Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

# PCI DSS and Incident Handling: What is required before, during and after an incident

There is no perfect security; PCI DSS certified companies should be prepared to handle security incidents.

Copyright SANS Institute
Author Retains Full Rights

AD

# PCI DSS and Incident Handling

## What is required before, during and after an Incident

GCIH Gold Certification

Author: Christian J. Moldes

Christian_moldes@hotmail.com

Adviser: Dominicus Adriyanto

Accepted: February 27, 2009

© SANS Institute 2009, Author retains full rights.

## Outline

**Abstract** ..... 3

**1. Introduction** ..... 4

**2. PCI Security Standards Council and PCI DSS** ..... 5

**2.1. Is PCI DSS enough to avoid being breached?** ..... 5

**3. Incident Handling Phases** ..... 7

**4. Preparation Phase** ..... 7

**4.1. Required Documentation** ..... 8

**4.2 Processes that Should Be in Place** ..... 16

**5. Identification and Containment Phases** ..... 18

**5.1. Common Attack Vectors** ..... 20

**6. Eradication and Recovery phases** ..... 21

**6.1. Reporting the Incident** ..... 21

**6.2. Forensic Investigations and Audits** ..... 21

**6.3. Failing to Report an Incident** ..... 23

**7. Lessons Learned Phase** ..... 23

**7.1. General Recommendations** ..... 24

**8. The Cost of a Security Breach** ..... 25

**9. Additional Payment Card Brands Consequences** ..... 26

**10. How the Payment Card Companies Determine Liability** ..... 27

**Appendix A: Requirements Matrix** ..... 29

**Appendix B: Payment Card References** ..... 31

**Acknowledgments** ..... 32



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

**References** ..... 33

© SANS Institute 2009, Author retains full rights.



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

## Abstract

PCI DSS requires companies to comply with a set of specific requirements whenever they process, transmit or store payment card transactions. Every year companies have to demonstrate compliance, and renew their certification; however, many of them are still suffering security breaches. Regardless their status, all those companies should be prepared to deal with a cardholder data breach. PCI DSS does not provide specific guidelines on how to handle a security breach. Each payment card brand has its own policies and procedures; and in some cases, they are different between them. A compromised organization that does not follow the payment brands' procedures or does not meet the reporting deadlines, may expose itself to hefty fines and the risk of losing the authorization to process payment card transactions.

This paper intends to be a guideline for chief security officers, compliance directors, IT auditors, and anyone responsible for PCI DSS compliance.



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

## 1. Introduction

According to the San Diego-based Identity Theft Resource Center (2009), the number of confirmed data breaches in 2008 increased by 47% from the total reported in 2007. Among them, several have something in common: payment card data was compromised.

During the last two years, several renowned companies hit the news reporting security breaches. Some of them include TJX Cos., Marshalls, BJ's Wholesale, Club Inc., Barnes & Noble Inc. bookstores, Sports Authority, Boston Market Corp., OfficeMax Inc., Dave & Buster's restaurants, DSW Inc. Shoe Stores, Hannaford Bros Co., Heartland Payment Systems Inc., and many others.

In 2001, several of the payment card companies instituted security compliance programs that merchants and service provider were required to comply.

Visa instituted CISP (Cardholder Information Security Program) and MasterCard created SDP (Site Data Protection). Complying with several different programs was a heavy burden to merchants and service providers. Hence, in 2004, CISP requirements were incorporated into a new industry standard know as Payment Card Industry (PCI) Data Security Standard (DSS) resulting from a cooperative effort between Visa and MasterCard to create common industry security requirements (Visa, 2009).

In 2006, the PCI Security Standards Council was formed as an entity responsible for the development, management, education, and awareness of PCI DSS and other related standards.



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

## 2. PCI Security Standards Council and PCI DSS

PCI Security Standards Council was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. Companies accepting payment card transactions from any of these payment brands have to comply with PCI DSS requirements. Non-compliant companies are exposed to higher transaction fees imposed by their acquirer banks, fines imposed by the payment brands, higher liability if a breach occurs, and even to the risk of losing the authorization to process payment card transactions.

