Western Oregon University
Data Security Breach
Incident Response Plan

This plan outlines the steps to follow in the event secure data is compromised and identifies and describes the roles and responsibilities of the Incident Response Team. The Incident Response Team is responsible for putting the plan into action.

Incident Response Team

The Incident Response Team is established to provide a quick, effective and orderly response to computer related incidents such as virus infections, hacker attempts and break-ins, improper disclosure of confidential information to others, system service interruptions, breach of personal information, and other events with serious information security implications. The Incident Response Team's mission is to prevent a serious loss of profits, public confidence or information assets by providing an immediate, effective and skillful response to any unexpected event involving computer information systems, networks or databases. The Incident Response Team is authorized to take appropriate steps deemed necessary to contain, mitigate or resolve a computer security incident. The Team is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-effective manner and reporting findings to management and the appropriate authorities as necessary. The Chief Information Security Officer will coordinate these investigations. The Incident Response Team will subscribe to various security industry alert services to keep abreast of relevant threats, vulnerabilities or alerts from actual incidents.

Incident Response Team Members

Each of the following members will have a primary role in incident response.

- Information Technology Director / Chief Information Security Officer
- Information Technology Assistant Director / Security Manager
- Vice President Finance and Administration
- Information Technology Service Request Desk
-

Each of the following members may provide supporting roles during incident response.

- Information Technology Unix Systems Administrator / Security Analyst
- Information Technology Windows Systems Administrator
- Information Technology Network Engineer
- Internal Audit

Incident Response Team Roles and Responsibilities

Information Technology Service Request Desk

- Central point of contact for all computer incidents
- Notifies Chief Information Security Officer to activate computer incident response team

Information Technology Director / Information Technology Assistant Director

- Determines the nature and scope of the incident
- Contacts qualified information security specialists for advice as needed
- Contacts members of the Incident Response Team
- Determines which Incident Response Team members play an active role in the investigation
- Provides proper training on incident handling
- Escalates to executive management as appropriate
- Contacts auxiliary departments as appropriate
- Monitors progress of the investigation
- Ensures evidence gathering, chain of custody, and preservation is appropriate
- Prepares a written summary of the incident and corrective action taken

Network Engineer

- Analyzes network traffic for signs of denial of service, distributed denial of service, or other external attacks
- Runs tracing tools such as sniffers, Transmission Control Protocol (TCP) port monitors, and event loggers
- Looks for signs of a firewall breach
- Contacts external Internet service provider for assistance in handling the incident
- Takes action necessary to block traffic from suspected intruder

Security Analyst

- Monitors business applications and services for signs of attack
- Reviews audit logs of mission-critical servers for signs of suspicious activity
- Contacts the Information Technology Operations Center with any information relating to a suspected breach
- Collects pertinent information regarding the incident at the request of the Chief Information Security Officer

Windows / Unix Operating Systems Administrators

- Ensures all service packs and patches are current on mission-critical computers
- Ensures backups are in place for all critical systems
- Examines system logs of critical systems for unusual activity

Internal Audit

Periodically reviews policies and procedures for compliance with information security standards.

Incident Response Team Notification

The Information Technology Service Request Desk will be the central point of contact for reporting computer incidents or intrusions. The Service Request Desk will notify the Chief Information Security Officer (CISO). All computer security incidents must be reported to the CISO. A preliminary analysis of the incident will take place by the CISO and that will determine whether Incident Response Team activation is appropriate.

Types of Incidents

There are many types of computer incidents that may require Incident Response Team activation. Some
examples include:

- Breach of Personal Information
- Denial of Service / Distributed Denial of Service
- Excessive Port Scans
- Firewall Breach
- Virus Outbreak

Breach of Personal Information - Overview

This Incident Response Plan outlines steps our organization will take upon discovery of unauthorized access to personal information on an individual that could result in harm or inconvenience to the individual such as fraud or identity theft. The individual could be either a customer or employee of our organization.

In addition to the internal notification and reporting procedures outlined below, credit card companies require us to immediately report a security breach, and the suspected or confirmed loss or theft of any material or records that contain cardholder data. Specific steps are outlined in Appendix A2. Selected laws and regulations require the organization to follow specified procedures in the event of a breach of personal information as covered in Appendix B1 and Appendix B2.

Personal information is information that is, or can be, about or related to an identifiable individual. It includes any information that can be linked to an

individual or used to directly or indirectly identify an individual. Most information the organization collects about an individual is likely to be considered personal information if it can be attributed to an individual.

For our purposes, personal information is defined as an individual's first name or first initial and last name, in combination with any of the following data:

- Social Security number/Social Insurance Number
- Driver's license number or Identification Card number
- Financial account number, credit or debit card number with personal identification number such as an access code, security codes or password that would permit access to an individual's financial account.
- Home address or e-mail address
- Medical or health information

Definitions of a Security Breach

A security breach is defined as unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by us. Good faith acquisition of personal information by an employee or agent of our company for business purposes is not a breach, provided that the personal information is not used or subject to further unauthorized disclosure.

Requirements

Data owners must identify and document all systems and processes that store or utilize personal information on individuals. Documentation must contain system name, device name, file name, location, database administrator and system administrator (primary and secondary contacts for each). The business area and the IT development group must maintain the contact list of database and system administrators.

Likewise, all authorized users who access or utilize personal information on individuals should be identified and documented. Documentation must contain user name, department, device name (i.e., workstation or server), file name, location, and system administrator (primary and secondary contacts).

