/cisp*?	

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 or compromised entity must ensure that only a Visa-approved Qualified Incident Response Assessor (QIRA) is engaged to perform a forensic investigation. All QIRAs are required to adhere to the following forensic investigation guidelines. Visa clients can also use these guidelines to monitor the work by the QIRA. Visa will NOT accept forensic reports from non-approved forensic companies. QIRAs are required to release forensic reports and findings to Visa.

Note: The Visa client or compromised entity should contact the appropriate Visa region for a list of QIRAs.

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

1. QIRA will assess compromised entity's computing environment to determine the scope of the forensic investigation and relevant sources of electronic evidence. This includes, but is not limited to:
   - Assessment of all external and internal connectivity points within each location involved.
   - Assessment of network access controls between compromised system(s) and adjacent and surrounding networks.

KEY POINT TO REMEMBER
Visa reserves the right to engage the QIRA.

2. QIRA will acquire electronic evidence from the compromised entity's host and network-based systems.
   - Forensic evidence acquisition must be conducted onsite at the compromised entity's premises.
   - If circumstances do not permit onsite evidence acquisition, QIRA must notify Visa.
   - Preservation of all potential electronic evidence on a platform suitable for review and analysis by a court of law, if applicable.
3. Forensically examine electronic evidence to find cardholder data and establish an understanding of how a compromise may have occurred.

4. Verify that cardholder data is no longer at risk and/or has been removed from the environment.
5. Verify that the compromised entity has contained the incident.
6. QIRA must use Visa's Incident Report template and provide a forensic report to all parties involved in the incident.
7. Perform external and internal vulnerability scans, including network and application scans.
8. The following actions must be included as part of the forensic investigation:
   - Determine and describe the type of processing environment:
     - Organization Description (check all that apply):
     - VisaNet processor
     - Issuer only
     - Acquirer only
     - Both issuer and acquirer
     - Pre-paid issuer
     - Third-party processor
     - Merchant
     - Other: _____
   - Estimated annual number of credit and or debit transactions for Visa-branded products (based on interview; exact numbers are not required):
     - Visa credit
     - Visa debit (Visa Signature only)
     - Visa with PIN (ATM with PIN)
     - Interlink (POS with PIN)
     - Plus (ATM with PIN)
     - Visa Prepaid (include list of Prepaid products)
     - Other: _____

9. Check and determine cardholder information that is at risk. This includes:
   - Number of and types of Visa/Plus/Interlink/Prepaid accounts at risk. Identity those stored and captured by malware (e.g., packet sniffer, key logger).
   - List of associated account information at risk:
     - Full magnetic-stripe data (e.g., Track 1 and 2)
     - PIN blocks and clear-text PINs. To identify potential presence of PIN blocks, also look for the PIN block format code field (see *Account Data Layout Format, Appendix E,* for more information).
     - CVV2
     - Account number
     - Expiration date
     - Other sensitive data elements (e.g., SSN, DOB)
     - Cardholder name
     - Cardholder address
     - Cardholder e-mail address
   - QIRA to examine all potential locations, including payment applications, to determine if full magnetic-stripe data, CVV2, and/or PIN blocks are stored (whether encrypted or unencrypted) on production, backups, tables, development, test, software engineer, and administrator's machines.
   - QIRA should also check volatile memory for cardholder data.
   - If malware was used to capture cardholder data, QIRA must review any malware output logs and validate whether cardholder data was captured and stored.
   - Other logs that must be reviewed include the following:
     - Server
     - Application
     - Transaction
     - Troubleshooting
     - Debug
     - Exception or error files
   - QIRA must provide account information to Visa (see *Requirements for Account Data Request*, page 15).

10. Determine time frame of accounts at risk. For example:
    - Determine how long accounts were stored on the system(s).
    - Determine the transaction date(s) of accounts stored on the system(s).
11. Perform incident validation and assessment. This includes:
    - Establishing how a compromise occurred.
    - Identifying the source of the compromise.
    - Window of system vulnerability. This is defined as the frame of time in which a weakness(s) in an operating system, application or network could be exploited by a threat to the time that weakness(s) is properly remediated.
    - Determining if any cryptographic keys have been exposed or compromised.
    - Reviewing the entire debit and/or credit processing environment to identify all compromised or affected systems; considering the e-commerce, corporate, test, development, production systems, VPN, modem, DSL, cable modem connections, and any third-party connections.
    - If applicable, review VisaNet endpoint security and determine risk.
    - Identifying the date(s) that account data was transferred out of the network by the intruder or malware.
    - Date(s) when the entity began using the payment application and version number. Determine if the payment application is PA-DSS compliant.
    - If available, identify the date(s) when the entity installed a patch or an upgrade to no longer retain prohibited data.
    - The date(s) that malware was installed on the system, if applicable.
    - Date(s) when malicious code, such as packet sniffer and/or key logger, was activated to capture payment card data on the network and system. QIRA must include date(s) of when malware was de-activated.
    - Determine the window of intrusion. This is the first confirmed date that the intruder or malware entered the system to the date of containment
12. Determine what applicable PCI security requirements apply:
    - PCI DSS
    - PCI PIN Security Requirements
    - PCI POS PIN Entry Device Security Requirements
    - PCI Encrypting PIN PAD (EPP) Security Requirements
    - PCI PA-DSS
13. If malware and bad IPs are identified in the compromise, the QIRA must submit the malware code and bad IPs via a secure distribution to *uscyberforensics@visa.com.*