PCI DSS requires documentation to be developed and maintained, preventive and detective security controls to be implemented, and processes to be in place in order to identify and contain any security breach attempts as soon as possible. PCI DSS and its supporting documents are available for download at PCI Security Standards Council website.

### 2.1. Is PCI DSS enough to avoid being breached?

The short answer is no. There is a huge difference between compliance and security, and certified companies do not have to fall into a false sense of security. PCI DSS certification does not guarantee companies that a breach is not going occur. Several factors may contribute to the standard not being a security “silver bullet”:

- First, there is not such a thing as perfect security. A company can only protect itself from known vulnerabilities and attack vectors. Newer attack vectors may not be covered by existent security controls.



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

- PCI DSS demands only a minimum set of requirements and one size does not fit all. Companies are complex entities and the security controls that may be sufficient for an average company may not be what a large or highly specialized company needs.

- Certification is based on the Qualified Security Assessor's opinion, and his judgment would obviously be based on his knowledge and experience. Inexpert assessors may be unable to conduct a thorough review, leading to an insecure infrastructure being certified as compliant.

- Assessments are snapshots in time. Certified companies may make mistakes over time, which may affect their security posture and create opportunities for a security incident.

Hannaford Bros Co. and Heartland Payment Services Inc., companies considered PCI DSS compliant, disclosed in 2008 and 2009 respectively that they suffered security breaches that exposed cardholder data. This and many other cases demonstrate that obtaining the certification may not be sufficient to avoid a security incident.

Preparation for an incident is critical, especially because the Payment Card brands have different security compliance programs and hence different approaches to deal with a security breach.

Lack of preparation may result in additional fines by the payment card brands, additional costs in engaging forensic services, and even the risk of losing the authorization to process payment card transactions indefinitely.



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

In order to minimize these risks, companies should carefully implement an incident handling process even if they are PCI DSS compliant.

## 3. Incident Handling Phases

There are six basic steps in incident handling: preparation, identification, containment, eradication, recovery, and lessons learned (SANS Institute, 2008, p.13). In general, PCI DSS does not provide any guidelines regarding incident handling, however, some requirement may apply to the preparation, identification, and lesson learned phases.

Some Payment Card Brands have very specific requirements for the containment, eradication, and recovery phases.

## 4. Preparation Phase

The goal of the preparation phase is to get the company's team and resources ready to handle a security incident, and per PCI DSS, a security breach that may affect cardholder data.

Most of the time, people consider PCI DSS as a compliance standard only focused on preventing security breaches. However, many of its requirements establish a foundation for an effective incident handling and forensic investigation process. From identification through lessons learned, PCI DSS includes controls related with many of the incident handling phases.

Properly implemented, PCI DSS compliance should provide all the necessary detective controls in order to identify and contain a



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

security breach.

## 4.1. Required Documentation

Part of the preparation consists of developing and maintaining proper documentation. The following documents are very important during an incident:

a) Cardholder data assets inventory

Your company should have an inventory of all the assets related with cardholder data. According to Verizon Business RISK Team, 38% of the breaches in 2009 include a system storing data that the organization did not know existed on that system (Verizon Business Risk Team, 2009). The same study also highlights that the breaches included a system that had unknown connections (24%) or unknown accounts or privileges (17%).

The inventory is not a requirement; however, it will not only help defining your cardholder data scope, but will also help identifying the locations where cardholder data should be protected, whether in transit or at rest. Include the following information in your inventory report:

- Cardholder data location
- Cardholder data components (cardholder name, card number, expiration date, other sensitive data)
- Data format (clear text, encrypted, masked, truncated)



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

- Data retention
- Security controls in place to protect the data
- Authorized accounts

b) Network diagrams with all connection to cardholder data

Diagrams are critical during an incident. They provide a quick and clear picture of the cardholder environment to incident handlers, forensic investigators, and law enforcement.

Diagrams should be up-to-date, complete, and accurate, otherwise they can potentially slow incident handling or even jeopardize the identification, containment, and eradication phases.

Additionally, dataflow diagrams should depict all the databases and files containing cardholder data, the dataflow from and to those repositories, and any external connections to the cardholder environment. If an assets inventory is not available, the diagrams should clearly show whether cardholder data is encrypted, truncated, masked or in clear text.