Data Owner Responsibilities

Data owners responsible for personal information play an active role in the discovery and reporting of any breach or suspected breach of information on an

individual. In addition, they will serve as a liaison between the company and any third party involved with a privacy breach affecting the organization's data.

All data owners must report any suspected or confirmed breach of personal information on individuals to the CISO immediately upon discovery. This includes notification received from any third party service providers or other business partners with whom the organization shares personal information on individuals. The CISO will notify the appropriate administrator and data owners whenever a breach or suspected breach of personal information on individuals affects their business area.

> Note: For ease of reporting, and to ensure a timely response 24 hours a day, seven days a week, the Service Request Desk will act as a central point of contact for reaching the CISO.

The CISO will determine whether the breach or suspected breach is serious enough to warrant full incident response plan activation (See "Incident Response" section.) The data owner will assist in acquiring information, preserving evidence, and providing additional resources as deemed necessary by the CISO, Legal or other Incident Response Team members throughout the investigation.

Departmental Manager Responsibilities

Departmental managers are responsible for ensuring all employees in their unit are aware of policies and procedures for protecting personal information.

If a breach or suspected breach of personal information occurs in their department, the department manager must notify the Service Request Desk immediately and open an incident report. (See "Incident Response" Section, Information Technology Service Request Desk.)

> Note: Education and awareness communication will be directed to all employees informing them of the proper procedures for reporting a suspected breach of personal information on an individual.

When Notification Is Required

The following incidents may require notification to individuals under contractual commitments or applicable laws and regulations:

> A user (employee, contractor, or third-party provider) has obtained unauthorized access to personal information maintained in either paper or electronic form.

An intruder has broken into database(s) that contain personal information on an individual.

Computer equipment such as a workstation, laptop, CD-ROM, or other electronic media containing personal information on an individual has been lost or stolen.

A department or unit has not properly disposed of records containing personal information on an individual.

A third party service provider has experienced any of the incidents above, affecting the organization's data containing personal information.

The following incidents may not require individual notification under contractual commitments or applicable laws and regulations providing the organization can reasonably conclude after investigation that misuse of the information is unlikely to occur, and appropriate steps are taken to safeguard the interests of affected individuals:

The organization is able to retrieve personal information on an individual that was stolen, and based on our investigation, reasonably concludes that retrieval took place before the information was copied, misused, or transferred to another person who could misuse it.

The organization determines that personal information on an individual was improperly disposed of, but can establish that the information was not retrieved or used before it was properly destroyed.

An intruder accessed files that contain only individuals' names and addresses.

A laptop computer is lost or stolen, but the data is encrypted and may only be accessed with a secure token or similar access device.

Incident Response – Breach of Personal Information

Incident Response Team members must keep accurate notes of all actions taken, by whom, and the exact time and date. Each person involved in the investigation must record his or her own actions.

Information Technology Service Request Desk

Contacts **Office Phone** 503-838-8925 **E-Mail** ucshelpdesk@wou.edu

Primary: Student on Duty
Alternate: Joan Guralnick -- supervisor

1. The IT Service Request Desk will serve as a central point of contact for reporting any suspected or confirmed breach of personal information on an individual.

2. After documenting the facts presented by the caller and verifying that a privacy breach or suspected privacy breach occurred, the IT Service Request Desk will open a Priority Incident Request. **This will begin an automated paging process** to immediately notify the Chief Information Security Officer.

3. The IT Service Request Desk will page the primary and secondary contacts in the Information Security Office. The IT Service Request Desk advises that a breach or suspected breach of personal information on an individual has occurred. After the Information Security Office analyzes the facts and confirms that the incident warrants incident response team activation, the Incident Request will be updated to indicate "**Incident Response Team Activation – Critical Security Problem**".

Chief Information Security Officer

Contacts **Office Phone** 503-838-8927 **E-Mail** kernanb@wou.edu
Primary: Chief Security Officer
Alternate: Information Security Manager

1. When notified by the Service Request Desk, the CISO performs a preliminary analysis of the facts and assess the situation to determine the nature and scope of the incident.
2. Informs the Vice President of Finance and the Security Manager that a possible privacy breach has been reported and provides them an overview of the situation.
3. Contacts the individual who reported the problem.
4. Identifies the systems and type(s) of information affected and determines whether the incident could be a breach, or suspected breach of personal information about an individual. Every breach may not require participation of all Incident Response Team members (e.g., if the breach was a result of hard copy disposal or theft, the investigation may not require the involvement of system administrators, the firewall administrator, and other technical support staff).
5. Reviews the preliminary details with the Security Manager.
6. If a privacy breach affecting personal information is confirmed, Incident Response Team activation is warranted. Contact the Service Request Desk

and advise them to update the Incident Request with “Incident ResponseTeam Activation – Critical Security Problem”.