Table of Entities and Requirements Applicability

REQUIREMENTS	TYPES OF ENTITIES						
	Issuer Processor	**Acquirer Processor**	**Credit Only Merchant**	**Debit Accepting Merchant**	**Issuer and Acquirer Processor**	**ATM Processor**	**Third-Party Servicer**
PCI DSS	Applies	Applies	Applies	Applies	Applies	Applies	Applies
PCI PIN Security Requirements	Applies if driving their own ATMs	Applies if processing debit	N/A	Applies	Applies	Applies	Applies if processing debit
PCI POS and PCI EPP PIN Entry Device Security Requirements	N/A	Applies if processing debit	N/A	Applies	Applies	Applies	Applies if processing debit
PCI PA-DSS	Applies	Applies	Applies	Applies	Applies	Applies	Applies

14. QIRAs must utilize Visa's report template. See *Appendices C and D, Incident Report template* for more information.

Appendix C: Preliminary Incident Report Template

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

The Preliminary Incident Response Report document can be completed by the compromised entity or by an approved QIRA. Once completed, the report must be distributed to Visa, the client, and the compromised entity. Visa will classify the report as Visa Confidential.

QUESTIONS	RESPONSES
Name of compromised entity	
Date arrived onsite	
Evidence of a breach (Y/N)	
First confirmed date that the intruder or malware entered the network	
Scope of forensic investigation (e.g., single vs. numerous locations)	
Type of data impacted (e.g., full track, CVV2, PIN blocks)	
Window of system vulnerability	
Initial thoughts on attack vector	
Is the security breach ongoing or has it been contained?	
Other comments	

Appendix D: Final Incident Report Template

I. Executive Summary (include the following information):

- Date when the forensic company was engaged
- Date(s) when forensic investigation began
- Location(s) visited or forensically reviewed
- A brief summary of the scope of the forensic investigation
- A brief summary of the environment reviewed (details must be documented under the "Findings" section)
- Cause of intrusion
- Date(s) of intrusion
- Data elements at risk (e.g., full track, CVV2, PIN blocks)
- Specify whether or not the security breach has been contained

II. Background

- Brief summary of compromised entity company:
- Type of business entity:
  - Merchant (brick and mortar, e-commerce or both)
  - Prepaid issuer
  - Issuer
  - Acquirer
  - Acquirer processor
  - Issuer processor
  - ATM processor
  - Third-party service provider (web hosting; co-location)
  - Encryption Support Organization (ESO)
  - Payment application vendor
  - Payment application reseller

- PCI compliance and other information:
  - PCI DSS level and compliance status
  - Number of locations
  - Parent company (if applicable)
  - Franchise or corporate-owned

III. Incident Dashboard

CLIENT	TYPE OF BUSINESS ENTITY
Date when entity identified compromise	
Method of identification	Self Detection or Common Point of Purchase
Window of system vulnerability	
Window of intrusion	
Malware installation date(s), if applicable	
Date(s) of real time capture, if applicable	
Date(s) that data was transferred out of the network, if applicable	
Window of payment card data storage	
Transaction date(s) of stored accounts	
Date and version of POS installation(s), if applicable	
Type of data exposed	▪ Cardholder name ▪ Cardholder address ▪ PAN ▪ Expiry date ▪ CVV2 ▪ Track data ▪ Encrypted PINs
Brand exposure	▪ Visa ▪ MC ▪ DISC ▪ AMEX ▪ JCB

CLIENT	TYPE OF BUSINESS ENTITY
Number of cards exposed (both live system space and unallocated space)	▪ Include breakdown by card brand type ▪ Include breakdown of the following: – Signature – PIN-based transactions – Issuer-only data – Non-issuer data – Prepaid data
Logs that provided evidence: ▪ Firewall logs ▪ Intrusion detection systems ▪ Database queries ▪ FTP server logs ▪ System login records ▪ Web server logs	▪ File integrity monitoring output ▪ Transaction logs ▪ Remote access logs ▪ Wireless connection logs ▪ Anti-virus logs ▪ Security event logs ▪ File creation/access date
Suspected cause summary	Insert brief case summary. Detailed findings should be included in the "Findings" section of the report.

If applicable, document the type of cryptographic keys at risk. (See "*PIN Security Requirements*", page 46 of this section.)

ISSUER SIDE CRYPTOGRAPHIC KEYS	ACQUIRER SIDE CRYPTOGRAPHIC KEYS
Issuer Working Keys (IWK)	Acquirer Working Keys (AWK)
PIN Verification Keys (PVK)	POS, ATM, EPP PIN Encryption Keys
CVV, DCVV, ICVV Verification Keys CVV2 Verification Keys (CVK2) Cardholder Authentication Verification Value Keys (CAVV and CAK) Cardholder Authentication Attempts Value Keys (CAAV)	POS, ATM, EPP Key Encrypting Keys (KEKs)
PIN Generation Keys	Remote Initialization Keys
Master Derivation Keys (MDK)	Host to Host Working Keys Key Encrypting Keys (KEKs)
Host to Host Working Keys Key Encrypting Keys (KEKs)	Switch Working Keys
Switch Working Keys	