These requirements are expressed in PCI DSS Audit Procedures v.1.2, requirements 1.1.2.a and 1.1.2b (PCI Security Standards Council [PCI SCC], 2008, p. 13).

During the incident, the diagrams would quickly provide information in order to answer the following questions:



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

- How far the attacker may have been able to infiltrate?
- Which cardholder data repositories may have been exposed or compromised?
- Was cardholder data protected at rest and during transmission (encryption, masking, truncation, etc)?
- What are the points of entry to the cardholder environment?

c) Documentation and business justification for services, protocols, and ports allowed

During a breach, the configuration of all the firewalls and routers protecting the cardholder environment will be reviewed. Every single firewall rule or router ACL may be questioned and a business justification should exist. If supporting documentation is not available in a timely fashion, it may complicate the containment phase and may create disruption for other business areas.

If the attacker were able to compromise firewalls and/or routers, non-approved rules or ACLs would be easily identified during the review by matching the rules to previous configuration backups, or by verifying their business justification.

This documentation would help answering the following questions:

- Was poor firewall and router configuration responsible



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

for the compromise?

- Were firewall and/or router configuration changes following proper change management procedures?
- Was the attacker able to compromise firewalls and routers?

This requirement is expressed in PCI DSS Audit Procedures v.1.2, requirement 1.1.5. (PCI SSC, 2008, p. 14)

d) Configuration standards and change control documentation for all system components

If configuration standards for the system components do not exist or provide insufficient documentation, it would make identification, containment, and eradication much more difficult. During the incident, configuration questions require quick and precise answers. The following are questions that a system administrator should be able to answer:

- Is process XYZ part of the OS or any of the approved applications?
- Is there a reason for server XYZ having been configured differently from the rest of the servers?
- Does any of the approved applications need XYZ OS component running and/or enabled?

Maintaining the configuration standards up-to-date is



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

extremely important. Up-to-date information contributes to the incident response process by providing assurance that operating system and applications configuration have not been altered by the attacker.

PCI DSS requirement 2.2 mentions that configuration standards must be based on industry-accepted system hardening standards (PCI SSC, 2008, p. 18). Make sure your company follows a consistent configuration standard for all system components.

Additionally, PCI DSS requirement 6.4 mentions the need for change control documentation in order to identify any unauthorized changes (PCI SSC, 2008, p. 32).

e) Documentation of all key-management processes related to cardholder data encryption

If PCI DSS has been strictly followed, cardholder data must have been rendered unreadable anywhere it is stored. If encryption has been the method used, it could be the last layer of defense before an attacker has access to cardholder data in clear text.

Forensic investigators, auditors, and law enforcement will need documentation on how encryption keys are managed. This includes generation, distribution, storage, destruction, revocation, and replacement of encryption keys.

The information would be needed in order to verify whether encryption keys have been compromised or not.



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

PCI DSS v.1.2, requirement 3.6 details all the information that configuration standard are expected to document (PCI SSC, 2008, p. 24).

f) Antivirus audit logs

In general, all logs would be critical to understand how attackers were able to breach the cardholder data environment. For example, antivirus logs would be useful to answer the following questions:

- Did the antivirus software detect any malware used by the attackers? If not, was that due to the antivirus being misconfigured, disabled, or not up-to-date?

- Did the attackers try to install spyware, backdoors, or Trojan applications that were detected by the antivirus? Moreover, if they were detected, did any member of the security team take any actions?

g) Video camera data

In some cases where physical security has been a factor, video camera data could be decisive for the forensic investigation. For example, it would help identifying the culprits for incidents such as rogue wireless access points or modems deployments, or the breach of publicly accessible systems such as kiosks.

According to an article published by InformationWeek, besides wireless networks, one other possible points of entry for TJX's breach may have been the employment



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

application kiosks located at many of their stores (Greenemeir, 2007).

PCI DSS Requirement 9.1.1 mentions the need for collected video data being correlated with other entries. This data should be stored for at least three months, unless restricted by law (PCI SSC, 2008, p. 42).

h) Media inventories

Identifying media content would be critical in the event of a lost backup tape. The following questions may arise:

- Did the lost backup media contain payment card data?
- Was the data on that tape rendered unreadable using encryption, truncation, or hashing?
- How many payment cards have been affected by this incident?