7. Notify the Public Relations Department of the details of the investigation and breach. Keep them updated on key findings as the investigation proceeds.
8. The Information Security Team is responsible for documenting all details of an incident and facilitating communication to executive management and other auxiliary members as needed.
9. Contact all appropriate database and system administrators to assist in the investigation effort. Direct and coordinate all activities involved with Incident Response Team members in determining the details of the breach.
10. Contact appropriate Incident Response Team members and First-Level Escalation members.
11. Identify and contact the appropriate Data Owner affected by the breach. In coordination with the Vice President of Finance and Administration, the Security Manager and Data Owner, determine additional notification requirements (e.g., Human Resources, external parties).
12. If the breach occurred at a third party location, determine if a legal contract exists. Work with the Business Office, the Security Manager and Data Owner to review contract terms and determine next course of action.
13. Work with the appropriate parties to determine the extent of the potential breach. Identify data stored and compromised on all test, development and production systems and the number of individuals at risk.
14. Determine the type of personal information that is at risk, including but not limited to: Name, Address, Social Security Number/Social Insurance Number, Account number, Cardholder name, Cardholder address, Medical and Health Information
15. If personal information is involved, have the Data Owner determine who might be affected. Coordinate next steps with the Vice President of Finance and Administration, Security Officer and Public Relations (e.g., individual notification procedures).
16. Determine if an intruder has exported, or deleted any personal information data.
17. Determine where and how the breach occurred. Identify the source of compromise, and the timeframe involved. Review the network to identify all compromised or affected systems. Consider e-commerce third party connections, the internal corporate network, test and production environments, virtual private networks, and modem connections. Look at appropriate system and audit logs for each type of system affected. Look at directory and file permissions. Document all internet protocol (IP) addresses, operating systems, domain name system names and other pertinent system information.
18. Take measures to contain and control the incident to prevent further unauthorized access to or use of personal information on individuals, including shutting down particular applications or third party connections, reconfiguring firewalls, changing computer access codes, and modifying

physical access controls. Change all applicable passwords for IDs that have access to personal information, including system processes and authorized users. If it is determined that an authorized user's account was compromised and used by the intruder, disable the account. Do not access or alter the compromised system. Do not turn off the compromised machine. Isolate the system from the network (i.e., unplug cable). Change the wireless network Service Set Identifier (SSID) on the access point (AP) and other authorized devices that may be using the corporate wireless network.

19. Monitor systems and the network for signs of continued intruder access.
20. Preserve all system and audit logs and evidence for law enforcement and potential criminal investigations. Ensure that the format and platform used is suitable for review and analysis by a court of law if needed. Document all actions taken, by whom, and the exact time and date. Each employee involved in the investigation must record his or her own actions. Record all forensic tools used in the investigation. Note: Visa has specific procedures that must be followed for evidence preservation.
21. Notify the Vice President of Finance and Administration as appropriate. Provide a summary of confirmed findings, and of the steps taken to mitigate the situation.
22. If credit cardholder data is involved, follow additional steps outlined under Appendix A. Bankcard companies, specifically Visa and MasterCard, have detailed requirements for reporting security incidents and the suspected or confirmed compromise of cardholder data. Reporting is typically required within 24 hours of compromise.
23. If an internal user (authorized or unauthorized employee, contractor, consultant, etc.) was responsible for the breach, contact the appropriate Human Resource Manager for disciplinary action and possible termination. In the case of contractors, temporaries, or other third-party personnel, ensure discontinuance of the user's service agreement with the company.

Customer Database Owners

Contacts Office Phone **Office Phone**: 503-838-8046 **E-Mail** rossm@wou.edu
Primary: Mike Ross
Alternate: Alex Ichinoe, Michael Ellis

1. If the Data Owners hear of or identifies a privacy breach, contact the Service Request Desk to ensure that the CISO and other primary contacts are notified.
2. The Data Owner will assist the CISO as needed in the investigation.

Process Steps

1. Monitor access to customer database files to identify and alert any attempts to gain unauthorized access. Review appropriate system and audit logs to see if there were access failures prior to or just following the suspected breach. Other log data should provide information on who touched what file and when. If applicable, review security logs on any non-host device involved (e.g., user workstation).
2. Identify individuals whose information may have been compromised. An assumption could be "all" if an entire table or file was compromised.
3. Secure all files and/or tables that have been the subject of unauthorized access or use to prevent further access.
4. Upon request from the CISO, provide a list of affected individuals, including all available contact information (i.e., address, telephone number, email address, etc.)

Credit Payment Systems

Contacts **Office Phone** 503-838-8176 **E-Mail** silbernd@wou.edu

Primary: Darin Silbernagel

1. If notified of a privacy breach by a business area directly, open an incident request with the Service Request Desk to activate the incident response plan for a suspected privacy breach.
2. When notified by the CISO that the privacy breach Incident Response Plan has been activated, perform a preliminary analysis of the facts and assess the situation to determine the nature of incident.
    a. Determine the type of personal information breached.
        i. Current credit card customers
        ii. New credit card applications
        iii. Personal check authorizations
    b. Determine data sources and method of breach (hardcopy, electronic)
    c. Determine method of breach if possible.
    d. Identify additional resources needed to complete investigation
3. Determine the scope of the breach.
    a. Time Frame
    b. Specific Data Elements
    c. Specific Customers
4. Take necessary steps to prevent additional compromise of personal information about individuals.
5. Report all findings to the Incident Response Plan Team.
6. Within 24 hours of notification of an account number compromise, contact the appropriate card companies:
    a. Visa Fraud Control Group
    b. MasterCard Compromised Account Team
    c. Discover Fraud Prevention
    d. American Express Merchant Services

7. Act as liaison between the card companies, CISO, and Legal.
8. Ensure credit card companies' specific requirements for reporting suspected or confirmed breaches of cardholder data are followed. For detailed requirements, see Appendix A2.

