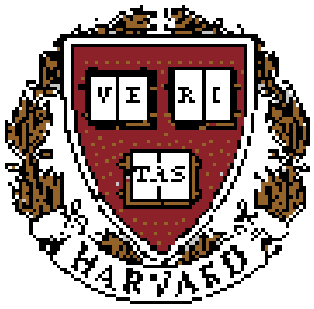

Harvard University

Payment Card Industry (PCI) Compliance
Business Process Documentation

Business Process:	PCI Data Security Breach
Documented By:	Stephanie Breen
Creation Date:	1/19/06
Updated	11/5/13

Change Record

Date	Name	Change
1/19	Gene	Initial Draft
1/20	Gene	Incorporated Michelle's edits, Placed questions as open items.
1/20	Gene	Incorporated Cheryl's Edits and updated PIRT requirements based on card associations' requirements
1/23	Gene	Incorporated Scott Bradner's Feedback
1/31	Gene	Additional tweaks from Scott & Cheryl
2/8/06	Gene	Changes based on feedback from 2-7 PCI Working Group meeting.
2/10/06	Gene	Changed to reflect information from Trustwave regarding level 1 assessments and forensic investigations.
2/21	Gene	Included word tracker on changes since original document.
3/26	Gene	Included Feedback from PCI Working Group and consistency Check with other documents
6/26	Gene	Updated with inclusion of IT IS on PIRT if CCS is involved
11/4/13	Stephanie	Reviewed and updated terminology and contact information

Reviewed by:

Date	Name
2/7	First Review by PCI Working Group

TABLE OF CONTENTS

DEFINITIONS

Local Unit. A Harvard department or school that has obtained a credit card merchant number assigned from Cash Management

PCI Incident Response Team. A team of technical and business representatives assembled to investigate a breach of a system containing or processing credit card data.

PCI Data Security Breach. A breach is any of the following

- An unauthorized access to a computer that accepts, processes or stores credit card information
- An unauthorized access to a computer that forwards users to a computer that accepts credit card information
- The loss or theft of a computer that stored credit card account numbers
- Or the unauthorized release of credit card account numbers.

Please note that unauthorized access includes viruses and worms as well as unauthorized access by Harvard personnel.

Personal Information. An individual's first name or first initial and last name in combination with any one or more of the following data elements:

- SSN;
- Driver's license number or government issued ID card number; or
- Account number, credit or debit card number, in combination with any required security code, access code, or password (e.g., a PIN) that would permit access to an individual's financial account.

ABBREVIATIONS

BAMS – Bank of America Merchant Services

OGC – Office of General Counsel

PCI – Payment Card Industry

PIRT – PCI Incident Response Team

RMAS – Risk Management and Audit Services

SSN – Social Security Number

HUIT –Harvard University Information Technology**HUIT IT SECURITY** University Technology Security Officer

PROCESS OVERVIEW

This procedure applies to all merchants regardless of the method they accept credit cards. If an individual breach is determined to only involve paper records the IT resources assigned to the PCI Incident response Team (PIRT) will be released.

- School IT Directors designate who should be the contact for any breaches in their school. HUIT designates who should be the contact for any breaches in departments they support.
- If a merchant has an infrastructure not supported by the school IT department, then the business owner must additionally identify IT contacts that are specific to the merchant.
- Credit card merchant business managers and system operators must notify cash management immediately in the event of a breach or suspected breach. A suspected breach is where there is evidence of access that can not be confirmed to be legitimate or a known lapse in physical or logical security regardless of whether evidence of access exists or not.
- A PIRT is activated to minimize the impact, fix the vulnerability exploited and investigate the breach: (see page 6 for responsibilities of team)
    - Cash Management (Team Leader)
    - Credit Card Merchant Business Owner
    - University Technology Security Officer
    - HUIT or School IT contact for PCI breaches
    - RMAS
    - Local IT Infrastructure support, if applicable
    - IT Support person(s) for web application compromised
- Cash Management makes the following notifications
    - Acquiring Bank: indicate that there is evidence of a possible breach and that we are investigating.
    - The Harvard's Office of News and Public Affairs (News Office): so that they can respond to inquiries if the incident becomes public. News Office is instructed to not release the information but only respond to queries that we are investigating the situation. (See page 8)
    - Office of General Counsel: To put them on notice that there is the potential need for a legal notification to individuals that had personal information compromised. Also that there is the possibility of law enforcement involvement in the investigation. (See page 8)
- PIRT has the following priorities in investigating the incident:
    - First priority is preventing any further damage if the breach is ongoing.
    - Second priority is closing any vulnerabilities exploited
    - Third priority is investigating what caused the problem and what data was compromised during the breach.
- If it is determined that credit card account numbers were or may have been compromised, the merchant will be required to undergo a full level 1 PCI Data Security Standards Assessment[1]. **If the breach appears to affect an IT infrastructure that supports more than one merchant, then all merchants supported by that infrastructure likely would be included in the review** (see open issue 5) The assessment must be performed by an authorized PCI Assessor. The local unit must assume all costs associated with this assessment.