PCI DSS Requirement 9.9.1 specifically mentions inventory logs of all media (PCI SSC, 2008, p. 44).

i) Audit trails for all system components

As mentioned above, logs are critical to understand how the attack happened. A compliant company should be able to solve the breach “puzzle” by inspecting the logs at different layers: network, OS, and application.

Logs should be exported from the system where logs are



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

generated to a secure server in order to avoid logs being altered or deleted during the intrusion.

All system components should keep accurate time by synchronizing their clocks to a common source. This requirement is very important; evidence obtained from logs may not be acceptable in court if there are inconsistencies in the logs provided by different system components.

PCI DSS section 10 details the requirements regarding logs. According to the standard, logs should be retained for at least one year. A minimum of three months should be available for immediate review.

j) Incident Response Plan

The Incident Response Plan should answer most of the procedural questions that could be asked during an incident. Reacting hastily under pressure only leads to making mistakes. The plan should provide a roadmap, templates, predetermined responses, and procedures on how to deal with the incident. The following questions should clearly be answered by your incident response plan:

- Should the systems be shutdown, disconnected from the network, or continue operating?
- Should this incident be reported to law enforcement?
- Should the payment card companies be notified?
- Should our company conduct its own incident response



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

and forensic investigation?

- How should the incident be reported to the card companies?
- Are there any Payment Card Brand specific requirements to handle and report the incident?

PCI DSS requirement 12.9 details several important aspects to consider regarding incident response such as regularly testing the plan and providing training to the personnel assigned to this task (PCI SSC, 2008, p. 56-58).

## 4.2 Processes that Should Be in Place

The other half of the preparation consists of processes that should be in place before an incident happens.

a) Daily operational security procedures

The impact that a security breach may have in an organization is highly influenced by how much time has passed from the moment the breach started to the moment it was detected. The longer the period, the higher the financial cost would be. Following daily operational security procedures is very important, especially those related to log monitoring. Procedures that have been documented but are not followed are useless.

PCI DSS requirements 12.2, 10.6, 12.5.2, and 12.5.5 mention the need for daily operational procedures and that log reviews for all system components should be performed on a



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

daily basis (PCI SSC, 2008, p. 48, 52, 54).

How your company handles the incident would reveal whether these requirements have been followed or not. During the investigation, it will be obvious whether the breach was detected by chance or due to daily reviews and log monitoring.

Statistics provided by Verizon Business' Data Breach Report demonstrated that 69% of the breaches were detected by a third party. This means that the company was not even aware that it has been breached. The other 24% was identified during normal work activities or by unusual system behavior, both of them considered passive detection. Finally, 7% was detected by log monitoring, which would be consider active detection (Verizon Business RISK Team, 2009, p. 37).

b) Formal Security Awareness Program

A formal security awareness program is an important factor to detect security breaches. The security awareness program for members of the IT department should include threats and vulnerabilities identified during the most recent risk assessment (requirement 12.1.2), the results of the most recent penetration tests and network vulnerability scanning reports (requirements 11.2 and 11.3), and new vulnerabilities identified through mailing lists or security newsletters (PCI SCC, 2008, p. 29, 49-50, 52).

PCI DSS Requirement 12.6 mentions the need for a formal



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

security awareness program (PCI SCC, 2008, p.55).

c) Formal Incident Response Training

Personnel with incident response responsibilities should be provided with appropriate training. As a minimum, the incident response team should be trained on the following areas:

- Initial incident response training for the specific IT infrastructure used by the organization.
- Electronic evidence preservation
- Incident response best practices
- Legal implications of an incident

## 5. Identification and Containment Phases

PCI DSS does not provide specific instructions to be followed whenever a security breach has been identified. However, the payment brands have specific requirements that companies should know in advance.

The confirmation of a security breach is the starting-time to comply with several requirements that the payment card brands have such as notification timelines and the use of certified incident response companies.

Although, your company may use internal resources in order to identify and contain a security breach, it is highly recommended to



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

use a third party specialized in incident response. There are several reasons behind this recommendation:

a) Experience

Attackers that may successfully breach the security of a company may attempt to use the same attacks with other companies. It is usual to find several companies that have been compromised using the same attack pattern.