Legal

Contacts	**Office Phone**	**E-Mail**
Primary:		
Alternate:		

1. Monitor relevant privacy-related legislation, provide input as appropriate, and communicate to our clients the effect that any enacted legislation may have on them.
2. Be cognizant of major contracts which the organization enters that may have an impact or effect on our customers, employees, and other data.
3. Be aware of other companies' privacy policies that may affect our organization and affiliates.

When a Privacy Breach Occurs:

1. After confirmation that a breach of personal information on individuals has occurred, notify the Chief Legal Counsel
2. Coordinate activities between business area and other departments (e.g., Human Resources, if necessary).
3. If necessary, notify the appropriate authorities (e.g., Federal Trade Commission (FTC)/RCMP, the relevant privacy commissioners office, etc.)
4. Coordinate with Public Relations on the timing and content of notification to individuals.
5. If the CISO determines that the breach warrants law enforcement involvement, any notification to individuals may be delayed if law enforcement determines the notification will impede a criminal investigation. Notification will take place after law enforcement determines that it will not compromise the investigation.
6. Notification to individuals may be delayed until the CISO is assured that necessary measures have been taken to determine the scope of the breach and properly investigated.
7. Follow approved procedures for any notice of unauthorized access to personal information about individuals.
8. Notification to individuals should be timely, conspicuous, and delivered in any manner that will ensure the individual receives it. Notice should be consistent with laws and regulations the organization is subject to.

Appropriate delivery methods include:

Written notice
Email notice

Substitute notice

- Conspicuous posting of the notice on the Online Sales website.
- Notification to major media

Items to consider including in notification to individuals:

A general description of the incident and information to assist individuals in mitigating potential harm, including a customer service number, steps individuals can take to obtain and review their credit reports and to file fraud alerts with nationwide credit reporting agencies, and sources of information designed to assist individuals in protecting against identity theft.

Remind individuals of the need to remain vigilant over the next 12 to 24 months and to promptly report incidents of suspected identity theft. Inform each individual about the availability of the Federal Trade Commission's (FTC's) online guidance regarding measures to protect against identity theft, and encourage the individual to report any suspected incidents of identity theft to the FTC. Provide the FTC's website address and telephone number for the purposes of obtaining the guidance and reporting suspected incidents of identity theft. At the time of this document's publication, the website address is http://www.ftc.gov/idtheft. The toll-free number for the identity theft hotline is 1-877-IDTHEFT. Inform each individual about the availability of the Canadian online guidance regarding measures to protect against identity theft. At the time of this document's publication, the website address for Canadian guidance is located on the Industry Canada website at http://strategis.ic.gc.ca/epic/internet/incmc-cmc.nsf/en/fe00084e.html and the RCMP website at http://www.rcmp-grc.gc.ca/scams/identity_theft_e.htm . Encourage the individual to report any suspected incidents of identity theft to the local law enforcement agency

Human Resources

Contacts **Office Phone** 503-838-8552 **E-Mail** vanderj@wou.edu
Primary: Judy Vanderburg
Alternate: Alice Sprague

1. If notified of a privacy breach affecting employee personal information, open an incident request with the IT Service Request Desk to activate the Incident Response Plan for suspected privacy breach.
2. When notified by the Information Security Office that the privacy breach incident response plan has been activated for a breach of information on an individual, perform a preliminary analysis of the facts and assess the situation to determine the nature of the incident.

3. Work with the IT Service Request Desk, CISO and business area to identify the extent of the breach.
4. If appropriate, notify the business area that a breach has been reported and is under investigation.
5. Work with the business area to ensure there is no further exposure to privacy breaches.
6. Work with the CISO and Legal Department to determine if the incident warrants further action.

Network Architecture

Contacts **Office Phone** 503-559-0707 **E-Mail** knabet@wou.edu
Primary: Travis Knabe
Alternate: Paul Lambert

1. When notified by the CISO that the privacy breach Incident Response Plan is activated, provide assistance as determined by the details of the potential breach.
2. Review firewall logs for correlating evidence of unauthorized access.
3. Implement firewall rules as needed to close any exposures identified during the investigation.

Public Relations

Contacts **Office Phone** 503-838—8349 **E-Mail** visuanod@wou.edu
Primary: Denise Visuano
Alternate: Lisa Pullman

Ongoing:

1. Monitor consumer privacy issues and practices of other companies.
2. Monitor consumer privacy breaches of other companies and how they respond.
3. Keep generic/situational talking points current.

When Privacy Breach Occurs:

1. After confirmation that a breach of personal information about individuals has occurred, notify the Public Relations Director.
2. Coordinate with the Vice President of Finance and Administration and Legal on the timing, content and method of notification. Prepare and issue press release or statement, if needed.

Vehicles for communicating include:

a. News wire services

b. Online Sales web site – Post statement on home page or conspicuous location of web site.
c. Internal Website – If appropriate for breach of employee information
d. E-mail
e. News conference – If privacy breach should reach a national and/or crisis level, coordinate brief news conference at headquarters or appropriate location.
i. Appoint appropriate spokesperson
ii. Prepare statement and, if necessary, potential Q & A.
iii. Coach spokesperson on statement and potential Q & A.
iv. Invite select media to attend and cover organization's proactive message.
v. Use conference as a platform for communicating who the breach involves, what the organization is doing to correct breach, how it happened and the organization's apology but reassurance of its privacy policies

3. Prepare appropriate response to media, customer, and/or employee; and have the CPO and Legal Department approve prior to distribution.
4. Proactively respond to media inquiries, if necessary.
5. Monitor media coverage and circulate accordingly.

Appendix A1 – Payment Card Industry Data Security Standard

Background:

The PCI Data Security Standard, published in January 2005, was the result of a joint initiative by VISA,
MasterCard, American Express, Discover, Diners Club, and JCB to create a single security standard for storing and
transmitting sensitive customer information.

Requirements

The PCI Data Security Standard applies to all members, merchants, and service providers that store, process or
transmit cardholder data. The standard consists of the following 12 requirements:

1. Install and maintain a firewall configuration to protect data;
2. Do not use vendor-supplied defaults for system passwords and other security parameters;
3. Protect stored data;
4. Encrypt transmission of cardholder data and sensitive information across public networks;
5. Use and regularly update anti-virus software;
6. Develop and maintain secure systems and applications;

7. Restrict access to data by business need to know;
8. Assign a unique ID to each person with computer access;
9. Restrict physical access to cardholder data;
10. Track and monitor all access to network resources and cardholder data;
11. Regularly test security systems and processes;
12. Maintain a policy that addresses information security.

Included in Requirement 12 is the implementation of an Incident Response Plan

For a complete copy of the Payment Card Industry Data Security Standard manual, see https://sdp.mastercardintl.com/pdf/PCD_Manual.pdf

Compliance

Failure to comply with the new standards could result in a merchant being subjected to a fine or the loss of
access to the credit card networks.

On-site reviews

Merchants, including e-commerce merchants, with more than 6 million total transactions annually, or merchants who have already experienced an account compromise are required to have an onsite review carried out annually. Any other merchant can also be subjected to an onsite review at the discretion of the payment card institution. The review can be carried out either by the merchant's internal audit function or an independent assessor acceptable to the payment card institution.

Self-Assessments

Merchants with e-commerce transactions between 20,000 and 6 million total transactions annually are required to
carry out a Self Assessment annually. For all other merchants, the credit card companies recommend that the
Self-Assessment be carried out on an annual basis. For a copy of the Payment Card Industry Self-Assessment
Questionnaire, see
https://sdp.mastercardintl.com/pdf/758_PCI_Self_Assmnt_Qust.pdf.

PCI Data Security Standard Incident Response Plan Details

Incident Response Plan

12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.

12.9.1 Create an incident response plan to be used in the event of system compromise. Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (for example, informing Acquirers and credit card associations).
12.9.2 Test the plan at least annually.
12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.
12.9.4 Provide appropriate training to staff with security breach response responsibilities.
12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.
12.9.6 Have a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

Appendix A2 – Cardholder Requirements

Specific requirements for reporting suspected or confirmed breaches of cardholder data.

MasterCard Specific Steps:

1. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100. In Canada, notify the MasterCard®
Global Service™ emergency services via telephone at 1-800-622-2774.
2. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail, to compromised_account_team@mastercard.com.
3. Provide the MasterCard Merchant Fraud Control Department with the complete list of all knowncompromised account numbers.
4. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).
5. Provide weekly written status reports to MasterCard, addressing open questions and issues, until the audit is complete to the satisfaction of MasterCard.
6. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
7. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs
2. Distribute the account number data to its respective issuers.

Visa U.S.A. Specific Steps

(Excerpted from Visa U.S.A. Cardholder Information Security Program (CISP), What To Do If Compromised, 3/8/2004)

Refer to documentation online at
http://www.usa.visa.com/media/business/cisp/What_To_Do_If_Compromised.pdf

In the event of a security breach, the **Visa U.S.A. Operating Regulations** require entities to immediately report the breach and the suspected or confirmed loss or theft of any material or records that contain cardholder data. Entities must demonstrate the ability to prevent future loss or theft of account information, consistent with the requirements of the Visa U.S.A. Cardholder Information Security Program. If Visa U.S.A. determines that an entity has been deficient or negligent in securely maintaining account information or reporting or investigating the loss of this information, Visa U.S.A. may require immediate corrective action.

If a merchant or its agent does not comply with the security requirements or fails to rectify a security issue, Visa may:

- Fine the Member Bank
- Impose restrictions on the merchant or its agent, or
- Permanently prohibit the merchant or its agent from participating in Visa programs.

Visa has provided the following step-by-step guidelines to assist an entity in the event of a compromise. In addition to the following, Visa may require additional investigation. This includes, but is not limited to, providing access to premises and all pertinent records.

1 Visa U.S.A. November 2003 Operating Regulations 2.3.F.5
2 Visa U.S.A. November 2003 Operating Regulations 2.3.F.7
3 Visa U.S.A. November 2003 Operating Regulations 2.3.F.3, 2.3.F.4, 2.3.F.5, 2.3.F.6

Steps and Requirements for Compromised Entities

1. Immediately contain and limit the exposure.

To prevent further loss of data, conduct a thorough investigation of the suspected or confirmed loss or theft of account information within 24 hours of the compromise. To facilitate the investigation:

- 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 Service Set Identifier (SSID) on the access point and other machines that may be using this connection (with the exception of any systems believed to becompromised).
- Be on HIGH alert and monitor all Visa systems.

2. Alert all necessary parties, including:

- Internal information security group and Incident Response Team, if applicable
- Legal department
- Merchant bank
- Visa Fraud Control Group at (650) 432-2978 in the U.S. or Visa Canada Risk Management at 416-860-3090 in Canada.
- Local FBI Office U.S. Secret Service, or RCMP local detachment, if Visa payment data is compromised.

3. Provide the compromised Visa account to Visa Fraud Control Group at (650) 432-2978 within 24 hours or Visa
Canada Risk Management at 416-860-3090 in Canada.

- Account numbers must be securely sent to Visa as instructed by Visa. It is critical that all potentially
- compromised accounts are provided. Visa will distribute the compromised Visa account numbers to
- Issuers and ensure the confidentiality of entity and non-public information.

4. Requirements for Compromised Entities

- All merchant banks must:
  - Within 48 hours of the reported compromise, proof of Cardholder Information Security Program compliance must be provided to Visa.
  - Provide an incident report document to Visa within four business days of the reported compromise

- Depending on the level of risk and data elements obtained the following must be completed
- within four days of the reported compromise:
  Undergo an independent forensic review
  A compliance questionnaire and vulnerability scan upon Visa's discretion

Steps for Merchant Banks

1. Contact Visa USA Fraud Control Group immediately at (650)432-2978), or if you are a merchant in Canada contact Visa Canada Risk Management at 416-860-3090.
2. Participate in all discussions with the compromised entity and Visa USA, or if you are a merchant in Canada with Visa Canada.
3. Engage in a Visa approved security assessor to perform the forensic investigation
4. Obtain information about compromise from the entity
5. Determine if compromise has been contained
6. Determine if an independent security firm has been engaged by the entity
7. Provide the number of compromised Visa accounts to Visa Fraud Control Group or Visa Canada Risk Management within 24 hours
8. Inform Visa of investigation status within 48 hours
9. Complete steps necessary to bring entity into compliance with CISP according to timeframes described in "What to do if Compromised"
10. Ensure that entity has taken steps necessary to prevent future loss or theft of account information, consistent with the requirements of the Visa USA Cardholder Information Security Program

Forensic Investigation Guidelines

Entity must initiate investigation of the suspected or confirmed loss or theft of account information within 24 hours of compromise.

The following must be included as part of the forensic investigation:

1. Determine cardholder information at risk.
   a. Number of accounts at risk, identify those stored and compromised on all test, development, and production systems
   b. Type of account information at risk
   c. Account number
   d. Expiration date
   e. Cardholder name
   f. Cardholder address
   g. CVV2
   h. Track 1 and Track 2
   i. Any data exported by intruder
2. Perform incident validation and assessment.

a. Establish how compromise occurred
b. Identify the source of compromise
c. Determine timeframe of compromise
d. Review entire network to identify all compromised or affected systems, considering the e-commerce, corporate, test, development, and production environments as well as VPN, modem, DSL and cable modem connections, and any third-party connections.
e. Determine if compromise has been contained.

3. Check all potential database locations to ensure that CVV2, Track 1 and Track 2 data are not stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments data on software engineers' machines, etc.).
4. If applicable, review VisaNet endpoint security and determine risk.
5. Preserve all potential electronic evidence on a platform suitable for review and analysis by a court of law if needed.
6. Perform remote vulnerability scan of entity's Internet facing site(s).

CVV2 is an authentication process established by credit card companies to further efforts towards reducing fraud for Internet transactions. It consists of requiring a card holder to enter the CVV2 number at transaction time to verify that the card is on hand. This number is printed on MasterCard & Visa cards in the signature area of the back of the card. (It is the last 3 digits AFTER the credit card number in the signature area of the card).

Track 1 is a "track" of information on a credit card that has a 79-character alphanumeric field for information. Normally a credit card number, expiration date and customer name are contained on track 1. Track 2 is a "track" of information on a credit card that has a 40-character field for information. Normally a credit card number and expiration date are contained on track 2.

Visa Incident Report Template

This report must be provided to Visa within 14 days after initial report of incident to Visa. The following report content and standards must be followed when completing the incident report. Incident report must be securely distributed to Visa and Merchant Bank. Visa will classify the report as "Visa Secret"

I. Executive Summary
a. Include overview of the incident
b. Include Risk Level (High, Medium, Low)
c. Determine if compromise has been contained

II. Background

III. Initial Analysis

IV. Investigative Procedures
    a. Include forensic tools used during investigation
V. Findings
    a. Number of accounts at risk, identify those stored and compromised
    b. Type of account information at risk
    c. Identify ALL systems analyzed. Include the following:
        i. Domain Name System (DNS) names
        ii. Internet Protocol (IP) addresses
        iii. Operating System (OS) version
        iv. Function of system(s)
    d. Identify ALL compromised systems. Include the following:
        i. DNS names
        ii. IP addresses
        iii. OS version
        iv. Function of system(s)
    e. Timeframe of compromise
    f. Any data exported by intruder
    g. Established how and source of compromise
    h. Check all potential database locations to ensure that no CVV2, Track 1 or Track 2 data is stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments data on software engineers' machines, etc.).
    i. If applicable, review VisaNet endpoint security and determine risk.
VI. Compromised Entity Action
VII. Recommendations
VIII. Contact(s) at entity and security assessor performing investigation

* This classification applies to the most sensitive business information, which is intended for use within Visa. Its unauthorized disclosure could seriously and adversely impact Visa, its employees, member banks, business partners, and/or the Brand.

Discover Card Specific Steps:

1. Within 24 hours of an account compromise event, notify Discover Fraud Prevention at (800) 347-3102.
2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances.
3. Prepare a list of all known compromised account numbers.
4. Obtain additional specific requirements from Discover Card.

American Express Specific Steps:

1. Within 24 hours of an account compromise event, notify American Express Merchant Services at (800) 528-5200 in the U.S. and (800) 876-9786 (Option 2) in Canada.
2. Prepare a detailed written statement of fact about the account compromise including the contributing
circumstances.
3. Prepare a list of all known compromised account numbers.
4. Obtain additional specific requirements from American Express.

Appendix B1 – U.S. Privacy Legislation

The following are selected United States. laws and regulations relating to the breach of personal information about an individual. This Appendix should not be considered a complete list.

California Civil Code 1798.82 (Senate Bill 1386)

On July 1, 2003, California Senate Bill 1386 became Civil Code 1798.82. The law requires companies that do business in California and own or license computerized data containing unencrypted personal information, to notify California residents of any security breach of their unencrypted personal information where the information was, or is reasonably believed to have been, acquired by an unauthorized person.

Note: Be prepared to identify and separate (if necessary) California residents from other records in databases containing personal information on individuals.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The primary focus of HIPAA was to improve the health insurance accessibility to people changing employers or leaving the workforce. It also addressed issues relating to electronic transmission of health-related data in Title II, Subtitle F of the Act entitled “Administrative Simplification”. The administrative simplification provisionsinclude four key areas:

- •National standards for electronic transmission
- •Unique health identifiers for providers, employers, health plans and individuals
- •Security Standards
- •Privacy Standards

The HIPAA Security Standards require a covered entity to implement policies and procedures to ensure:

•the confidentiality, integrity, and availability of all electronic protected health information
•protect against any reasonably anticipated threats or hazards to the security of such information
•protect against any reasonably anticipated uses or disclosures that are not permitted

Within this context, HIPAA requires a covered entity to implement policies and procedures to address security incidents. A security incident means the attempted or successful unauthorized access, use disclosure, modification, or destruction of information or interference with system operations in an information system. Response and reporting implementation requirements include identifying and responding to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

The HIPAA security standards were effective on April 21, 2003. The compliance date for covered entities is by April 21, 2005 and April 21, 2006 for small health plans.

Gramm-Leach-Bliley Act (GLBA)

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions. The GLB Act gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule and the Safeguards Rule. These two regulations apply to "financial institutions", which include not only banks, securities firms and insurance companies, but also companies providing many other types of financial products and services to consumers. Among these services are lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, providing residential real estate settlement services, collecting consumer debts and an array of other activities. Such non-traditional "financial institutions" are regulated by the FTC. The Financial Privacy Rule governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies, whether or not they are financial institutions, who receive such information.

The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their

own customers, but also to financial institutions – such as credit reporting agencies – that receive customer information from other financial institutions. The Rule requires the organization to consider all areas of its operations including employee management and training; information systems; and managing system failures. Effective security includes the prevention, detection and response to attacks, intrusions or other system failures. Specific considerations include maintaining up-to-date and appropriate programs and controls by following a written contingency plan to address any breaches of nonpublic personal information and notify customers if their personal information is subject to loss, damage, or unauthorized access. The Pretexting provisions of the GLB Act protect consumers from individuals and companies that obtain their personal financial information under false pretenses, a practice known as "pretexting." The Privacy Rule took effect on November 13, 2000 and compliance on July 1, 2001. The Safeguard Rule was effective on May 23, 2003.

Appendix B2 – Canadian Privacy Legislation

The following are selected Canadian laws and regulations relating to personal information about an individual. This Appendix should not be considered a complete list.

Canadian legislation does not state specifically that an organization is required to take action when there is a breach of privacy. For example, it does require an organization to advise the Office of the Privacy Commissioner of Canada or the appropriate Provincial Commissioner, as well as clients, patients and/or employees of the organization. However, it is considered good privacy practice, and it is in the spirit of the legislation to do so. "Best practices" related to the protection of personal information by organizations are continually evolving within each jurisdiction. It is recommended that organizations consult the resources found on the Commissioners' web sites. For details of a landmark privacy incident and example best practices, see "A Canadian Privacy Breach" and "Evolving Best Practices in Canada" later in this Appendix.

Personal Information Protection and Electronic Documents Act (Canada)

The Federal Personal Information Protection and Electronic Documents Act (PIPEDA) was introduced in 2001 to defend against the abuse of person-specific information. PIPEDA applied first to federally regulated businesses such as banking, telecommunications and transportation. Starting in 2004, PIPEDA encompasses all Canada's private sector. Part 1 of PIPEDA seeks a balance between an individual's right to the privacy of personal information with the need of organizations to collect, use or disclose personal information for legitimate business purposes. PIPEDA sets out the rules and principles

that organizations must follow in the collection, use and disclosure of personal information. Schedule 1, Principle 4.7 of PIPEDA states the following with respect to the safeguarding of personal information: "Personal information shall be protected by security safeguards appropriate to the sensitivity of the information."

4.7.1 "The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying use or modification Organizations shall protect personal information regardless of the format in which it is held".
4.7.2 "The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of s orage. More sensitive information should be safeguarded by a higher level of protection."
4.7.3 "The methods of protection should include
a) physical measures, for example, locked filing cabinets and restric ed access to offices;
b) organizational measures, for example, security clearances and limiting access on a 'need-to-know' basis; and
c) technological measures, for example the use of passwords and encryption."

An assessment of adequate information security under PIPEDA depends upon the sensitivity of the information. Security standards are constantly evolving and the task for organizations of maintaining adequate security is an ongoing one. Principle 4.7 of PIPEDA would apply with especial vigor in the event of a privacy breach and subsequent complaint. Organizations would be judged poorly if they did not keep up with industry standards, for example a failure to deploy SSL for online commerce transactions. In the case of a large organization, particularly those holding sensitive information, it is expected that threat and risk assessments and security audits be regularly performed.

For a comprehensive list of privacy legislation in Canada, see www.PrivacyInfo.ca maintained by Professor Michael Geist of the University of Ottawa.

Part 2 of PIPEDA provides a framework by which federal statutes and regulations may be adjusted to accommodate electronic alternatives to paper-based means of communication. It also describes the characteristics of technologies and processes related to secure electronic signatures. This part of PIPEDA applies to government agencies and is administered by the Treasury Board Secretariat. Personal information that flows across provincial or national borders will be subject to PIPEDA and PIPEDA will continue to apply within a province to the activities of federal works, undertakings and

businesses that are under federal jurisdiction such as banking, broadcasting, telecommunications and transportation.

Personal Information Protection Act (Alberta)

Alberta has introduced its own provincial privacy legislation. Bill 44 - Personal Information Protection Act (PIPA) received Royal Assent on December 4, 2003 and the Personal Information Protection Act Regulation was enacted on December 10, 2003. PIPA has been deemed to be substantially similar to PIPEDA and therefore takes precedence over PIPEDA for the private sector organizations conducting commercial activity in Alberta. However, PIPA does not apply to health information as defined in the Alberta Health Information Act (HIA) where that information is collected, used or disclosed by an organization for health care purposes including health research and management of the health care system. PIPA does apply to employee personal information inclusive of the health information contained in the employer/employee relationship.

Part 3, Division 2, Section 34 of PIPA states the following with respect to the protection of personal information: ”An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.”

Personal Information Protection Act (British Columbia)

British Columbia has introduced its own provincial privacy legislation. Bill 38 - Personal Information Protection Act (PIPA) and the Personal Information Protection Act Regulation was effective January 1, 2004 and declared substantially similar to PIPEDA by the Federal Cabinet on October 25, 2004. PIPA therefore takes precedence over PIPEDA for the private sector organizations conducting commercial activity solely in British Columbia.

Part 3, Section 5 of PIPA states the following with respect to policies and practices related to the protection of
personal information:

”An organization must
a) develop and follow policies and practices that are necessary for the organization to meet the obligation under this Act,
b) develop a process to respond to complaints that may arise respecting the application of this Act, and
c) make information available on request about (i) the policies and practices referred to in paragraph (a), and (ii) the complaint process referred to in paragraph (b)“.

Part 9, Section 34 of PIPA states the following with respect to the protection of personal information:

> “An organiza on must protect personal information in its custody or under its control by making reasonable security arrangements to p event unau horized access, collection, use, disclosure, copying modification or disposal or similar risks ”

A Canadian Privacy Breach

In January 2003 a hard disk drive, containing personal information was stolen from ISM Canada by an ISM employee compromising over one million Canadians. This theft impacted the Saskatchewan Department of Finance, Co-operators Life Insurance, SaskPower Energy and Investors Group. However, these organizations were quick to notify their customers and warn them of the potential privacy breach to personal information. The costs for dealing with this breach are estimated to be somewhere in the neighborhood of fifty million dollars for issuing notices and letters, responding to an increase in telephone calls from worried customers, internal investigations and reviews and updates of the privacy policies and procedures for the organizations affected. There is also the cost related to damaged reputation, company image and credibility, and potential loss of business, which has yet to clearly identify a price tag. The organizations concerned appear to have handled the breach and situation fairly well and undertook to review the management and handling of information under their control and make improvements where needed.

Evolving Best Practices in Canada

- Organizations should have a comprehensive inventory of the personal information under their control. This includes information held in any form and media; e.g. hard drives, magnetic tapes, magnetic disks, optical storage media, paper as well as information held at off-site storage facilities.
- Organizations should keep an updated inventory of all hardware.
- Review all contracts and agreements with third parties, e.g. outsourcing organizations, to ensure appropriate security and safeguards are identified and included. Ensure that the third party is aware of the organization’s privacy policies and position and they acknowledge and agree to the same or higher level of protection over the personal information entrusted to them.
- Include the “right to audit” or conduct regular reviews of the third parties operations, which impact the organizations assets such as customer personal information.
- Organizations should have an incident response and handling process and procedures in place. The procedures should include identification and notification to clients who may be impacted by a loss or disclosure of personal information.

• Organizations should have communication and training plans and procedures in place to inform employees what they need to do in the case of a breach.
• Organizations should inform the appropriate Privacy Commissioner (Provincial and/or Federal) as soon as possible about the breach.
• Organizations should have a process in place for dealing with the media.

Organizations should have a process in place for reviewing the existing information management and handling processes and procedures in order to identify the gaps and required enhancements and changes to correct where the breach occurred. This should include security over the hardware that houses the personal information. Consideration should also be given to increased safeguards for “sensitive” personal information, i.e. financial and medical.