[1] This is the same onsite audit that level 1 merchants and service providers must undergo to obtain certification. The audit or assessment is performed by an authorized 3rd party assessor.

- Many states now require notification to individuals whose personal information was or may have been accessed without proper authorization. If it is determined that personal information (whether or not credit card data was included) was or may have been compromised, local units must work with OGC to determine whether notice is required and how it should be sent.
- Within four (4) business days, a report is issued by Cash Management concerning the breach. Copies to Vice President for Finance, Chief Information Officer, Director of Risk Management and Audit Services and the Director/Manager of the unit involved. If the unit is within a school the Administrative Dean, Financial Dean, and IT Director of the School will also receive a copy.

General Business Process

Local Unit Responsibilities

1) Be alert to potential breaches and always review logs on a regular basis for:
   - Suspicious behavior
   - Unusual incidents in audit logs
   - User or anonymous reports of problems
   - Unauthorized security configuration changes
   - Unusual traffic or activity
   - Lapsed physical security
   - Sensitive information in the wrong place or hands
   - User complaint which triggers an investigation.
   - Loss or theft of a computer or backup media
2) Contain and limit the exposure *immediately*.
   - Document all actions taken
   - Remove the machine from the network. Do not turn the compromised machine off.
   - Do not access or alter compromised systems.
   - Preserve all available logs (firewall, IDS, web server, operating system, remote access, etc.) that could be used to help identify the source and extent of the attack.
   - If using wireless network, change SSID on the AP and other machines that may be using this connection with the exception of any systems believed to be compromised.
   - Be on high alert and monitor other systems that accept, store or process credit card account numbers as well as any other computers that users on the breached computer have accounts (too often the same password is used).
3) Contact Cash Management (pci_compliance@harvard.edu) mmediately that a breach or suspected breach has occurred or is in progress.
4) Work with PCI Incident Response Team (PIRT) to investigate the breach and repair the systems.
5) Identify what account numbers or other personal information (PI) may have been compromised.
6) Work with HUIT IT SECURITY , RMAS Associate Director of IS Audit, Manager Cash Management and OGC Coordinator to determine if notification should be sent to individuals affected by the incident.
7) Compromised systems must not be put back into production or connected to the Internet until the PIRT gives its consent.
8) Assume any extra costs associated with the incident:
   - Any external resources contracted to participate in the investigation
   - HUIT resources used to supplement local IT support resources
   - It is up to the individual school to determine if IT resources expended on PIRT are billed to the local unit or absorbed as overhead.

- Cost of level 1 PCI Security Standard Assessment performed by external third party.[1]
- Any fines or penalties assessed by the Bank or credit card associations
- Any legal fees or penalties incurred as a result of the incident
- Any costs associated with producing and sending notifications
- Any external costs associated with a follow-up audit by RMAS