Specialized incident response teams offer support in hundreds of incidents every year. Using their services may help identifying and containing a security breach very quickly.

b) Payment card requirements

MasterCard and Visa may require your company to use the services of an incident response assessor accepted by their respective companies, especially if your organization is a financial institution. American Express will require you to use a third party forensic investigator.

If you don’t choose one of their approved assessors, your company may have to incur additional expenses in the event the payment card brands not accepting your forensic report. They may require your company to hire one of the approved companies to validate the findings and recommendations provided by a non-approved incident response company.

A reference to the list of Visa Qualified Incident Response Assessors (QIRAs) is available in Appendix B.



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Visa has special requirements to be followed in order to preserve evidence and facilitate the investigation. The following requirements have been excerpted from Visa's CISP website:

- Do not access or alter compromised systems (i.e., don't log on at all to the machine and change passwords, do not log in as ROOT).
- Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug cable).
- Preserve logs and electronic evidence.
- Log all actions taken.
- If using a wireless network, change 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 all systems with cardholder data.

## 5.1. Common Attack Vectors

In the past, attackers have used several attack vectors in order to compromise systems. The following list details usual attack vectors:

- Wireless networks (Lack of strong encryption algorithms)
- Web Applications (SQL Injection and other OWASP top 10



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

vulnerabilities)

- Operating Systems (Lack of hardening and/or patching)
- Remote Access Accounts (IT Admins, employees, and vendors)
- Partners connections (Point-to-point connections and VPNs)
- Insider access (Employees and contractors)

## 6. Eradication and Recovery phases

Once the breach has been contained, eradication and recovery should be carefully executed. Your company should be diligent to eradicate all pieces of malware deployed by the attacker. Failing to do so may allow the attacker to recover remote access by using backdoors or Trojan applications installed during the initial intrusion. Your company will have to report the new intrusion and that may adversely affect your company's reputation to the payment card companies.

### 6.1. Reporting the Incident

American Express, Discovery, and Visa require you to notify them immediately upon confirming a security breach. MasterCard requires to be notified within 24 hours of knowledge.

### 6.2. Forensic Investigations and Audits

Visa requires you to produce a forensic report within three business days from the reported compromise. MasterCard specifies that



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

the report should be available within 72 hours of knowledge, which may not be business days in all the cases.

Payment card brands will demand to know how many cards of their respective brands may have been compromised. Your company should be ready to provide that information. Within ten business days, Visa will require you to provide a list of all the compromised cards. MasterCard has similar requirement to report compromised cards, as well as a specific formats for the list.

Visas' report has also a specific format and its main objectives are:

1) Determining how the breach occurred.

2) Confirming the number of credit cards compromised.

3) Determining your company's PCI DSS compliance at the time of the breach.

4) Verifying that the eradication and recovery efforts have been effective and that your company is no longer compromised.

The audit report is very important, since it will be used to establish your company's PCI DSS compliance and will definitely determine whether your company is liable and to what extent.

It is highly probable that payment card brands may require an additional PCI DSS Assessment in order to identify specific non-compliances and for your company to develop a detailed remediation plan.



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

## 6.3. Failing to Report an Incident

Some companies may think that not reporting an incident would better serve their interests. However, in the absence of self-reporting, eventually those companies may be identified as a source of cardholder data compromise. In fact, as mentioned previously, according to Verizon Business' 2009 Breach Report, many of the security breaches are not detected by the companies themselves, but by third parties, among them, the payment card brands or the law enforcement agencies (Verizon Business RISK Team, 2009, p.37).

The payment card companies have implemented process to identify the source of a breach as precisely as possible. Charge-backs and fraudulent transactions are reported to the payment card companies, which use that information to identify merchants or service providers that may have been breached.

Failing to report the incident may affect your company with additional fines, as well as expose your company to legal liabilities. On the other hand, reporting the incident may actually help your company to demonstrate that the security controls in place were actually working.

# 7. Lessons Learned Phase

After the security breach has been handled, your company will have to improve its security strategy, incident response plan, and monitoring processes.

PCI DSS requires companies to develop processes to modify and evolve the incident response plan according to the lessons learned



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

from the incident.