IV. Network Infrastructure Overview

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

V. Findings

- Provide specifics on firewall, infrastructure, host, and personnel findings
- Identify any and all changes made to the compromised entity's computing environment after the identification of a compromise
- Provide specific dates of network, system, or payment application changes
- Include any and all forensic evidence supporting changes made to networks, systems, and POS components
- Identify any data accessed by unauthorized user(s)

- Identify any data transferred out of the network by unauthorized user(s)
- Identify any evidence of data deletion from systems involved in a compromise
- If applicable, identify any deleted data recovered through forensic file recovery methods
- Identify any third-party payment applications, including version number
- Identify any upgrades/patches to the payment application that address removal of magnetic-stripe data, CVV2, and/or encrypted PIN blocks
- Provide an attack timeline of events. Include relevant date(s) and activities (e.g., date/time created, system/file evidence, description of evidence)
- Include a list of compromised systems/hosts (e.g., operating system; application and its functionality)
- Include a list of malicious IPs. Include any information related to malicious IPs (e.g., part of hacker group)
- Include a list of all malware identified. Include the following information on malware:
  - Name of malware
  - MD5 Hash
  - Registry settings
  - File size
  - System path

VI. Compromised Entity Containment Plan

- Document what the entity has done to contain the incident. Include date(s) of containment.

VII. Recommendation (s)

- List recommendations by priority level

VIII. PCI DSS Compliance Status

- Based on findings identified in the forensic investigation, indicate the compliance status for each of the 12 basic requirements under the PCI DSS
- Document the specific PCI DSS requirements and sub-requirements that contributed to the security breach

PCI DSS		
REQUIREMENTS	**IN PLACE**	**NOT IN PLACE**
BUILD AND MAINTAIN A SECURE NETWORK		
Requirement 1: Install and maintain a firewall configuration to protect cardholder data		
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters		
PROTECT CARDHOLDER DATA		
Requirement 3: Protect stored cardholder data		
Requirement 4: Encrypt transmission of cardholder data across open, public networks		
MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM		
Requirement 5: Use and regularly update anti-virus software		
Requirement 6: Develop and maintain secure systems and applications		
IMPLEMENT STRONG ACCESS CONTROL MEASURES		
Requirement 7: Restrict access to cardholder data by business need-to-know		
Requirement 8: Assign a unique ID to each person with computer access		
Requirement 9: Restrict physical access to cardholder data		
REGULARLY MONITOR AND TEST NETWORKS		
Requirement 10: Track and monitor all access to network resources and cardholder data		
Requirement 11: Regularly test security systems and processes		
MAINTAIN AN INFORMATION SECURITY POLICY		
Requirement 12: Maintain a policy that addresses information security		

Appendix E: Account Data Layout Format

As mentioned in the previous section, clients are required to follow the following format on all account data requests. The account data must be **AUTHORIZATION DATA ONLY.**

Submitted data should be limited to one file. In cases where one file isn't possible, make every effort to minimize total file counts. If multiple files are provided, all of them must be consistent and contain the same formatting and transaction details.

The data submission may be a fixed width or delimited text file. Acceptable field delimiters are comma, tab, semicolon, space, or pipe (with or without text qualifiers). Field headers must be in the file or included on a separate file layout document.

Acceptable formats for each field (alpha (A), numeric (N), alphanumeric (AN), or alphanumeric special character (ANS)) are included in the descriptions. The International Standards Organization (ISO) field is noted if there is a corresponding field for further information.

The following are acceptable examples of file layouts and account data formats.

Advanced Format

In some cases, Visa will require additional transaction detail for further analysis. Provide information in as many fields as possible.

- Credit accounts signature (to include transaction details, see following bulleted list)
- Debit accounts signature (to include transaction details, see following bulleted list)
- Debit accounts used with a PIN (to include transaction details, see following bulleted list)
- Key-entered accounts (to include transaction details, see following bulleted list)

Transaction details are defined as follows:

- Primary account number (PAN)
- Expiration date
- Transaction amount
- Transaction date
- Merchant Category Code (MCC)
- Point-of-Service Entry Mode Code (POS entry)
- Visa Acquiring Bank Identification Number (BIN)

- Visa Acquiring Processor Control Record (PCR)
- Card Acceptor Identification Code (CAID)
- Card Acceptor Terminal Identification
- PIN transaction indicator
- Card acceptor name/location
- Card acceptor city
- Card acceptor country

Descriptions

Primary Account Number (PAN)

Format: N

ISO Field 2

The PAN contains the number identifying the cardholder account or relationship. The value is a cardholder account number of up to 19 numeric digits embossed on the card and also encoded on Track 1 and Track 2 of the magnetic stripe. The PAN is present in both face-to-face and card not present (CNP) transactions.

Allowable Card Account Number Lengths

Visa Card 16 digits.

16-digit example: 4444333322221111

Expiration Date

Format: N

ISO Field 7 (Track 1)

ISO Field 4 (Track 2)

Transaction Amount

Format: N

Cardholder transaction amount is in either U.S. dollars or per the currency code in Field 49. If the amount is not in U.S. dollars, then the currency code should also be present in a separate field.

Examples:

$45.30

45.30

45.30, 250 (ISO currency code)

Transaction Date

Format: AN

Field contains the date of cardholder transaction. Acceptable formats should include the month, day, and year of transaction. Julian date is allowable.

Examples:

MM/DD/YYYY (03/15/2006)
DD/MM/YYYY (15/03/2006)
MM/DD/YY (03/15/06)
DD-MMM-YY (15-MAR-06)
March 15, 2006
YYDDD (06074) – Julian date

Merchant Category Code (MCC)

Format: N

ISO Field 18

Field contains a code describing the merchant's type of business product or service (also known as the Merchant Category Code (MCC)). Valid codes are listed in the *Visa U.S.A. Inc.* and *Visa International Operating Regulations.*

Examples:

5192 – Books, Periodicals, and Newspapers
5542 – Automated Fuel Dispensers
6011 – Financial Institutions – Automated Cash Disbursements
7230 – Hair Salon

Point-of-Service Entry Mode Code (POS entry)

Format: N

ISO Field 22: Positions 1 and 2 required

Field contains codes that identify the actual method used to capture the account number and expiration date and, when a point-of-transaction terminal is used, its PIN capture capability. This field is fixed-length with three sub-fields. The position assignments are as follows:

Positions 1 and 2

PAN and Date Entry Mode: A two-digit code that identifies the actual method used to enter the cardholder account number and card expiration date. This code specifies whether the entire magnetic stripe is included in an authorization or financial request.

Position 3

PIN Entry Capability – A one-digit code that identifies the capability of a terminal to accept PINs; it does not necessarily mean that the PIN was entered or is included in the message. A value of "1" means that the terminal can accept PINs; a value of "2" indicates that the terminal can not accept PINs.

Examples:

90 – Magnetic-stripe read and exact contents of Track 1 or Track 2 included. CVV or dCVV check is possible.

02 – Magnetic-stripe read; CVV checking may not be possible.

01 – Manual key entry

Visa Acquiring Bank Identification Number (BIN)

Format: N

This field identifies the financial institution acting as the acquirer of this customer transaction. The acquirer is the client or system user that signed the merchant, installed the ATM or ADM, or dispensed cash.

Visa BINs are six (6) digits. For processing centers handling multiple acquirers, this code identifies the individual acquirer or system user, not the overall processing center.

Examples:

400850

458307

Visa Acquiring Processor Control Record ("PCR")

Format: N

This field, consisting of four (4) digits, identifies the processing center acting as the agent of the acquiring client that provides authorization, clearing, or settlement services for the merchant.

Examples:

4321 – ABC Processing Services

5678 – ABC Merchant

Card Acceptor Identification Code (CAID)

Format: ANS

ISO Field 42

This field contains the identifier of the card acceptor operating the point-of-sale or point-of-service (POS) terminal (or at the ATM) in local and in interchange environments. The CAID can be up to 15 bytes; if the ID is less than 15 positions, it must be left-justified and space-filled.

Examples:

140000015613401
58678062890003
6922I858RP357H
3655139M

Card Acceptor Terminal Identification

Format: ANS

ISO Field 41

This field contains a code that identifies the card acceptor terminal or ATM. For electronic POS terminals, when the ID is not unique to a specific terminal, Field 42 (CAID) can be used along with this field. ATM terminal IDs must be unique within the acquirer's network.

An identification code of fewer than eight (8) bytes must be left-justified and the remainder of the field space filled.

Examples:

80046578
8RNL9055
073
RI895B

PIN Transaction Indicator

Format: AN

This field indicates whether or not the transaction was PIN-based. This is the field that is used to differentiate signature-based versus PIN-based transactions.

Examples:

PIN, No PIN
Yes, No
Numeric codes: 1=PIN, 2=No PIN

Personal Identification Number (PIN) Data

ISO Field 52

Attributes: Fixed Length 8 bytes; 64-bit string/16 hex

Hex values include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

Description: Field 52 contains an encrypted PIN block , formatted as a block of

16 hexadecimal digits. (0 – 9, A – F)

Examples:

2B9FFC29A40A25F3
9A40A252B9FFCBB1
40A2529A4077440A
BA669A40A2527229
2529A40A90ACD199
C510AE889FA92B7F

Security-Relate Control Information

ISO Field 53

Attributes: Fixed Length 8 bytes; 16 numeric 4-bit BCD

Positions 5 - 6 PIN Block Format Code

The code in Field 53.3 ("PIN Block Format Code") defines the format of Field 52 ("The PIN Block"). This field describes the PIN block format used by the acquirer/merchant and indicates the presence of a PIN. Values for Positions 5 – 6 are "01", "02", "03" and "04" and indicate the format of the PIN block used.

Note: Visa PIN block format numbering is different than that of ISO 9564, which is used in the PIN Security Requirements.

Card Acceptor Name/Location

Format: ANS

ISO Field 43

This field contains the name and location of the card acceptor (such as merchant or ATM) and includes the city name and country code. Field 43 has a single fixed length format, but the content of positions 1-25 depends on whether the request is for a Visa Interlink POS transaction, a Visa or Visa Plus ATM, or a VisaPhone transaction.

For Visa Interlink POS/ATM and Visa Plus ATM transactions, when the point of service is not in the same country as the acquirer, Field 43 must identify the card acceptor country. Field 43 also identifies the merchant or ATM location.

Positions 1-25, Card Acceptor Name:

POS: Merchants name as known to the cardholder.

ATM: The ATM location, branch number, or street address only (**Note**: the institution name is in Field 42).

Examples:

Bob's Fish Shack
AM RED CROSS DONATION
WWW MOULIN COM
Bookstore 53

Position 26-38, City Name:

POS: City where the customer transaction occurs.

Custom Payment Service (CPS) Card Not Present: Instead of the city name, these positions must contain the merchant's customer service telephone number, including country and area codes.

ATM: City where the ATM is located, branch number or street address only (**Note**: the institution name is in Field 42).

Examples:

Savannah
888 777 8888
PARIS
Madrid

Positions 39-40, Country Code:

POS and ATM: The two-character alpha code in uppercase format for the country where the cardholder transaction occurs or the ATM is located.

Examples:

US
FR
ES
PE

The following are samples of File Layouts:

Sample 1

File Layout

Primary Account Number|Transaction Amount|Transaction Date|Merchant Category Code|POS entry|Acquirer BIN|Acquirer PCR|Card Acceptor ID|Card Acceptor Terminal ID|PIN Indicator|Card Acceptor Name|Card Acceptor City|Card Acceptor Country

File

4111111111111111|87.5|06057|4816|01|426696|4008|426696100008681|1954|N|GO MAN COM|BALTIMORE|US

4321432143214321|570.28|06068|5912|01|400088|9088|1420005995|05995TS0|N|WALRUS|MT WHISKEY|US

4222222222222222|50|06066|7399|02|469216|2840|924944000192138||N|J2 COMMUNICATE|323 850 3214|US

4141414141414141|11.89|06057|4816|01|400088|9088|106171000991232||N|YABO VOICE|0821230270|EU

4564564564564568|174.5|06063|5399|01|400088|9088|000324202994996|00110825|N|SOYLENT VENTURES|SUNNYTOWN|US

4987654321987654|1|06066|4814|01|461043|4401|67211400015P003|Q3B50F0Q|N|UNICYCLE INTERNET|866 844 1849|US

4846512378945678|60.16|06056|4900|90|461043|8402|67354430019P003|Q3AAF40Q|Y|AQUILA INC|800 378 3357|US

4123456789123456|5.33|06058|7311|01|400088|9088|22628782|24680137|N|GOGGLE CC GOGGLE|OG ADWORDS|GB

Sample 2 for PIN Debit

File Layout (Debit Accepting Merchant)

Primary Account Number|Transaction Amount|Transaction Date|Merchant Category Code|POS entry|Acquirer BIN|Acquirer PCR|Card Acceptor ID|Card Acceptor Terminal ID|PIN Entry Capability|Card Acceptor Name|Card Acceptor City|Card Acceptor Country | PIN Block Format Code | PIN block

File

4111111111111111|87.5|06057|4816|01|426696|4008|426696100008681|1954|1|GO MAN COM|BALTIMORE|US|01| 2B9FFC29A40A25F3

4321432143214321|570.28|06068|5912|01|400088|9088|1420005995|05995TS0|1|WALRUS|MT WHISKEY|US|01| 9A40A252B9FFCBB1

4222222222222222|50|06066|7399|02|469216|2840|924944000192138||1|J2 COMMUNICATE|323 850 3214|US |01|40A2529A4077440A

4141414141414141|11.89|06057|4816|01|400088|9088|106171000991232||1|YABO VOICE|0821230270|EU|01| BA669A40A2527229

4564564564564568|174.5|06063|5399|01|400088|9088|000324202994996|00110825|1|SOYLENT VENTURES|SUNNYTOWN|US |01|2529A40A90ACD199

4987654321987654|1|06066|4814|01|461043|4401|67211400015P003|Q3B50F0Q|1|UNICYCLE INTERNET|866 844 1849|US |01|C510AE889FA92B7F

4846512378945678|60.16|06056|4900|90|461043|8402|67354430019P003|Q3AAF40Q|1|AQUILA INC|800 378 3357|US |01|8A2527229C510AE8

4123456789123456|5.33|06058|7311|01|400088|9088|22628782|24680137|1|GOGGLE CC GOGGLE|OG ADWORDS|GB |01|9FA92B7FA2527229

Sample 3

File Layout

"PAN";"Transaction Amount";"Transaction Date";"MCC";"POS entry";"Acq BIN";"Acq PCR";"CAID";"CA Terminal ID";"PIN Indicator";"CA Name";"CA City";"CA Country"

File

"4111111111111111";"87.5";"06057";"4816";"01";"426696";"4008";"4266961000008681";"1954";"N";"GO MAN COM";"BALTIMORE";"US"

"4321432143214321";"570.28";"06068";"5912";"01";"400088";"9088";"1420005995";"05995TS0";"N";"WALRUS";"MT WHISKEY";"US"

"4222222222222222";"50";"06066";"7399";"02";"469216";"2840";"9249444000192138";;"N";"J2 COMMUNICATE";"323 850 3214";"US"

"4141414141414141";"11.89";"06057";"4816";"01";"400088";"9088";"106171000991232";;"N";"YABO VOICE";"0821230270";"EU"

"4564564564564568";"174.5";"06063";"5399";"01";"400088";"9088";"000324202994996";"00110825";"N";"SOYLENT VENTURES";"SUNNYTOWN";"US"

"4987654321987654";"1";"06066";"4814";"01";"461043";"4401";"67211400015P003";"Q3B50F0Q";"N";"UNICYCLE INTERNET";"866 844 1849";"US"

"4846512378945678";"60.16";"06056";"4900";"90";"461043";"8402";"67354430019P003";"Q3AAF40Q";"Y";"AQUILA INC";"800 378 3357";"US"