Cash Management Responsibilities

1) Activate PIRT
   - Cash Management Representative
   - Credit Card Merchant business owner or designated contact
   - HUIT IT Security OfficerSchool IT contact for PCI Breaches (For the school where the breach occurred) and/or HUIT contact if HUIT hosted or managed system
   - IT Support Person for the web application compromised
     - Contact supplied by business owner
   - Others as needed (e.g., HUIT Networks Operations Manager, IS Auditing in RMAS, subject matter experts from HUIT or school IT department)
2) Alert all necessary parties **within 24 hours** of original notification**.** (For card associations this must be within 24 hours elapsed time of discovering the breach. For other contacts it must be within one business day of discovering the breach.)
   - Internal Harvard contacts
     - PCI incident response Team (see above)
     - News Office (617) 495-1585
     - Office of General Counsel (617) 496 4172
     - School financial dean
   - Bank of America Merchant Services (The bank will notify the card associations)
   - Local law enforcement office: (See Open Issue 6)
     - U.S. Secret Service and/or
     - Federal Bureau of Investigation (FBI)
3) Provide all possibly compromised account numbers within 24 hours to:
   - Merchant Bank –Bank of America Merchant Services
   - Card Associations
4) Contact Trustwave to conduct a Level 1 PCI Security Standard Assessment if it has been determined that credit card account numbers were compromised. The timing and extent of this review will be determined after consulting the acquiring bank. The review typically would only include the merchant that was breached. However, if the IT infrastructure that was compromised also includes other merchants, then all merchants supported by that infrastructure would be included in the level 1 PCI Security Standard Assessment. The Merchant will remain at the tier 1 compliance level for 12 months following the incident.
5) If requested by HUIT IT SECURITY , contact an Approved vendor to help the PIRT team conduct a PCI forensic investigation. PCI regulations prohibit a certification vendor from conducting forensic investigations related to a PCI Breach for their own customers. Therefore Cash Management will contact one of the following vendors:[2]

FIRM	PRIMARY CONTACT	HOW TO REACH

[1] The typical cost of a Level 1 PCI Security Standard Assessment for a single merchant is $20,000
[2] This list should be updated if the card associations add or change vendors that can perform PCI forensic investigations.

Security Metrics www.securitymetrics.com	Wenlock Free	wfree@securitymetrics.com (801) 724-9600
Ubizen http://www.ubizen.com	Bryan Sartin	bryan.sartin@us.ubizen.com (212) 271-0374
Verisign (Guardent) http://www.verisign.com	Vern Cole	vcole@verisign.com (206) 356-6827

6) Contact RMAS to have local unit involved in incident receive a full Information Systems audit of their system 6 months after the onsite level 1 PCI Security Assessment is completed.. If RMAS must use outside resources to accomplish this, the local unit will bear the costs associated with the audit.

7) Maintain a list of contacts for the PCI Incident response teams. Contact school IT directors and HUIT every 6 months to confirm the accuracy of the contact names.

8) Maintain a log of PCI incidents

University Technology Security Officer Responsibilities

1) Participate on PIRT

2) Monitor the progress of the team
   - If the PIRT is making insufficient progress due to lack of resources, the HUIT IT SECURITY may take the following escalation action or other actions as deemed appropriate
     - Notify the School IT director, determine if additional local resources can be made available
     - Request additional resources from HUIT if needed (Extra HUIT resources will be billed to the local unit or school.)
     - Request Cash Management to engage an authorized vendor to perform an Incident/Forensic Investigation and Vulnerability Scan to augment the resources of the PIRT. The local unit will be billed this cost.

3) If the report of a PIRT calls for action beyond the local unit. Monitors actions taken by those other parties. Follows-up where required.

PCI Incident Response Team Responsibilities

1) Cash Management representative is team leader. As such they are responsible for ensuring that regular updates and communication between team members takes place. They are responsible for ensuring that all steps in this document are assigned to team members and carried out. (See Appendix A – PIRT Checklist.) They also have the primary responsibility for performing the notifications that are to take place in the first 24 hours. Any technical forensic investigations of systems are conducted primarily by HUIT/School IT representatives, Merchant IT representatives and RMAS under the direction of the HUIT IT SECURITY . In the absence of the HUIT IT SECURITY the HUIT/School representative shall lead the forensic investigation.

2) Ensure that the system compromised has been removed from the network until its vulnerability has been corrected.

3) If possible, make a backup copy of the disk of the breached machine then preserve the original disk for forensics and evidence - switch the system to run on the copy

4) Write down all actions taken while working on compromised machines.

5) Preserve all logs and electronic evidence.

6) Through reviewing system and network logs, configuration of the compromised system, application audit trails, and other evidence determine the cause and extent of the compromise.
7) Identify potential remedies.
8) If requested, assist local unit in choosing the most appropriate remedy and/or in determining what data (e.g., what cardholder credit card numbers) was compromised if any.
9) Work with card association incident response teams, if they choose to get involved.
10) If needed, work with any law enforcement agencies involved in the breach. Support their investigations under the direction of the Office of the General Counsel.
11) If notifications are to be sent:
    a) Draft notification communication
    b) Have it reviewed by OGC and News Office
    c) Send notification to affected individuals
    d) Send copies of notification and the date it was distributed to OGC, RMAS, HUIT IT SECURITY and Cash Management
12) Have all compromised systems scanned by Trustwave for vulnerabilities prior to allowing them to be placed back into production. Perform other tests or probes of the system as appropriate.
13) If the investigation reveals that other systems are at risk, notify the individuals or the university community as appropriate of the potential risk and suggested steps to take to minimize it.
14) PCI requires that the Bank and card associations receive a report on the incident within 4 business days. In addition the following Harvard individuals should also receive a copy with a cover page that provides a brief overview and identifies additional areas within Harvard that may have similar exposure:
    - Vice President for Finance
    - OTM Assistant Treasurer
    - Manager Cash Management
    - Chief Information Officer
    - Director of Risk Management and Audit Services
    - Director/Manager of the unit involved.
    - If the unit is within a school the Administrative Dean, Financial Dean, and IT Director of the School will also receive a copy.
15) The template for the report can be found in Appendix B.

Other Responsibilities

Office of General Counsel

- Consult on whether and how notification must be made to individuals who had or may have had personal information compromised. Approve final wording for any legal notifications
- Be primary interface with law enforcement agencies if they become involved.

News Office

- Be aware of incident
- Respond to press inquiries as needed. Initial responses should only indicate that we are investigating the situation. We should not confirm that a breach has taken place before the PIRT has finished their investigation.

- If there are inquiries the News Office should notify Cash Management.
- Serve as only interface with the press regarding the incident
- Release only information cleared with Cash Management and OGC.

School IT Directors

- Appoint primary and backup individuals to serve on PIRT for credit card sites within their school. These are generally network engineers or system administrators. Contact information must include a way to reach someone who can respond to emergencies on a 24/7 basis. If the Schools network is supported by another IT department such as HUIT the director can name contacts from those departments with their permission.
- In the event of a breach, make a best effort to provide any additional support required by PIRT.
- Provide immediate emergency response to any security incidents with PCI covered sites within their school.

Local IT Support Groups

- Appoint primary and backup individuals to serve on PIRT for credit card sites they support. These are generally network engineers or system administrators and web developers. Contact information must include a way to reach someone who can respond to emergencies on a 24/7 basis.
- In the event of a breach, make a best effort to provide any additional support required by PIRT.
- Provide immediate emergency response to any security incidents with PCI covered sites within their school.

Harvard University Information Technology

- Appoint primary and backup individuals to serve on PIRT for those departments they support. These are generally network engineers or system administrators. Contact information must include a way to reach someone who can respond to emergencies on a 24/7 basis.
- In the event of a breach, make a best effort to provide any additional support required by PIRT.
- Provide immediate emergency response to any security incidents with PCI covered sites within their school.
- If requested by HUIT IT SECURITY to provide additional resources, because local unit is unable to provide, make a best effort to address the need on a charge back basis, to support or augment PIRT.

Exceptions

There are no exceptions to this process.

Open Items

1. Should RMAS be included on the PIRT for each breach? **Resolved that RMAS will be included on PIRT.**

2. Should a draft notification be created by Cash Management or OGC? **This issue became mute for this document as the notification format was removed from this document. Cash Management will Develop a separate document that addresses a template for notifications.**

3. Who is the team leader for the PCI Incident Response Team? Should it rotate? **The Cash Management representative on the PIRT will be the team leader.**

4. Determine specific contacts in News Office and Bank of America Merchant Services to place initial call. **Resolved and telephone numbers entered.**

5. PCI requires that if a breach occurs the merchant is immediately elevated to Tier 1 and must have an onsite assessment of compliance. We need to confirm with Trustwave whether in Harvard's case this would include all of Harvard or just the individual merchant that had the breach. We also need to determine if this elevation to tier 1 is permanent or temporary. The major difference in requirements is an annual onsite assessment by an authorized PCI assessor versus a self assessment questionnaire. The onsite assessment, if for all of Harvard, would require the equivalent of full IT audit of all systems where cardholder data is retained, stored or processed. **Generally the elevation to tier 1 is only for the merchant that had the breach and they will remain at that level for 12 months. If the breach appears to affect an IT infrastructure that supports more than one merchant, then all merchants supported by that infrastructure likely would be included in the review. The acquiring bank, for us Bank of America, determines the scope and length of time for the Tier 1 elevation.**

6. Who is responsible for bringing in or notifying law enforcement? Is it us or does the bank and or card associations bring them in. **Confirmed that Bank will notify the card associations. It is our responsibility to notify law enforcement. Will need to check with OGC on what procedure they would like to follow.**

SCREEN SHOTS

None

Appendix A PIRT Checklist

This check list is to be used by the PIRT team leader while dealing with an incident. It serves as a reminder of the steps to be completed as well as a way of documenting when they were done and who performed the tasks.

Merchant:

Date and Time of start of incident:

Date and Time when breached system removed from network:

Date and Time Cash Management notified:

PIRT Members

Team Member	Name	Email	Phone(s)
Cash Management (Team Leader)			
Credit Card Merchant Business Owner			
HUIT IT Security Officer			
HUIT/School IT contact for PCI breaches			
RMAS			
Local IT Infrastructure, if applicable			
IT Support person(s) for web application			
Others			

Tasks	Who	Expected	Completed
Alert all parties within 24 hours			
Internal Harvard contacts			
PIRT activated			
News Office (617) 495-1585			
Office of General Counsel (617) 496 4172			
School financial dean			
Bank of America Merchant Services (800) 228-5882			
Card Associations:			
American Express: Client Manager or (800) 528-5200			
Discover: Relationship Manager or Merchant Security Department at (800) 347-3083			
MasterCard: Compromised Account Team at (636) 722-4100 or compromised_account_team@mastercard.com			
Visa: Fraud Control Group at (650) 432-2978			
Local law enforcement office:			
U.S. Secret Service and/or			
Federal Bureau of Investigation (FBI)			
Convene first PIRT meeting, generally this is a conference call. The following should be accomplished in this meeting: • Confirm that any affected computers have been removed from the network • Agree on assignment of tasks (who and when) • Determine if additional PIRT members are required • If determined that there are no computers involved in the breach, Release IT support members from team. • Set time for first update- usually another conference call. • Establish how often team will have conference calls	Team Leader	Within first hour of Cash Management being notified	
Team Leader emails contact information on team to all team members			
If possible, make a backup copy of the disk of the breached machine then preserve the original disk for forensics and evidence - switch the system to run on the copy			
Keep a log of all actions taken while working on compromised machines.	All team members responsible for writing down their own actions. Each member forwards to team leader.		
Preserve all logs and electronic evidence.			

Conduct Forensic investigation: Through reviewing system and network logs, configuration of the compromised system, application audit trails, and other evidence determine the cause and extent of the compromise.			
Additional tasks identified by PIRT			
Additional Tasks identified to support Card Association incident response teams or law enforcement			
If notifications are to be sent:			
• Draft notification communication			
• Have it reviewed by OGC and News Office			
• Send notification to affected individuals			
• Send copies of notification and the date it was distributed to OGC, RMAS, HUIT IT SECURITY and Cash Management			

Have all compromised systems scanned by Trustwave for vulnerabilities prior to allowing them to be placed back into production. Perform other tests or probes of the system as appropriate.			
Determine whether merchant can place system back into production. All team members should agree.			
If the investigation reveals that other systems are at risk, notify the individuals or the university community as appropriate of the potential risk and suggested steps to take to minimize it.			
Within 4 business days, prepare incident report to the Bank and card associations required by PCI.			

Appendix B – Incident Report Template

The report content and format standards outlined below must be followed when completing the Incident Response Report for the bank and card associations.

I. Executive Summary:

- Provide overview of the incident
  - – Include Risk Level (High, Medium, or Low) during forensic analysis
  - – Specify if compromise has been contained

II. Background

III. PCI Status

- Based on findings identified on the forensic investigation, list non-compliant PCI requirements

IV. Network Infrastructure Overview

- Include a diagram of the network

V. Investigative Procedures

- Include forensic tools used during investigation

VI. Findings

- Type of account information at risk:
  - _ Account number
  - _ Expiration date
  - _ Cardholder name
  - _ Cardholder address
  - _ CVV2
  - _ Track 1 and Track 2
  - _ PIN blocks
- Number of accounts at risk
- Timeframe of accounts at risk
- Timeframe of compromise and source of compromise
- Identify any data exported by intruder.
- Provide specifics on firewall, infrastructure, host, and personnel findings.
- If no hacker utilities/tools were found, explain how intrusion could occur.
- Identify any third-party payment application, including product version.

VII. Compromised Entity Action

VIII. Recommendations

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