

Incident Response Plan

Template For
Breach of Personal Information



Notice to Readers

Incident Response Plan — Template for Breach of Personal Information does not represent an official position of the American Institute of Certified Public Accountants, and it is distributed with the understanding that the author and the publisher are not rendering accounting, or other professional services in the publication. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Copyright © 2004 by

American Institute of Certified Public Accountants, Inc.

New York, NY 10036-8775

All rights reserved.

Permission is hereby granted to you for copying, downloading, tailoring, and disseminating the Incident Response Plan for internal use within your own company, providing that you fully acknowledge the AICPA source, including media form, title, author (AICPA), copyright date, the extent to which you may have modified the original text, and also that you do not directly or indirectly sell the reproductions.

It is imperative that all of your reproductions include the italicized AICPA copyright notice that appears elsewhere on this page.

To apply for permission to reproduce any part of this work for commercial purposes, you must complete and submit the AICPA Copyright Permission Request Form, which is currently available on the AICPA Web site at <https://util.aicpa.org/feedback/copyright.htm>

Acknowledgments

The AICPA expresses appreciation to everyone who provided assistance in the development of the Incident Response Plan.

AICPA/CICA Privacy Task Force

Chair

Everett C. Johnson, CPA
Deloitte & Touche LLP (retired)

Vice Chair

Kenneth D. Askelson, CPA/CITP, CIA

Mary Grace Davenport, CPA
PricewaterhouseCoopers

Eric K. Federing
KPMG LLP

Marilyn Greenstein, Ph.D.
Accounting & Information Systems
Arizona State University—West

Don H. Hansen, CPA
Moss Adams LLP

Philip M. Juravel, CPA
Juravel & Company, LLC

Sagi Leizerov, Ph.D.
Ernst & Young LLP

Doron M. Rotman, CPA (Israel), CISA, CIA, CISM
KPMG LLP

Kerry Shackelford, CPA
KLS Consulting LLC

Donald E. Sheehy, CA, CISA
Deloitte & Touche LLP

AICPA Staff

Nancy A. Cohen, CPA, Senior Technical Manager, Business Reporting,
Assurance and Advisory Services

Paul Herring, Director, Business Reporting, Assurance and Advisory Services

CICA Staff

Bryan Walker, Principal, Assurance Services Development

A special word of appreciation goes to Kenneth D. Askelson, CPA/CITP, CIA,
for his dedication to this project.

Introduction

Maintaining the privacy and protection of customers' and employees' personal information is a risk management issue for all organizations. Research continues to show that consumers have widespread distrust of many organizations business practices, including how they collect, use and retain personal information.¹ The increase in identity theft is a concern for all of us. Business systems and processes are increasingly more complex and sophisticated and more and more personal information continues to be collected. Laws and regulations continue to place requirements on businesses for the protection of personal information.

To help organizations address these issues and implement good privacy practices, the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) introduced the AICPA/CICA Privacy Framework for protecting personal information. The Framework can be used by CPAs/CAs² (both in industry and public practice) to guide and assist the organizations they serve in implementing good privacy programs. It incorporates concepts from significant domestic and international privacy laws, regulations and guidelines. You can download the Framework at www.aicpa.org/privacy

Headline articles have demonstrated that the privacy and protection of personal information is not absolute. Many organizations have already had to deal with numerous challenges that must be confronted when a breach of personal information occurs. In addition, some laws and regulations require organizations to have an incident response plan in place to address a breach of personal information (refer to Appendix B).

Is your organization prepared to effectively handle this type of event?

This Incident Response Plan Template can be used to help you design, develop or adapt your own plan and better prepare you for handling a breach of personal information within your organization. The template is only an illustration of what an Incident Response Plan may contain; it is not intended to be a complete list of items to consider nor a Plan that fits your organization's specific environment.

AICPA/CICA Privacy Task Force

¹ 2004 Yankelovich Survey - *Consumer Confidence in Crisis: Rebuilding the Bonds of Trust*.

² CPA/CA refers to a certified public accountant in the United States, and a chartered accountant in Canada, or their equivalent in other countries, whether in public practice, private industry, government or education.

Table of Contents

Incident Response Plan	6
Incident Response Team	6
Incident Response Team Members	6
Incident Response Team Roles and Responsibilities	7
Incident Response Team Notification	8
Types of Incidents	9
Breach of Personal Information - Overview	9
Definitions of a Security Breach	9
Requirements	10
Data Owner Responsibilities	10
Location Manager Responsibilities	10
When Notification Is Required	11
Incident Response – Breach of Personal Information	12
Information Technology Operations Center	12
Chief Information Security Officer	12
Customer Database Owners	14
Online Sales Department	15
Credit Payment Systems	16
Legal	17
Human Resources	18

Network Architecture	19
Public Relations	19
Location Manager	20
Appendix A	21
MasterCard Specific Steps	21
Visa U.S.A. Specific Steps	21
Discover Card Specific Steps	26
American Express Specific Steps	26
Appendix B	27
California Civil Code 1798.82 (Senate Bill 1386)	27
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	27
Gramm-Leach-Bliley Act (GLBA)	28
Appendix C	29
Escalation Members (VP Level of Management)	29
Auxiliary Members (as needed)	29
External Contacts (as needed)	29
Notification Order	30
Escalation Member Notification List	31

Incident Response Plan

An Incident Response Plan is documented to provide a well-defined, organized approach for handling any potential threat to computers and data, as well as taking appropriate action when the source of the intrusion or incident at a third party is traced back to the organization. The Plan 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

An 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 areas will have a primary and alternate member:

- Information Security Office (ISO)
- Information Technology Operations Center (ITOC)
- Information Privacy Office (IPO)
- Network Architecture
- Operating System Architecture
- Business Applications
- Online Sales
- Internal Auditing

Incident Response Team Roles and Responsibilities

Information Security Office

- 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

Information Technology Operations Center

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

Information Privacy Office

- Coordinates activities with the Information Security Office
- Documents the types of personal information that may have been breached
- Provides guidance throughout the investigation on issues relating to privacy of customer and employee personal information
- Assists in developing appropriate communication to impacted parties
- Assesses the need to change privacy policies, procedures, and/or practices as a result of the breach

Network Architecture

- 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

Operating Systems Architecture

- 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

Business Applications

- 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 Office

Online Sales

- 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 Office

Internal Auditing

- Reviews systems to ensure compliance with information security policy and controls
- Performs appropriate audit test work to ensure mission-critical systems are current with service packs and patches
- Reports any system control gaps to management for corrective action

Incident Response Team Notification

The Information Technology Operations Center will be the central point of contact for reporting computer incidents or intrusions. The Operations Center 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 A**. Selected laws and regulations require the organization to follow specified procedures in the event of a breach of personal information as covered in **Appendix B**.

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
- 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).

* If the individual is a Visa U.S.A., MasterCard, American Express, or Discover cardholder, follow additional procedures outlined in the Appendix A.

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 Chief Privacy Officer (CPO) 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 Information Technology Operations Center will act as a central point of contact for reaching the CISO and CPO.

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 CPO, CISO, Legal or other Incident Response Team members throughout the investigation.

Location Manager Responsibilities

Location 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 location, the location manager must notify the Information Technology Operations Center immediately and open an incident report. (See "Incident Response" Section, Information Technology Operations Center).

*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 Operations Center

<u>Contacts</u>	<u>Office Phone</u>	<u>Pager</u>	<u>E-Mail</u>
Primary:	_____	_____	_____
Alternate:	_____	_____	_____

1. The ITOC will serve as a central point of contact for reporting any suspected or confirmed breach of personal information on an individual.
ITOC contact information: (800) XXX-XXXX
2. After documenting the facts presented by the caller and verifying that a privacy breach or suspected privacy breach occurred, the ITOC will open a Priority Incident Request. This will begin an automated paging process to immediately notify the Chief Information Security Officer.
3. The ITOC will page the primary and secondary contacts in the Information Security Office. The ITOC 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

<u>Contacts</u>	<u>Office Phone</u>	<u>Pager</u>	<u>E-Mail</u>
Primary:			
Chief Security Officer	_____	_____	_____
Alternate:			
Information Security Manager	_____	_____	_____

1. When notified by the ITOC, the CISO performs a preliminary analysis of the facts and assesses the situation to determine the nature and scope of the incident.
2. Informs the Legal Department and the Chief Privacy Officer 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 Legal Department and the Chief Privacy Office.
6. If a privacy breach affecting personal information is confirmed, Incident Response Team activation is warranted. Contact the ITOC and advise them to update the Incident Request with “**Incident Response Team 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 Office 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 Legal Department, Information Privacy Office 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 Legal Department, Information Privacy Office 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, 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 Legal Department, Information Privacy Office 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 (VPNs), and modem connections. Look at appropriate system and audit logs for each type of system affected.
 - 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 CPO in coordination with the Legal Department 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

<i>IT Customer Database Contacts</i>	<i>Office Phone</i>	<i>Pager</i>	<i>E-Mail</i>
Primary: _____	_____	_____	_____
Alternate: _____	_____	_____	_____
<i>Data Owner Contacts</i>	<i>Office Phone</i>	<i>Pager</i>	<i>E-Mail</i>
Primary: _____	_____	_____	_____
Alternate: _____	_____	_____	_____

Notification Steps

1. If the IT Customer Database group or Data Owners hear of or identifies a privacy breach, contact the ITOC to ensure that the CISO and other primary contacts are notified.
2. The IT Customer Database group and Data Owner will assist the CISO as needed in the investigation.
3. IT Customer Database contact notifies the IT Contractor Liaison (if warranted).

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, e-mail address, etc.).

Online Sales Department

<u>Contacts</u>	<u>Office Phone</u>	<u>Pager</u>	<u>E-Mail</u>
Primary: _____	_____	_____	_____
Alternate: _____	_____	_____	_____

1. Online Sales System Support will serve as the primary contact for the Online Sales Department. Online System Support is available 24/7 and should be contacted using the following pager numbers:
Primary: _____
Backup: _____
2. When notified by Information Security Office that the privacy breach incident response plan has been activated, Online System Support will collect pertinent information regarding the incident from the CISO and determine the appropriate systems in which to begin inspecting. If notification of a possible breach of information on an individual comes from any other source (a customer, an individual outside the organization), refer the caller to the ITOC to begin the official incident response notification process.

3. Online System Support, using the information gathered from the sources listed in item 2, will begin by inspecting Web server logs and operating system logs (e.g., Windows event logs, UNIX syslogs). They will look for suspicious activity that may suggest the application interface to processing systems was compromised. From there they will look at the operating system level to ensure that servers were not compromised and used as a pass-through into the backend network. This will also be done by checking the NT Event logs, looking at the network for abnormal connections, inspecting the NT registry for non-standard entries, looking at the running process list for any abnormal executing processes, etc.

4. Due to the sensitivity of a security breach, Online Systems Support will only notify and communicate with the following management/groups:

Chief Information Security Officer: phone number

Primary Business Contact: phone number

Online Sales Contact: phone number

Online System Support will keep these persons informed until it can be confirmed or denied that the Online Sales systems were compromised.

Credit Payment Systems

<i>Contacts</i>	<i>Office Phone</i>	<i>Pager</i>	<i>E-Mail</i>
Primary: _____	_____	_____	_____
Alternate: _____	_____	_____	_____

1. If notified of a privacy breach by a business area directly, open an incident request with the ITOC to activate the incident response plan for a suspected privacy breach.
2. When notified by Information Security Office 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 A.

Legal

<i>Contacts</i>	<i>Office Phone</i>	<i>Pager</i>	<i>E-Mail</i>
Primary: _____	_____	_____	_____
Alternate: _____	_____	_____	_____

Ongoing

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), etc.).
4. Coordinate with Public Relations on the timing and content of notification to individuals.
5. If the Information Security Office 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 that it has been 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
- E-mail notice
- Substitute notice
 - Conspicuous posting of the notice on the Online Sales Web site.
 - 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 Web site 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 Web site address is www.ftc.gov/idtheft. The toll-free number for the identity theft hotline is 1-877-IDTHEFT.

Human Resources

<i>Contacts</i>	<i>Office Phone</i>	<i>Pager</i>	<i>E-Mail</i>
-----------------	---------------------	--------------	---------------

Primary: _____

Alternate: _____

1. If notified of a privacy breach affecting employee personal information, open an incident request with the ITOC 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 ITOC, CISO, CPO 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, CPO and Legal Department to determine if the incident warrants further action.

Network Architecture

<u>Contacts</u>	<u>Office Phone</u>	<u>Pager</u>	<u>E-Mail</u>
-----------------	---------------------	--------------	---------------

Primary: _____

Alternate: _____

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

<u>Contacts</u>	<u>Office Phone</u>	<u>Pager</u>	<u>E-Mail</u>
-----------------	---------------------	--------------	---------------

Primary: _____

Alternate: _____

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 CPO 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 Web site — 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.

Location Manager

<i>Contacts</i>	<i>Office Phone</i>	<i>Pager</i>	<i>E-Mail</i>
Primary:	_____	_____	_____
Alternate:	_____	_____	_____

1. If the Location Manager becomes aware of or identifies a privacy breach, contact the ITOC to ensure that the CISO and other primary contacts are notified.
2. The Location Manager will secure the area of the breached information (e.g., computer room, data center, records room).
3. The Location Manager will assist the CISO as needed in the investigation.
4. The Location Manager will keep the CISO updated on appropriate investigation information gathered.

Appendix A

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.
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 known compromised 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 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.¹ 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.²

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.³

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).³
 - 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 be compromised).
 - 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
- Local FBI Office U.S. Secret Service — if Visa payment data is compromised

3. Provide the compromised Visa account to Visa Fraud Control Group at (650) 432-2978 within 24 hours.

- Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. 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.

³ A person with unlimited access privileges who can perform any and all operations on the computer.

4. Requirements for Compromised Entities

- All merchant banks must:
 - Provide to Visa, within 48 hours of the reported compromise, proof of Cardholder Information Security Program compliance.
 - 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.
2. Participate in all discussions with compromised entity and Visa U.S.A.
3. Engage 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 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 U.S.A. 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. CVV2⁴
 - h. Track 1 and Track 2⁵
 - 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).

⁴ 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 a 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).

⁵ 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 1-800-347-3102.
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 1-800-528-5200.
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 B

The following are selected 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 provisions include 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 C

Escalation Members (VP Level of Management)

Escalation — First Level

- Chief Information Security Officer (CISO)
- Data Processing Operations
- IT Audit Director
- Network Architecture Manager
- Online Sales Director

Escalation — Second Level

- Chief Information Officer (CIO)
- Chief Privacy Officer (CPO)
- Chief Audit Executive

Auxiliary Members (as needed)

- Business Client Systems Manager
- Management of Client Department Affected by Incident
- Risk Management
- Legal
- Loss Prevention
- Public Relations

External Contacts (as needed)

- Internet Service Provider (if applicable)
- Internet Service Provider of Intruder (if applicable)
- Communications Carriers (local and long distance)
- Business Partners
- Insurance Carrier
- External Response Teams as applicable (CERT Coordination Center⁶, etc.)
- Law Enforcement
 - Local Police Force (jurisdiction determined by crime)
 - Federal Bureau of Investigation (FBI) (especially if a federal interest computer or a federal crime is involved)
 - Secret Service

⁶ The CERT/CC is a major reporting center for Internet security problems. Staff members provide technical advice and coordinate responses to security compromises, identify trends in intruder activity, work with other security experts to identify solutions to security problems, and disseminate information to the broad community. The CERT/CC also analyzes product vulnerabilities, publishes technical documents, and presents training courses. For more detailed information about the CERT/CC, see www.cert.org.

Notification Order

Information Technology Operations Center (central point of contact)
Information Security Office
Information Privacy Office
Appropriate Client Systems Manager
System Administrator(s) of Area Affected by Incident
Manager of Area Affected by Incident
Customer Database Manager
Payment Systems Manager
Legal Counsel
Public Relations
Online Sales Manager
Employee Systems Manager (where appropriate)
Network Architectures Manager
Internal Auditing
Risk Management (where appropriate)
Loss Prevention (where appropriate)
Executive VP and CIO (when nature and impact of incident have been determined)
Chief Audit Executive
Business Partners (if connection/data has been compromised; avoid downstream liability)
Human Resources

Escalation Member Notification List

Incident Response Team Members

Department	Member	Office Phone	Pager/Cell	Text Pager	Home Phone	E-Mail
Information Security Office						
	Primary	_____	_____	_____	_____	_____
	Alternate	_____	_____	_____	_____	_____
IT Operations Center						
	Primary	_____	_____	_____	_____	_____
	Alternate	_____	_____	_____	_____	_____
Information Privacy Office						
	Primary	_____	_____	_____	_____	_____
	Alternate	_____	_____	_____	_____	_____
Network Architecture						
	Primary	_____	_____	_____	_____	_____
	Alternate	_____	_____	_____	_____	_____
Operating System Architecture						
	Primary	_____	_____	_____	_____	_____
	Alternate	_____	_____	_____	_____	_____
Business Applications						
	Primary	_____	_____	_____	_____	_____
	Alternate	_____	_____	_____	_____	_____
Online Sales						
	Primary	_____	_____	_____	_____	_____
	Alternate	_____	_____	_____	_____	_____
Internal Auditing						
	Primary	_____	_____	_____	_____	_____
	Alternate	_____	_____	_____	_____	_____

Department	Member	Office Phone	Pager/Cell	Text Pager	Home Phone	E-Mail
Customer Database						
	Primary	_____	_____	_____	_____	_____
	Alternate	_____	_____	_____	_____	_____
Credit Payment Systems						
	Primary	_____	_____	_____	_____	_____
	Alternate	_____	_____	_____	_____	_____
Legal						
	Primary	_____	_____	_____	_____	_____
	Alternate	_____	_____	_____	_____	_____
Human Resources						
	Primary	_____	_____	_____	_____	_____
	Alternate	_____	_____	_____	_____	_____
Public Relations						
	Primary	_____	_____	_____	_____	_____
	Alternate	_____	_____	_____	_____	_____
Location Manager						
	Primary	_____	_____	_____	_____	_____
	Alternate	_____	_____	_____	_____	_____