A thorough analysis of how the incident was detected, notified, handled and contained should be performed. The incident plan should be updated according to the results of the analysis in order to improve monitoring alerts analysis, response times, and to optimize the incident response procedures.

## 7.1. General Recommendations

After a successful breach, an attacker may have been able to obtain a vast knowledge of the company's IT infrastructure. Consider that the attacker may have obtained the following information:

1) Operating systems in use, name conventions, applications and services running for most of the servers.

2) List of employees and their positions, users IDs and passwords, e-mail accounts, and other personal information.

3) Application source code.

4) Encryption keys.

Armed with all that information, it would be easier for an attacker to spend their time trying to compromise the same company again rather than trying to compromise a new company for which he doesn't have any information at all.

Your company has to plan for the worst-case scenarios, in special attacks involving social engineering. The attacker may send forged e-mails resembling internal e-mails urging users to enter



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

information, to download software or to click on links of malicious websites.

In order to avoid these attacks, your company will have to monitor endpoint security controls including antivirus software, web-filtering logs, and networks IDS covering end-user segments and others.

## 8. The Cost of a Security Breach

In April 10, 2007, a Forrester Report, "Calculating the Cost of a Security Breach" by Khalid Kark, determined that a security breach can cost a company between $90 and $305 per record.

In January 2007, TJX announced that a security breach of its transaction processing network had resulted in data thieves stealing information on 45.6 million payment cards (Lemos, 2007). As a result of the breach, banks and banks associations sued the company for their costs in replacing payment cards. Banks that issue Visa-Branded credit and debit cards agreed to a settlement for an amount of nearly $41 millions. MasterCard issuers agreed to similar terms for up to $24 million settlement. It is estimated that TJX's other breach related costs are around $30 million (Lemos, 2008).

According to the bank associations, banks paid up to $25 per card to replace credit-card and debit-card accounts. They also blamed the company for a surge in credit-card and debit-card fraud of at least $8 million.

Hence, at least the following costs should be considered in the event of a breach:



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

- Cost of replacing payment cards
- Fraudulent transactions charged to compromised payment cards
- Regulatory fines from the Payment Brands
- Forensic investigations costs
- Audit costs (Post-Incident)
- Audits costs (Compliance)
- Expenses of legal fees
- PR costs
- Lost employee productivity

MasterCard Rules mentions that MasterCard may impose a fine of up to $100,000 per security breach.

## 9. Additional Payment Card Brands Consequences

Payment card brands assign levels to merchants and service providers based on the number of transactions performed during a year.

Level 1 merchants and service providers have to be audited by a QSA. If a company is breached, independently of the number of transactions, the payment card brands will assign the compromised companies a Level 1 status, requiring yearly audits.



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

## 10. How the Payment Card Companies Determine Liability

In October 2006, Visa implemented ADCR (Account Data Compromise Recovery), a process to calculate acquirers' liability whenever magnetic-stripe data has been determined as compromised.

A whitepaper, entitled "What Every Merchant Should Know About the New Account Data Compromise Recovery Process", was published to describe the process, however, it's no longer available on Visa's website. A copy can be obtained on the National Retail Federation's website.

The process describes how Visa calculates an acquirer's liability and may help your company determine the impact of a security breach where magnetic-stripe data have been compromised. Other types of compromises may follow a similar process.

The document also mentions one of the key systems used during the breach report process: Compromised Account Management System (CAMS). According to the whitepaper, CAMS offers a secure channel for acquirers, merchants, law enforcement agencies, and issuers to transmit compromised and stolen/recovered to and from Visa through an encrypted site (Visa, 2006).

According to a recent publication, MasterCard seems to have a similar process to report compromised cards (McGlasson, 2009).

## 11. Conclusion

There is no perfect security; PCI DSS certified companies should be prepared to handle security incidents.



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Unlike PCI DSS, the Payment Card Companies don't have standard procedures or policies regarding incident handling, breach notification, and forensic analysis.

By following the recommendations in this paper, companies would minimize the risk of additional financial impacts in the event of a security breach. Understanding how difficult it is to deal with a security breach would definitely help raising security awareness within a company.

© SANS Institute 2009, Author retains full rights.