"4123456789123456";"5.33";"06058";"7311";"01";"400088";"9088";"22628782";"24680137";"N";"GOGGLE CC GOGGLE";"OG ADWORDS";"GB"

Sample 4

File Layout

Primary Account Number,Amount,Date,Merchant Category Code,POS entry,Acquirer BIN,Acquirer PCR,Card Acceptor ID,Card Acceptor Terminal ID,PIN Transaction ID,Card Acceptor Name,Card Acceptor City,Card Acceptor Country

File

4111111111111111,87.5,06057,4816,01,426696,4008,426696100008681,1954,N,GO MAN COM,BALTIMORE,US

4321432143214321,570.28,06068,5912,01,400088,9088,1420005995,05995TS0,N,WALRUS,MT WHISKEY,US

4222222222222222,50,06066,7399,02,469216,2840,924944000192138,,N,J2 COMMUNICATE,323 850 3214,US

4141414141414141,11.89,06057,4816,01,400088,9088,106171000991232,,N,YABO VOICE,0821230270,EU

4564564564564568,174.5,06063,5399,01,400088,9088,000324202994996,00110825,N,SOYLENT VENTURES,SUNNYTOWN,US

4987654321987654,1,06066,4814,01,461043,4401,67211400015P003,Q3B50F0Q,N,UNICYCLE INTERNET,866 844 1849,US

4846512378945678,60.16,06056,4900,90,461043,8402,67354430019P003,Q3AAF40Q,Y,AQUILA INC,800 378 3357,US

4123456789123456,5.33,06058,7311,01,400088,9088,22628782,24680137,N,GOGGLE CC GOGGLE,OG ADWORDS,GB

Sample 5

File Layout

Field Name, Field Length

Primary Account Number, 19

Transaction Amount, 25

Transaction Date, 25

Merchant Category Code, 4

POS Entry Mode, 2

Acquirer BIN, 6

Acquirer PCR, 4

Card Acceptor ID, 15

Card Acceptor Terminal ID, 8

PIN Transaction ID, 1

Card Acceptor Name, 25

Card Acceptor City, 15

Card Acceptor Country, 2

File

4111111111111111 87.5 06057 481601426696400842669610000868119 54 NGO MAN COM BALTIMORE US

4321432143214321 570.28 06068 591201400088908814200059950 5995TS0NWALRUS MT WHISKEY US

4222222222222222 50 06066 739902469216284092494400019213 8 NJ2 COMMUNICATE 323 850 3214 US

4141414141414141 11.89 06057 481601400088908810617100099123 2 NYABO VOICE 0821230270 EU

4564564564564568 174.5 06063 539901400088908800032420299499600110825NSOYLENT VENTURES SUNNYTOWN US

4987654321987654 1 06066 481401461043440167211400015P003Q3B50F0QNUNICYCLE INTERNET 866 844 1849 US

4846512378945678 60.16 06056 490090461043840267354430019P003Q3AAF40QYAQUILA INC 800 378 3357 US

4123456789123456 5.33 06058 731101400088908822628782 24680137NGOGGLE CC GOGGLE OG ADWOR

Appendix F: PIN Security Requirements

PCI PIN SECURITY REQUIREMENTS			
OBJECTIVE 1			
PINs used in transactions governed by these requirements are processed using equipment and methodologies to ensure that they are kept secure.			
1. All cardholder-entered PINs are processed in equipment that conforms to the requirements for Tamper-Resistant Security Modules (TRSMs). TRSMs are considered tamper responsive or physically secure devices (i.e., penetration of the device will cause immediate erasure of all PINs, secret and private cryptographic keys, and all useful residues of PINs and keys contained within it). All newly deployed ATMs and POS PIN acceptance devices are compliant with the applicable PCI PIN Entry Device and Encrypting PIN Pad Security Requirements.	**YES** ☐	**NO** ☐	**N/A** ☐
2a. All cardholder PINs processed online are encrypted and decrypted using an approved cryptographic technique that provides a level of security compliant with international and industry standards. Any cryptographic technique implemented meets or exceeds the cryptographic strength of TDEA using double length keys.	**YES** ☐	**NO** ☐	**N/A** ☐
2b. All cardholder PINs processed offline using IC Card technology must be protected in accordance with the requirements in Book 2 of the *EMV IC Card Specifications for Payment Systems* and ISO 9564.	**YES** ☐	**NO** ☐	**N/A** ☐
3. For online interchange transactions, PINs are only encrypted using ISO 9564–1 PIN block formats 0, 1 or 3. Format 2 must be used for PINs that are submitted from the IC card reader to the IC card.	**YES** ☐	**NO** ☐	**N/A** ☐
4. PINs are not stored except as part of a store-and-forward transaction, and only for the minimum time necessary. If a transaction is logged, the encrypted PIN block must be masked or deleted from the record before it is logged.	**YES** ☐	**NO** ☐	**N/A** ☐

OBJECTIVE 2

Cryptographic keys used for PIN encryption/decryption and related key management are created using processes to ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.

		YES	NO	N/A
5.	All keys and key components are generated using an approved random or pseudo-random process.	☐	☐	☐
6.	Compromise of the key-generation process is not possible without collusion between at least two trusted individuals.	☐	☐	☐
7.	Documented procedures exist and are demonstrably in use for all key-generation processing.	☐	☐	☐

OBJECTIVE 3

Keys are conveyed or transmitted in a secure manner.

		YES	NO	N/A
8.	Secret or private keys are transferred by: a. Physically forwarding the key as at least two separate key shares or full-length components (hard copy, smart card, TRSM) using different communication channels, **or** b. Transmitting the key in ciphertext form **Note:** Public keys must be conveyed in a manner that protects their integrity and authenticity.	☐	☐	☐
9.	Any single unencrypted key component is at all times during its transmission, conveyance, or movement between any two organizational entities: a. Under the continuous supervision of a person with authorized access to this component, **or** b. Locked in a security container (including tamper-evident packaging) in such a way that it can be obtained only by a person with authorized access to it, **or** c. In a physically secure TRSM	☐	☐	☐
10.	All key encryption keys used to transmit or convey other cryptographic keys are (at least) as strong as any key transmitted or conveyed.	☐	☐	☐
11.	Documented procedures exist and are demonstrably in use for all key transmission and conveyance processing.	☐	☐	☐

OBJECTIVE 4

Key loading to hosts and PIN entry devices is handled in a secure manner.

		YES	NO	N/A
12.	Unencrypted keys are entered into host Hardware Security Modules (HSMs) and PIN Entry Devices (PEDs) using the principles of dual control and split knowledge.	☐	☐	☐
13.	The mechanisms used to load keys (such as terminals, external PIN pads, key guns, or similar devices and methods) are protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component.	☐	☐	☐
14.	All hardware and passwords used for key loading are managed under dual control.	☐	☐	☐
15.	The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised.	☐	☐	☐
16.	Documented procedures exist and are demonstrably in use (including audit trails) for all key-loading activities.	☐	☐	☐

OBJECTIVE 5

Keys are used in a manner that prevents or detects their unauthorized usage.

		YES	NO	N/A
17.	Unique secret cryptographic keys must be in use for each identifiable link between host computer systems.	☐	☐	☐
18.	Procedures exist to prevent or detect the unauthorized substitution (i.e., unauthorized key replacement and key misuse) of one key for another or the operation of any cryptographic device without legitimate keys.	☐	☐	☐
19.	Cryptographic keys are only used for their sole intended purpose and are never shared between production and test systems.	☐	☐	☐
20.	All secret and private cryptographic keys ever present and used for any function (e.g., key-encipherment or PIN-encipherment) by a transaction-originating terminal (i.e., PED) that processes PINs must be unique (except by chance) to that device.	☐	☐	☐

OBJECTIVE 6

Keys are administered in a secure manner.

		YES	NO	N/A
21.	Keys used for enciphering PIN encryption keys (or for PIN encryption) must never exist outside of TRSMs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.	☐	☐	☐
22.	Procedures exist and are demonstrably in use to replace any known or suspected compromised key and its subsidiary keys (those keys enciphered with the compromised key) to a value not feasibly related to the original key.	☐	☐	☐
23.	Key variants are only used in devices that possess the original key. Key variants are not used at different levels of the key hierarchy (e.g., a variant of a key encipherment key used for key exchange cannot be used as a working key or as a master file key for local storage).	☐	☐	☐
24.	Secret and private keys and key components that are no longer used or have been replaced are securely destroyed.	☐	☐	☐
25.	Access to secret and private cryptographic keys and key materials must be limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use.	☐	☐	☐
26.	Logs are kept for any time that keys, key components, or related materials are removed from storage or loaded to a TRSM.	☐	☐	☐
27.	Backups of secret and private keys must exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups must exist only in one of the allowed storage forms for that key.	☐	☐	☐
28.	Documented procedures exist and are demonstrably in use for all key administration operations.	☐	☐	☐

OBJECTIVE 7

Equipment used to process PINs and keys is managed in a secure manner.

		YES	NO	N/A
29.	PIN-processing equipment (PEDs and HSMs) is placed into service only if there is assurance that the equipment has not been substituted or made subject to unauthorized modifications or tampering prior to the loading of cryptographic keys.	☐	☐	☐
30.	Procedures exist that ensure the destruction of all cryptographic keys and any PINs or other PIN-related information within any cryptographic devices removed from service.	☐	☐	☐
31.	Any TRSM that is capable of encrypting a key and producing cryptograms of that key is protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of either or both of the following: a. Dual access controls are required to enable the key encryption function. b. Physical protection of the equipment (e.g., locked access to it) under dual control.	☐	☐	☐
32.	Documented procedures exist and are demonstrably in use to ensure the security and integrity of PIN-processing equipment (e.g., PEDs and HSMs) placed into service, initialized, deployed, used, and decommissioned.	☐	☐	☐

Appendix G: 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*

- Qualified CISP Incident Response Assessor (QIRA) List – List of forensic companies qualified to perform a PCI forensic investigation on compromised entities.
- Qualified PCI 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, merchants, 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 a PCI QSA in verifying that an entity is in compliance with the PCI DSS.
- 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).*

Appendix H: 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.
Acquirer	Financial institution that enters into agreements with merchants to accept Visa cards as payment for goods and services. Commonly referred to as the "merchant bank".
Agent	Any contractor, including third-party processors and servicers, whether a client or non-client, engaged by a client to provide services or act on its behalf in connection with Visa payment services.
At Risk Accounts	Refers to accounts that were included in a CAMS "Alert" of a suspected or confirmed compromised event.
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 Not Present	A merchant, market, or sales environment where transactions occur without a valid Visa card being present. "Card not present" is used to refer to mail order/telephone order merchants and sales environments, as well as the Internet.
Card Present	A merchant, market, or sales environment in which a transaction can be completed only if both a valid Visa card and the cardholder are present and the sale is processed by an individual representing the merchant or the acquirer. Card present transactions include face-to-face retail sales and cash disbursements.

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 fraud scheme of similar character. The "common point of purchase" is assumed to be the point of compromise.
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 (e.g., account number, expiration date, data provided by the client, other electronic data gathered by the merchant/agent). This term also applies to other personal insights gathered about the cardholder such as address, telephone number, etc.
Client	An organization that is a member of Visa and issues cards and/or signs merchants.
Compromise	Process that exposes cardholder account information to third parties, placing cardholders at risk of fraudulent use.
Compromised Account	Accounts downloaded by an intruder or found in criminal possession.
Compromised Account Management System (CAMS)	Via CAMS, acquirers, merchants and law enforcement officers can safely upload compromised and stolen/recovered accounts directly to Visa. As this information is received by CAMS, e-mail alert messages are automatically sent to registered issuer users to notify them of the compromised and stolen/recovered accounts.
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.
Entity	An organization that stores, processes or transmits account information. Typically the victim in a compromise. Also refers to any payment industry organization that must be PCI DSS compliant.
Encryption	An online data security method that scrambles data so that it is difficult to interpret without a corresponding decryption key.
Event	Refers to a single 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	Refers to each single occurrence of known or suspected data compromise. It is used interchangeably with the term "event".
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 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.
Member	An organization that is a member of Visa and issues Visa cards and/or acquires merchant transactions.
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. These requirements apply to all members, merchants, and service providers that store, process, or transmit cardholder data.
Payment Card Industry (PCI) PIN Security Requirements	A comprehensive set of measures 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/*.
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 where account number data was obtained by unauthorized third parties.
Qualified CISP Incident Response Assessor (QIRA)	Visa-approved security vendors who perform forensic investigations in the event of a security incident. A list of QIRAs can be obtained at *www.visa.com/cisp*.

Qualified Data Security Company (QDSC)	A security company qualified by the PCI SSC to perform a PCI Data Security Assessment according to the PCI Security Audit Procedures. Please visit the PCI Security Standards Council website (*www.pcisecuritystandards.org*) for details on the PCI program requirements.
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*.
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.

Appendix I: Investigation Definitions

TERMINOLOGY	DESCRIPTION
Date(s) that data was transferred out of the network	The confirmed date(s) that data was transferred out of the network by the intruder or malware.
Date and Version of POS Installation (s)	Date(s) of when the entity began using the POS application and version number. If available, include date(s) of when entity installed a patch or an upgrade to no longer retain prohibited data.
Malware Installation Date(s)	The date(s) that malware was installed on the system, if applicable.
Date(s) of Real-Time Capture	Date(s) of when malicious code/malware, such as packet sniffer and/or key logger, was activated to capture payment card data on the network and system. Should also include date(s) of when malware was de-activated.
Window of Intrusion	First confirmed date that intruder or malware entered the system to the date of containment. Examples of containment include, but not limited to: ▪ Removal of malware or rebuilt of compromised systems ▪ Compromised system removed from the network ▪ Blocking of malicious IPs on the firewall ▪ Rotation of compromised passwords
Window of Storage	"Window of Storage" is defined as the frame of time in which a given set of prohibited data is initially placed on a system to the time that same data was removed. It answers the question, "how long was the given set of data stored?"
Transaction date(s) of stored accounts	Transaction date(s) is defined as the date of the transactions stored on the system.
Window of System Vulnerability	"Window of Vulnerability" is defined as the frame of time in which a weakness in an operating system, application or network could be exploited by a threat to the time that weakness is properly remediated. It answers the question, "how long was the system at risk to a given compromise?" Overall time period that a system was vulnerable to attack due to system weaknesses. For example, lack of/or poorly configured firewall, missing security patches, insecure remote access configuration, default passwords to POS systems, insecure wireless configuration.

Appendix J: Secret Service Electronic Crimes Task Force (ECTF)

New England Electronic Crimes Task Force
(617) 565-6640

Metro-Charlotte Electronic/Financial Crimes Task Force
(704) 442-8370

Chicago Electronic Crimes Task Force (CECTF)
(312) 353-5431

Cleveland Electronic Crimes Task Force
(216) 706-4365

Dallas N-Tec Electronic Crimes Task Force
(972) 868-3200

Houston HITEC Electronic Crimes Task Force
(713) 868-2299

Las Vegas Electronic Crimes Task Force
(702) 388-6571

Los Angeles Electronic Crimes Task Force
(213) 533-4650

Miami Electronic Crimes Task Force
(305) 863-5000

New York Electronic Crimes Task Force
(718) 625-7135

San Francisco Bay Area Electronic Crimes Task Force
(415) 744-9026

South Carolina Electronic Crimes Task Force
(803) 772-4015

Washington -Metro Electronic Crimes Task Force
(202) 406-8000

For Further Information:

www.ectaskforce.org or
www.secretservice.gov

(305) 863-5000

Appendix K: Federal Bureau of Investigations (FBI)

Infragard at *www.infragard.net*

FBI at *www.fbi.gov*