Payment Card Acceptance Procedures

Incident Response Plan and The Specific Steps to Take if Cards or Cardholder Environment is Compromised

September 2016

Contents

Summary

Protecting the payment card system is a shared responsibility. At a minimum, all parties involved in the handling of payment card data, as well as those that provide services that can impact payment card data, must maintain compliance with Payment Card Industry Data Security Standard (PCI DSS) requirements. Merchants that suspect or have confirmed a security breach or an account data compromise must take prompt action to prevent additional exposure of payment card data and ensure proper PCI DSS and PCI PIN security controls are in place and functioning correctly. Security breaches are not limited to network intrusions and the procedures and timelines also apply to compromises involving Point of Sale (POS), PIN Entry Device (PED) tampering or "skimming".

Adherence to the procedures contained in this document will ensure compliance with Visa's Cardholder Information Security and MasterCard Site Date Protection Programs.

This document contains required procedures and timelines for reporting and responding to a suspected or confirmed account data compromise.

Overview

This incident response plan assembles and organizes the resources for dealing with events that may harm or threaten the security of information assets. Such an event may be a malicious code attack, an unauthorized access to information or systems, the unauthorized use of services or information, a denial of service attack, or a hoax. The goal is to facilitate quick and efficient incident response and to limit the impact while protecting state or client information. The plan should define roles and responsibilities, documents the steps necessary for effectively and efficiently manage an information security incident, and define communication channels. The plan also describes the training needed to achieve these objectives.

Purpose

The purpose of an information security incident response plan is to ensure the effective response and handling of security incidents that affect the availability, integrity and confidentiality of agency information. In addition, an incident response program will ensure information security events, incidents and vulnerabilities associated with information and information systems are communicated in a manner enabling timely corrective action.

Incident Identification

Identification of an incident is the process of analyzing an event and determining if that event is normal or deleterious. An incident is an adverse event and it usually implies either harm, or the attempt to harm the Agency or its clients. Events occur routinely and will be examined for impact. Those showing either harm or intent to harm may be escalated to an incident.

The term incident refers to an adverse event impacting one or more Agency's information assets or to the threat of such an event. Examples include but are not limited to the following:

- Unauthorized use
- Denial of Service
- Malicious code
- Network system failures (widespread)
- Application system failures (widespread)
- Unauthorized disclosure or loss of information
- Information Security Breach

Incidents can result from any of the following:

- Intentional and unintentional acts
- Actions of employees
- Actions of vendors or constituents
- Actions of third parties
- External or internal acts
- Credit card fraud
- Potential violations of Policies
- Natural disasters and power failures
- Acts related to violence, warfare or terrorism
- Serious wrongdoing

Remediation Plan

Based on a thorough understanding of vulnerability(s) a remediation plan addresses those vulnerability(s)to prevent a reoccurrence of the incident. The goal is to prepare for the resumption of normal operations with confidence that the initial problem has been fixed. The remediation of the threat/vulnerability should be developed via a team effort to include the person investigation the incident, system/network admin, application developer, subject matter experts (SME), data owners, and representatives of the ancillary functions. Changes to the system to insure the incident is not repeated should be documented in the service request system and the change(s) will be developed, tested, and implemented following the established change management process.

The timing of the remediation should be either:

- Immediate Action – This approach should be implemented when it is considered more important to immediately stop the attacker's activities than to continue the investigation.
- Delayed Action – This approach allows the investigation to conclude before any direct actions are taken against the attacker.
- Combined Action – This approach implements containment on only a specific aspect of the incident while letting the rest of the incident continue.

Threat/Vulnerability Eradication

After an incident, efforts will focus on identifying, removing and repairing the vulnerability that led to the incident and thoroughly clean the system. The goals are:

- Remove the attacker's ability to access the environment
- Deny the attacker access to compromised systems, accounts, and data
- Remove the attack vector the attacker used to gain access to the environment
- Restore the Agency's and other's trust in its computer systems and user accounts

The following actions may be taken based on the incident:

- Disconnecting the infected area from the internet during eradication
- Blocking malicious IP addresses
- Blackholing domain names
- Changing user account passwords
- Implementing or altering network segmentation
- Rebuilding the compromised system(s) is best instead of cleaning the system by removing the malware/virus.

The timing of the eradication event is critical to a successful remediation. The indicators to consider if the timing is correct are:

- The investigator believes that they have a good visibility into the breached environment and they understood the attackers Tactics, Techniques, and Procedures (TTPs).
- The number of compromised systems discovered per time period has decreased significantly.
- Most of the compromised systems detected contain known indicators of compromised
- The remediation effort has been thoroughly planned.

Communication is critical during the eradication process. Communications among the investigator and system administrators is required to verify and validation the eradication plan is being implemented in the correct order and there are no issues requiring the plan to be backed out. Communication with data owners, users,

and management is required to inform them of system outages to apply the eradication, the progress being made, and the completion of the eradication. The eradication plan includes providing the helpdesk information about the indicators of the compromised and to notify the investigator if users are reporting these indicators over the next several days.

Confirm Threat/Vulnerability has been eliminated

After the cause of an incident has been remediated and data or related information restored, it is critical to confirm all threats and vulnerabilities have been successfully mitigated and that new threats or vulnerabilities have not been introduced. This is accomplished by looking for indicators of compromised via the methods used in the investigation. Often, the verification process will identify a small number of systems which were accidently overlooked, improperly rebuilt, or not rebuilt at all. Trace evidence of the malware/virus may reside in the system's registry or configuration files. These areas should be scanned to verify the system is clean. Finally, if applicable, verify account (users and admins) passwords have been changed or have been set to be changed via Active Directory or LDAP.

Resumption of Operations

Resuming operations and closing the incident is a business decision, but it is important to conduct the preceding steps to ensure it is safe to resume operations.

- Complete the documentation of the incident.
- Validate the vulnerability has been remediated or is being addressed in a scheduled release.
- Verify and validate vulnerability has been removed from all systems.
- Validate the vulnerability has been be detected for a period of time. The period of time is based on the critically of the systems and data.

Post-incident Activities

A post event analysis will be performed for all incidents. The analysis may consist of one or more meetings and include production of an event report. The purpose of the analysis is to give participants an opportunity to share and document details about the incident and to facilitate lessons learned. The meeting should be held within one week of closing the incident.

Education and Awareness

The Agency shall ensure that incident response is addressed in education and awareness programs. The programs shall include:

- Educating personnel in their incident response roles and responsibilities and providing annual refresher training
- Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations
- Provide user training to recognize potential incidents and how to report it

Required Steps for Potentially Compromised Entities

Agencies that have experienced a suspected or confirmed Payment Card security breach must take prompt action to help prevent additional damage and adhere to the requirements listed below:

Preserve Evidence and Limit Additional Exposure

To identify the underlying cause and facilitate investigations, it is important to ensure the integrity of the system components and environment by preserving all evidence.

- Do not access or alter compromised system(s) (e.g., do not log on to the compromised system(s) and change passwords; do not log in with administrative credentials or as ROOT). Compromised system(s) should be taken offline immediately and not be used to process payments or interface with payment processing systems.
- Do not turn off, restart, or reboot the compromised system(s). Instead, isolate the compromised systems(s) from the rest of the network by unplugging network cable(s) or through other means.
- Identify and document all suspected compromised components (e.g. PCs, servers, terminals, logs, security events, databases, Pin Entry Device overlay's etc.).
- Document containment and remediation actions taken, including dates/times (preferably in Coordinated Universal Time - UTC), individuals involved, and detailed actions performed.
- Preserve all evidence and logs (e.g. original evidence such as forensic image of systems and malware, security events, web logs, database logs, firewall logs, etc.).
- If using a wireless network, change SSID on the AP and other machines that may be using this connection with the exception of any systems believed to be compromised.

Execute Notification Plan

Immediately notify all relevant parties, including:

- Internal incident response team and information security group
- The NM Enterprise Payment Card Industry-DSS Steering Committee (PCISC) (505) 827-3682
- Merchant service bank (also known as your acquirer or acquiring bank)
  - If you do not know the name and/or contact information for your merchant bank or the PCISC for assistance:
  - If Wells Fargo is your merchant service provider Contact Wells Fargo "Association Compliance"
    - Monica Bourgeois
    - Wells Fargo Merchant Solutions
    - 1200 Montego Way
    - Walnut Creek, Ca. 94598
    - bourgeml@wellsfargo.com
    - (925)746-3761
  - Also Contact Wells Fargo Merchant Relationship Manager - Patty.White@wellsfargo.com (Cell 720-284-2843 | eFax 866-609-4838)

- Manufacturer of the impacted payment device if you have determined that the incident involves the compromise of a PIN Entry Device (PED), specifically if it is a PCI PTS-approved device.
- Legal department to determine if laws mandating customer notification are applicable.

It is strongly recommended that you also immediately notify:

- The appropriate law enforcement agency in the event of an account data compromise.
- Federal law enforcement if the compromise is in the United States. The United States Secret Service Electronic Crimes Task Forces (ECTF) focuses on investigating financial crimes and can assist with incident response and mitigation of an account data compromise.

  Visit www.secretservice.gov/investigation for ECTF field office contact information.

Be Prepared to Perform Forensic Investigation

Agency may be required to engage a Payment Card Industry Forensic Investigator (PFI) to perform an independent forensic investigation. If advised that a forensic investigation is required, the following timeline must be followed.

Upon discovery of an account data compromise, or receipt of an independent forensic investigation notification, an entity must:

- Engage a PFI (or sign a contract) within five (5) business days
- Provide requesting entity with the initial forensic (i.e. preliminary) report within ten (10) business days from when the PFI is engaged (or the contract is signed)
- Provide requesting entity with a final forensic report within ten (10) business days of completion of the review

The PFI cannot be an organization that is affiliated with the compromised entity or has provided services to the compromised entity such as previous PFI investigation, Qualified Security Assessor (QSA), advisor, consultant, monitoring or network security support, etc.

Forensic reports from non-approved PFI forensic organizations will not be accepted. PFIs are required to provide forensic reports and investigative findings directly to requesting entity.

A list of approved PFI organizations is available at:
www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators

If Wells Fargo is your Merchant Services provider they offered the following suggestions.

Trustwave	**Verizon**	**Security Metrics**
Colin Sheppard (North America) csheppard@trustwave.com 1 -312- 873- 7474	Chris Novak (N. Amer & Lat. Amer.) Chris.Novak@verizonbusiness.com 1-914-574-2805	Sherry Ferguson (USA) PFI@securitymetrics.com 1 -(801-705-5621

Document the Incident

Document the incident by collecting information about the incident and keeping a record of the incident until it closed. The document should include the following information.

Incident Summary Checklist

- Date and time of the incident was reported as being an incident
- Date and time the incident was detected
- Contact information of the person reporting the incident
- Contact information of the person documenting the information
- The nature of the incident. For example:
    - Mass Malware
    - Spear Phising Attempt
    - Virus
    - Unauthorized Access
- How the incident was detected
- Number of people impacted and who they are in summary
- Functions impacted
- Critically of the system(s) and its impact to business operations
- Who has been notified of the incident and when
- Has anything related to the data sources changed recently

System Details

- Individual System Details (repeat as necessary):
    - Physical Location
    - Unique name (e.g. computer name, host name)
    - System's make and model
    - Operating System installed
    - Primary function of the system
    - Responsible system admin or user
    - Assigned IP Address
    - Critical information stored on the system
    - Whether backups exist for the system
    - Malware/Virus Details – For each malicious file:
        - Name of malware/virus
        - Date and time of detection
        - How it was detected
        - Name of the file and directory
        - Detection Mechanism
        - If copy of the file is preserved
        - Status of any analysis
        - Whether the malware was submitted to a third party or other state Department
    - Remediation steps that have been taken
    - If any data is being preserved, what process is being used and where it is being stored

Attack Timeline

Using the information collected, build an Attack Timeline of events. The timeline will keep the incident organized, provide context help identify inconsistencies, and provide an overall picture of what happen. The following is an example of an Attack Timeline:

Date Added	Event Time	Host	Event Description	Data Source
2015-08-22	2015-08-21 16:32:23	Host1234	Infected email attachment by the user "bsmith"	File system, recent document list
2015-08-22	2015-08-21 16:32:39	Host1234	C:\windows\PreFetch\malware.exe created	File system, metadata

Evidence Preservation

Carefully balancing the need to restore operations against the need to preserve evidence is a critical part of incident response. Gathering evidence and preserving it are essential for proper identification of an incident, and for business recovery. Follow-up activities, such as personnel actions or criminal prosecution, also rely on gathering and preserving evidence. If applicable, compromised data and information will be stored on an external drive and not be connected to the Internet nor the Department's network.

Provide All Exposed Accounts

All compromised accounts (known or suspected) must be identified and communicated to card entities, typically within five (5) business days from the first to occur of the following events: (a) the date card company requests account numbers, (b) a Window of Exposure (WOE) is determined, or (c) discovery of compromised account data is identified.

- Entities should work with their acquiring bank to upload impacted accounts
- If Wells Forgo is your Merchant Service provider the compromised accounts numbers must be sent to Wells Fargo's Association Compliance Group (see contact above).
- NOTE: communication of this data must be via an encrypted .txt file that contains all potentially compromised accounts

Provide Initial Incident Report

Within four (4) business days of a suspected or confirmed account data compromise, provide the a Initial Incident Report—beginning on page 5—to the acquiring bank, Enterprise Payment Card Industry Steering Committee (PCISC), State Board of Finance and possibly credit card company

Initial Incident Report

Upon notification of a suspected or confirmed account data compromise, compromised entities must initiate a preliminary investigation of all potentially impacted systems and those of any third-party service providers. Compromised entities must share the findings with their acquiring bank, if applicable. A preliminary incident report is not the same as a PFI preliminary report. The initial investigation will assist all entities in understanding the compromised entity's network environment and potential scope of the incident.

To comply with investigation requirements, the entity must submit securely (e.g., encryption, PGP encryption, Secure Email, etc.) the following information within four (4) business days of a suspected or confirmed account data compromise:

Incident Report	
Date of Report:	
Contact Name and Phone #	
Name of entity:	
Type of entity:	
Description of the incident	
Name of Acquirer and (Interbank Card Association) Bank Identification Number (s): (List all that are applicable.)	
Does the entity send transactions to a payment processor?	■ Yes ■ No *(If yes, attach a list of processor(s) and provide name and contact information. If reporting entity is a Processor, please provide a list of all Acquirer BINs and all Merchant Names, Merchant Card Acceptor IDs, City*
Entity PCI DSS Level *(e.g. Level 1-4):*	
Entity PCI DSS Compliance Status:	*(If compliant, please attach proof of PCI DSS compliance documentation.)*
Approximate number of transactions processed per year	• POS PIN/Debit • Credit
Is merchant entity corporate-owned or an individual franchise?	*(If merchant has other locations, please attach a list.)*
Name of payment application(s) and version(s):	• • • •

<table>
<tr><td rowspan="4">Identify responsible party(s) for the configuration and support of the Point of Sale (POS) solution
(e.g. Integrator, Reseller, or Agent).</td><td>NAME</td><td>TITLE</td><td>CONTACT</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td colspan="3">(If entity is an Integrator or Reseller, please attach a list all Acquirer BINs and all Merchant Names, Merchant Card Acceptor IDs, City and State.)</td></tr>
<tr><td>Is this a corporate or franchise mandated payment application and version?</td><td colspan="3"></td></tr>
<tr><td>Is the terminal PC-based or is it connected to a PC-based environment?</td><td colspan="3"></td></tr>
<tr><td>Is there remote access connectivity to the entity's environment?</td><td colspan="3">■ Yes ■ No
If yes, which organizations have remote access?
•
•
•</td></tr>
<tr><td>What type of remote access solution is used?</td><td colspan="3"></td></tr>
<tr><td>Is remote access always on or is it enabled upon request?</td><td colspan="3"></td></tr>
<tr><td>Is the Point of Sale device EMV enabled?</td><td colspan="3">■ Yes ■ No
If yes, provide name and model number.</td></tr>
<tr><td>Is the POS solution enabled with point-to-point encryption?</td><td colspan="3">■ Yes ■ No
If yes, provide details.</td></tr>
<tr><td>Does the entity accept PIN?</td><td colspan="3">■ Yes ■ No</td></tr>
<tr><td>Is the entity's PIN entry device (PED), PCI PTS approved and listed on the PCI SSC website?</td><td colspan="3">■ Yes ■ No
Provide the PED model, hardware, firmware and application and version numbers. Visit www.pcisecuritystandards.org/pin for the list of PCI-approved PIN entry devices.</td></tr>
</table>

Is the entity co-located or hosted?	If hosted, provide name and contact information of the hosting provider.
Provide the shopping cart application and version information, if applicable.	
Describe any recent changes to the network and/or systems.	• Payment application upgrades ☐ Yes ☐ No • Installation of a firewall ☐ Yes ☐ No • Installation of an anti-virus program ☐ Yes ☐ No • Changes to remote access authentication ☐ Yes ☐ No OTHER: • • •
Has the entity received complaints regarding fraudulent transactions from their customers?	☐ Yes ☐ No Is yes, please describe.
Has entity been contacted by law enforcement regarding fraudulent transactions?	☐ Yes ☐ No If yes, list date(s) and by which law enforcement agency. • • •
If Account Data Compromise is Confirmed Provide the Following	
How and when was the incident identified?	
How did the compromise take place?	Attach documentation of the following, if known: • List of vulnerabilities that caused or contributed to the compromise • Sample of any phishing emails • Details of unauthorized activity • List of malicious IPs • Malware information, if applicable

Did entity notify law enforcement?	■ Yes ■ No If yes, which agency and when were they notified? Provide contact information if applicable.
If known, how many cards were compromised (accounts made vulnerable as a result of a data security breach)?	Stratify by Brand (Visa, Master Card, etc.)
Have the impacted accounts been uploaded to CAMS?	
What data elements were compromised and/or exposed?	■ Primary Account Number (PAN) ■ Expiration Date ■ Full Track 1 and/or 2 ■ PIN ■ CVV2 Cardholder personally-identifiable information (PII) ■ Cardholder Name ■ Social Security Number ■ Date of Birth ■ Other:
Has the compromise been contained? If yes, how?	■ Yes ■ No If yes, how?
Steps taken to remediate the risk/vulnerabilities?	
Was entity storing	Track 1 or track 2 data? CVV, CVC 2 data?
How long is the data stored on the system?	
Additional information on the investigation and the remediation of your systems you feel necessary	

Remediation Plan

A remediation plan requires vulnerability(s) to be clearly identified so the incident isn't repeated. The goal is to prepare for the resumption of normal operations with confidence that the initial problem has been fixed. The remediation of the threat/vulnerability should be developed via a team effort to include the person investigation the incident, system/network admin, application developer, subject matter experts (SME), data owners, and representatives of the ancillary functions. Changes to the system to insure the incident is not repeated should be documented in the service request system and the change(s) will be developed, tested, and implemented following the established change management process.

The timing of the remediation should be either:

- **Immediate Action** – This approach should be implemented when it is considered more important to immediately stop the attacker's activities than to continue the investigation.
- **Delayed Action** – This approach allows the investigation to conclude before any direct actions are taken against the attacker.
- **Combined Action** – This approach implements containment on only a specific aspect of the incident while letting the rest of the incident continue.

Threat/Vulnerability Eradication

After an incident, efforts will focus on identifying, removing and repairing the vulnerability that led to the incident and thoroughly clean the system. The goals are:

- Remove the attacker's ability to access the environment
- Deny the attacker access to compromised systems, accounts, and data
- Remove the attack vector the attacker used to gain access to the environment
- Restore the Department and other's trust in its computer systems and user accounts

The following actions may be taken based on the incident:

- Disconnecting the infected area from the internet during eradication
- Blocking malicious IP addresses
- Blackholing domain names
- Changing user account passwords
- Implementing or altering network segmentation
- Rebuilding the compromised system(s) is best instead of cleaning the system by removing the malware/virus.

The timing of the eradication event is critical to a successful remediation. The indicators to consider if the timing is correct are:

- The investigator believes that they have a good visibility into the breached environment and they understood the attackers Tactics, Techniques, and Procedures (TTPs).
- The number of compromised systems discovered per time period has decreased significantly.
- Most of the compromised systems detected contain known indicators of compromised
- The remediation effort has been thoroughly planned.

Communication is critical throughout the eradication process. Communications among the investigator and system administrators is required to verify and validation the eradication plan is being implemented in the correct order and there are no issues requiring the plan to be backed out. Communication with data owners,

users, and management is required to inform them of system outages to apply the eradication, the progress being made, and the completion of the eradication. The eradication plan includes providing the helpdesk information about the indicators of the compromised and to notify the investigator if users are reporting these indicators over the next several days.

Confirm that Threat/Vulnerability has been eliminated

After the cause of an incident has been removed or eradicated and data or related information is restored, it is critical to confirm all threats and vulnerabilities have been successfully mitigated and that new threats or vulnerabilities have not been introduced. This is accomplished by looking for indicators of compromised via the methods used in the investigation. Often, the verification process will identify a small number of systems which were accidently overlooked, improperly rebuilt, or not rebuilt at all. Trace evidence of the malware/virus may reside in the system's registry or configuration files. These areas should be scanned to verify the system is clean. Finally, if applicable, verify account (users and admins) passwords have been changed or have been set to be changed via Active Directory or LDAP.

Resumption of Operations

Resuming operations and closing the incident is a business decision, but it is important to conduct the preceding steps to ensure it is safe to do so and there is an agreement to resume operations.

- Complete the documentation of the incident.
- Validate the vulnerability has been remediated or is being addressed in a scheduled release.
- Verify and validate vulnerability has been removed from all systems.
- Validate the vulnerability has been be detected for a period of time. The period of time is based on the critically of the systems and data.

Post-incident Activities

An after-action analysis will be performed for all incidents. The analysis may consist of one or more meetings and/or reports. The purpose of the analysis is to give participants an opportunity to share and document details about the incident and to facilitate lessons learned. The meeting should be held within one week of closing the incident.

Education and Awareness

The Agency shall ensure that incident response is addressed in education and awareness programs. The programs shall address:

- Train incident personnel in their incident response roles and responsibilities as well as providing annual refresher training
- Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations
- Provide user training to recognize potential incidents and how to report it