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

## Appendix A: Requirements Matrix

| REQUIREMENTS | AMERICAN EXPRESS | DISCOVER NETWORK | JCB CARDS | MasterCard | VISA |
|---|---|---|---|---|---|
| **Notification** | Immediately | Immediately | Not specified | Within 24 hours of knowledge | Immediately |
| **Forensic Investigation & Audit** | Should be performed by a third party forensic investigator. | Not specified | Not specified | Should be performed by a data security firm acceptable to MasterCard. | Independent forensic investigation may be required at Visa and merchant bank's discretion. A QIRA (Qualified Incident Response Assessor) should perform the forensic investigation.<br>An independent third party acceptable to Visa must conduct a security review after eradication / vulnerabilities remediation. |
| **Forensic Investigation Timeframe** | Not specified | Not specified | Not specified | Within 72 hours of knowledge. | Within 3 business days of the reported |

© SANS Institute 2009, Author retains full rights.

| REQUIREMENTS | AMERICAN EXPRESS | DISCOVER NETWORK | JCB CARDS | MasterCard | VISA |
|---|---|---|---|---|---|
| | | | | | compromise, an incident report should be provided to your merchant bank. |
| **Contact information** | Service Providers:<br>▪ Contact your third party processor relationship manager or (800)-528-5200<br>Merchants:<br>▪ Contact your client manager or (800)-528-5200 | Contact (800) 347-3083 | Not specified | Contact MasterCard Compromised Account Team at compromised_account_team@mastercard.com or (636) 722-4100 | Contact:<br>▪ Your merchant bank or Visa Fraud Investigations and Incident Management Group at (650) 432-2978<br>▪ United States Secret Service |
| **Compromised Account Reporting** | Not specified | Not specified | Not specified | Use a text file (.txt) and expiration date in a MMYY format. | Provide all the compromised accounts within 10 business days. |
| **Additional Requirements** | Not specified | Not specified | Not Specified | Weekly Status reports. | Specific report format. |

© SANS Institute 2009, Author retains full rights.

## Appendix B: Payment Card References

Data Security

https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=home&ln=en&frm=US

In case of a breach (Merchants)

https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=merchinfo&ln=en&frm=US&tabbed=breach

In case of a breach (Service Providers)

https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=spinfo&ln=en&frm=US&tabbed=breach

Discovery Information Security & Compliance (DISC)

http://www.discovernetwork.com/fraudsecurity/disc.html

http://www.jcbusa.com/

Site Data Protection (SDP), MasterCard rules, section 5: 10

http://www.mastercard.com/us/wce/PDF/MasterCard_Rules_5_08.pdf

Cardholder Information Security Program (CISP)

http://usa.visa.com/merchants/risk_management/cisp.html?ep=v_sym_cisp

CISP – What to do if compromised

http://usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf

Qualified CISP Incident Response Assessors

http://usa.visa.com/download/merchants/cisp_qualified_cisp_incident_response_assessors_list.pdf



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

## Acknowledgments

Special thanks to Ronald R. Dormido, Verizon Business Investigative Response Team for providing feedback and proofreading the document. Thanks to Todd Bell and Matthew Arntsen, Verizon Business PCI DSS Assessment Team, for their feedback.

© SANS Institute 2009, Author retains full rights.



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

## References

Greenemeir, L. (2007). The TJX Effect. Retrieved April 3, 2009, from InformationWeek Website: http://www.informationweek.com/news/security/cybercrime/showArticle.jhtml?articleID=201400171

Identity Theft Resource Center. (2009). ITRC 2008 Breach List. Retrieved February 23, 2009, from Identity Theft Center. Website: http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml

Lemos, R. (2007). TJX theft tops 45.6 million card numbers. Retrieved February 23, 2009, from SecurityFocus.com Website: http://www.securityfocus.com/news/11455

Lemos, R. (2008). TJX completes MasterCard breach settlement. Retrieved February 23, 2009, from SecurityFocus.com Website: http://www.securityfocus.com/brief/740

McGlasson, L. (2009). Beyond Heartland: Another Payments Processor Linked to Data Breach. Retrieved March 10, 2009, from BankInfoSecurity.com Website: http://www.bankinfosecurity.com/articles.php?art_id=1230

PCI Security Standards Council [PCI SCC]. (2008). PCI DSS. Retrieved February 23, 2009, from PCI Security Standards Council Website: https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html

SANS Institute. (2008). Security 504.1 Incident Handling Step-by-Step and Computer Crime Investigation. SANS Institute.

Verizon Business RISK Team. (2009). 2009 Data Breach Investigations Report. Retrieved April 3, 2009, from Verizon Business Website: http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

VISA. (2006). What Every Merchant Should Know About the New Account Data Compromise Recovery Process. Retrieved March 10, 2009, from National Retail Federation website: http://www.nrf.com/modules.php?name=Documents&op=viewlive&sp_id=261

VISA. (2008). Responding to a Data Breach: Communications Guidelines for Merchants. Retrieved March 10, 2009, from Visa website: http://usa.visa.com/download/merchants/cisp_responding_to_a_data_breach.pdf

Visa. (2009). Carholder Information Security Program Overview. Retrieved February 23, 2009, from Usa.visa.com Website: http://usa.visa.com/merchants/risk_management/cisp_overview.html

© SANS Institute 2009, Author retains full rights.



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Last Updated: September 5th, 2015

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| SANS Crystal City 2015 | Crystal City, VAUS | Sep 08, 2015 - Sep 13, 2015 | Live Event |
| SANS Network Security 2015 | Las Vegas, NVUS | Sep 12, 2015 - Sep 21, 2015 | Live Event |
| SANS Seoul 2015 | Seoul, KR | Sep 14, 2015 - Sep 19, 2015 | Live Event |
| SANS Tallinn 2015 | Tallinn, EE | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Baltimore 2015 | Baltimore, MDUS | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| Data Breach Investigation Summit & Training | Dallas, TXUS | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Perth 2015 | Perth, AU | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS ICS Amsterdam 2015 | Amsterdam, NL | Sep 22, 2015 - Sep 28, 2015 | Live Event |
| SANS Bangalore 2015 | Bangalore, IN | Sep 28, 2015 - Oct 17, 2015 | Live Event |
| SANS Seattle 2015 | Seattle, WAUS | Oct 05, 2015 - Oct 10, 2015 | Live Event |
| SANS DFIR Prague 2015 | Prague, CZ | Oct 05, 2015 - Oct 17, 2015 | Live Event |
| SOS: SANS October Singapore 2015 | Singapore, SG | Oct 12, 2015 - Oct 24, 2015 | Live Event |
| SANS Tysons Corner 2015 | Tysons Corner, VAUS | Oct 12, 2015 - Oct 17, 2015 | Live Event |
| SANS Gulf Region 2015 | Dubai, AE | Oct 17, 2015 - Oct 29, 2015 | Live Event |
| SANS Tokyo Autumn 2015 | Tokyo, JP | Oct 19, 2015 - Oct 31, 2015 | Live Event |
| SANS Cyber Defense San Diego 2015 | San Diego, CAUS | Oct 19, 2015 - Oct 24, 2015 | Live Event |
| SANS Sydney 2015 | Sydney, AU | Nov 09, 2015 - Nov 21, 2015 | Live Event |
| SANS South Florida 2015 | Fort Lauderdale, FLUS | Nov 09, 2015 - Nov 14, 2015 | Live Event |
| SANS London 2015 | London, GB | Nov 14, 2015 - Nov 23, 2015 | Live Event |
| Pen Test Hackfest Summit & Training | Alexandria, VAUS | Nov 16, 2015 - Nov 23, 2015 | Live Event |
| SANS Hyderabad 2015 | Hyderabad, IN | Nov 24, 2015 - Dec 04, 2015 | Live Event |
| SANS Cape Town 2015 | Cape Town, ZA | Nov 30, 2015 - Dec 05, 2015 | Live Event |
| SANS San Francisco 2015 | San Francisco, CAUS | Nov 30, 2015 - Dec 05, 2015 | Live Event |
| Security Leadership Summit & Training | Dallas, TXUS | Dec 03, 2015 - Dec 10, 2015 | Live Event |
| SANS Milan 2015 | OnlineIT | Sep 07, 2015 - Sep 12, 2015 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |