January 1, 20XX

ABC Company

123 Main Street

Los Angeles, CA 90744

(800) ABC-COMP

[www.ABCCompany.com](http://www.ABCCompany.com)

Table of Contents

[I. Introduction 4](#_Toc37074007)

[II. Incident Response Team 5](#_Toc37074008)

[A. Incident Response Team Members 5](#_Toc37074009)

[B. Incident Response Team Roles and Responsibilities 5](#_Toc37074010)

[III. Incident Response Team Notification 8](#_Toc37074011)

[A. Examples of Incidents 8](#_Toc37074012)

[B. Risk Assessment Classification 8](#_Toc37074013)

[C. Incident Declaration 8](#_Toc37074014)

[IV. Response Procedures 10](#_Toc37074015)

[A. Incident Response Phases 10](#_Toc37074016)

[B. Issues 11](#_Toc37074017)

[V. Breach of Information Security 12](#_Toc37074018)

[A. Overview 12](#_Toc37074019)

[B. Security Breach 12](#_Toc37074020)

[C. Data Owner Responsibilities 12](#_Toc37074021)

[D. Location Manager Responsibilities 13](#_Toc37074022)

[E. When Notification Is Required 13](#_Toc37074023)

[Appendix A - Incident Response Notification 14](#_Toc37074024)

[A. Escalation 14](#_Toc37074025)

[B. Internal Contact Auxiliary Members (as needed) 14](#_Toc37074026)

[C. External Contacts (as needed) 14](#_Toc37074027)

[D. Notification Order 14](#_Toc37074028)

[Appendix B - Incident Response Team Members 16](#_Toc37074029)

[Appendix C - Legislation 17](#_Toc37074030)

[A. U.S. Security Breach/Breach Notification Laws 17](#_Toc37074031)

[B. Gramm-Leach-Bliley Act (GLBA) 17](#_Toc37074032)

[C. Health Insurance Portability and Accountability Act (HIPAA) 18](#_Toc37074033)

[D. Health Information Technology for Economic and Clinical Health (HITECH) Act 18](#_Toc37074034)

[E. General Data Protection Regulation (GDPR) 19](#_Toc37074035)

[Appendix D - Payment Card Standards 21](#_Toc37074036)

[A. Requirements 21](#_Toc37074037)

[B. On-site reviews 21](#_Toc37074038)

[C. Self-Assessments 21](#_Toc37074039)

[D. PCI Data Security Standard Plan 21](#_Toc37074040)

[E. MasterCard Specific Steps 21](#_Toc37074041)

[F. Visa U.S.A. Specific Steps 22](#_Toc37074042)

[G. Steps and Requirements for Compromised Entities 22](#_Toc37074043)

[H. Steps for Merchant Banks 23](#_Toc37074044)

[I. Forensic Investigation Guidelines 23](#_Toc37074045)

[J. Visa Incident Report Template 24](#_Toc37074046)

[K. Discover Card Specific Steps 24](#_Toc37074047)

[L. American Express Specific Steps 24](#_Toc37074048)

[Appendix E - Incident Response Team Procedures 26](#_Toc37074049)

[A. IT Operations Team 26](#_Toc37074050)

[B. Chief Security Officer (CSO) 26](#_Toc37074051)

[C. Information Privacy Team 28](#_Toc37074052)

[D. Network Architecture Team 28](#_Toc37074053)

[E. Operating System Architecture Team 28](#_Toc37074054)

[F. Business Applications Team 29](#_Toc37074055)

[G. Online Sales Team 29](#_Toc37074056)

[H. Internal Audit Team 29](#_Toc37074057)

[I. Customer Database Team 30](#_Toc37074058)

[J. Credit Payment Systems Team 30](#_Toc37074059)

[K. Legal Team 31](#_Toc37074060)

[L. Human Resources Team 32](#_Toc37074061)

[M. Public Relations Team 32](#_Toc37074062)

[N. Location Manager Team 33](#_Toc37074063)

[Appendix F - Security Breach/Data Breach Resources 34](#_Toc37074064)

[A. Data Breach Notification and Response Services 34](#_Toc37074065)

[B. Credit/Monitoring Services 34](#_Toc37074066)

[Appendix G – Receipt and Acknowledgement 35](#_Toc37074067)

# I. 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. 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.

This Incident Response Plan (Plan) is established to help protect the integrity, availability and confidentiality of information, prevent loss of service, and comply with legal requirements. This Plan specifies the process for identifying and reporting an Incident, initial investigation, risk classification, documentation and communication of Incidents, responder procedures, Incident reporting, and training.

This Plan provides 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.

# II. 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 implications. The Incident Response Team’s mission is to prevent damage to our Information Resource assets that can result in loss of revenue, negative impact on our image or reputation, or loss of goodwill. This Plan documents the process by which the Incident Response Team provides an immediate, effective, and skillful response to any unexpected event involving Information Resources.

The Incident Response Team is authorized to take appropriate steps deemed necessary to contain, mitigate, or resolve Information Resource Incidents. The Team is responsible for investigating suspected intrusion attempts or other Incidents in a timely, cost-effective manner and reporting findings to management and the appropriate authorities as necessary. The Chief Security Officer (CSO) will coordinate these investigations.

The Incident Response Team will implement various monitoring systems and subscribe to security alert services to keep abreast of relevant threats, vulnerabilities, or alerts from actual Incidents.

### A. Incident Response Team Members

Each of the following will assign a primary and alternate member to the appropriate team:

* Business Applications Team
* Credit Payment Systems Team
* Customer Database Team
* Human Resources Team
* Information Privacy Team
* Information Security Team
* Internal Audit Team
* IT Operations Team
* Legal Team
* Location Manager Team
* Network Architecture Team
* Online Sales Team
* Operating System Architecture Team
* Public Relations Team

### B. Incident Response Team Roles and Responsibilities

IT Operations Team

* Central point of contact for all IT related Incidents
* Preliminary investigation of Incidents to determine if CSO needs to be notified
* Notifies CSO to activate Incident Response Team

CSO

* Contacts members of the Incident Response Team
* Determines which Incident Response Team members play an active role in the investigation
* Determines the nature and scope of the Incident with assistance from other Incident Response Team members
* Escalates to executive management as appropriate
* Contacts auxiliary departments as appropriate
* For direction and guidance, any extortion demands are brought to the attention of executive management
* 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 Security Team

* Contacts qualified information security specialists for advice as needed
* Provides proper training on Incident handling

Information Privacy Team

* Coordinates activities with the CSO
* Evaluates known or suspected unauthorized access to personally identifiable or other Sensitive Information
* 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 a breach

Network Architecture Team

* 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
* Evaluates unauthorized access to computers, system, network, or other Information Resources
* Evaluates corruption of, or damage to, electronic data

Operating Systems Architecture Team

* 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 Team

* Monitors business applications and services for signs of attack
* Reviews audit logs of mission-critical servers for signs of suspicious activity
* Contacts the IT Operations Team with any information relating to a suspected breach
* Collects pertinent information regarding the Incident at the request of the CSO

Online Sales Team

* Monitors business applications and services for signs of attack
* Reviews audit logs of mission-critical servers for signs of suspicious activity
* Contacts the IT Operations Team with any information relating to a suspected breach
* Collects pertinent information regarding the Incident at the request of the CSO

Internal Audit Team

* 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

# III. Incident Response Team Notification

The IT Operations Team will be the central point of contact for reporting computer Incidents or intrusions. The IT Operations Team will notify the CSO.

All computer security Incidents must be reported to the CSO. A preliminary analysis of the Incident will take place by the CSO and that will determine whether Incident Response Team activation is appropriate.

An Incident Response Form shall be used to identity incidents, classify, and document actions taken.

### A. Examples of Incidents

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

* Loss of laptop containing sensitive information
* Breach of Personal Information
* Denial of Service / Distributed Denial of Service
* Excessive Port Scans
* Firewall Breach
* Virus Outbreak

Many security Incidents, such as isolated occurrences of computer viruses, are easily handled via well-established procedures (especially in larger companies), and do not justify calling out the entire Incident Response Team. This Plan describes the criteria used to classify the severity of security Incidents, and those severities that result in Plan activation.

### B. Risk Assessment Classification

Incidents should usually be grouped into a few different risk classification or severity levels, with broad sets of criteria for each level. For example:

* ***Severity* 1** – Small numbers of system probes or scans detected on internal systems; isolated instances of known computer viruses easily handled by antivirus software.
* ***Severity 2*** – Small numbers of system probes or scans detected on external systems; intelligence received concerning threats to which systems may be vulnerable.
* ***Severity 3*** – Significant numbers of system probes or scans detected; penetration or denial of service attacks attempted with no impact on operations; widespread instances of known computer viruses easily handled by anti-virus software; isolated instances of a new computer virus not handled by anti-virus software.
* ***Severity 4*** – Penetration or denial of service attacks attempted with limited impact on operations; widespread instances of a new computer virus not handled by anti-virus software; some risk of negative financial or public relations impact.
* ***Severity 5*** – Successful penetration or denial of service attacks detected with significant impact on operations; significant risk of negative financial or public relations impact.

In this example, Incidents of Severity 3, 4, and 5 would result in Plan activation, while Incidents of Severity 1 and 2 would be handled without Incident Response Team involvement.

### C. Incident Declaration

When an Incident requiring Plan activation occurs, a formal Incident is declared. The IT Operations Team notifies the CSO that an Incident has been detected. The CSO is then responsible for confirming the IT Operations Team findings and analysis and, if appropriate, activates the Incident Response Team.

# IV. Response Procedures

Response procedures can be described at two levels of detail in the Plan. The first level of detail is a set of general guidelines that describes the principal phases of Incident response, and what happens during each phase. Every Plan should include this level of detail. The second level of detail is a set of step-by-step response procedures, specific to individual Incident types (e.g., procedure(s) for handling virus Incidents, procedure(s) for handling hacker break-ins, etc.). These procedures will generally be created over time, and can be added to the Plan in appendices as they are developed.

### A. Incident Response Phases

There are five principal phases of Incident response, shown below. The general procedures to be followed in each phase are described in the appendices.

* ***Alert Phase*** - The alert phase is the process of learning about a (potential) security Incident, and reporting it to the Incident Response Team. Alerts may arrive from a variety of sources including: monitoring systems, Staff reporting of an event, firewalls and intrusion detection systems, anti-virus software, threats received via electronic mail, media reports about a new threat, etc. The Incident Response Team is usually notified by providing a “hotline” telephone number that is reachable 24 hours a day, 7 days a week.
* ***Triage Phase*** - The triage phase is the process of examining the information available about the Incident to determine first if it is a “real” Incident, and second, if it is, its severity. The Incident Response Team Manager usually does this, with assistance from the permanent team members. If the Incident’s severity warrants, the Incident Response Team management advisory board will also be alerted in this phase. The board must do two important things in this phase: A decision to “pursue” or “protect” must be made. In other words, does the company want to attempt to catch the perpetrator(s) of the attack for later criminal or civil action, or does it simply want to stop the Incident and restore normal operations? This decision must be made before response begins, because it influences how the response will happen. Resources (personnel and financial) must be allocated to the response and recovery teams at a level appropriate to the severity of the Incident.
* ***Response Phase*** - In the response phase, the Incident Response Team gathers evidence (audit trails, log files, contents of files, etc.). If the “pursue” option was chosen, this process must be performed in a forensically sound manner so that the evidence will later be admissible in court; the team may need specialized technical assistance and advice from a third party to do this successfully. Once evidence has been gathered, it is analyzed to determine the cause of the Incident, the vulnerability or vulnerabilities being exploited, how to eliminate these vulnerabilities and/or stop the Incident. An assessment is also made of how far the Incident has spread, i.e., which systems are involved, and how badly have they been compromised.
* ***Recovery Phase*** - The recovery phase begins once the response phase has been completed (there may at times be some overlap). In this phase, the Incident Response Team restores the systems affected by the Incident to normal operation. This may require reloading data from backup tapes, or reinstalling systems from their original distribution media. Once the affected systems have been restored, they are tested to make sure they are no longer vulnerable to the attack(s) that caused the Incident. They are also tested to make sure they will function correctly when placed back into production.
* ***Maintenance Phase*** - The maintenance phase is also called “lessons learned.” In this phase, the Incident and response are reviewed to determine the parts of the Plan that worked correctly, and the parts that need improvement. The areas in which improvement is needed are then corrected, and the Plan updated accordingly. Other areas that need to be changed (policies, system configurations, etc.) may also be identified during this phase.

### B. Issues

Five important issues that must be addressed by the above steps include:

1. The systems impacted and the extent of damage or breach
2. How the breach occurred
3. Steps taken to mitigate or remedy the situation
4. Suspects (internal or external)
5. Evidence that exists or needs to be preserved

# V. Breach of Information Security

### A. Overview

This 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 the Appendix. Selected laws and regulations require the organization to follow specified procedures in the event of a breach of personal information as covered in the Appendix.

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 the purposes of this Plan, and as defined by the Federal Trade Commission (FTC), personal information is defined as “individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license or other state-issued identification number; (g) credit or debit card information, including card number, expiration date, and security code; (h) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies an individual consumer; or (i) any information that is combined with any of (a) through (h) above.”

### B. 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.

ABC Company 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).

### C. 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 CSO 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 CSO 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 IT Operations Team will act as a central point of contact for reaching the CSO and CPO.

The CSO will determine whether the breach or suspected breach is serious enough to warrant full 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, CSO, Legal or other Incident Response Team members throughout the investigation.

### D. 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 IT Operations Team immediately and open an Incident report. (See “Incident Response” Section, IT Operations Team.)

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.

### E. 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, mobile device, 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.

# Appendix A - Incident Response Notification

### A. Escalation

1. First Level

Chief Security Officer (CSO)

Director of IT

IT Audit Director

Network Architecture Manager

Online Sales Director

2. Second Level

Chief Privacy Officer (CPO)

Chief Audit Executive

### B. Internal Contact Auxiliary Members (as needed)

Business Client Systems Manager

Management of Client Department Affected by Incident

Risk Management

Legal

Loss Prevention

Public Relations

### C. 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 Center, 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

### D. Notification Order

IT Operations Center (central point of contact)

Chief Security Officer (CSO)

Information Security Team

Information Privacy Team

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 Director of IT (When nature and impact of Incident has been determined)

Chief Audit Executive

Business Partners (if connection/data has been compromised; avoid downstream liability)

Human Resources

# Appendix B - Incident Response Team Members

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Department** | **Member** | **Office Phone** | **Cell** |  | **Home Phone** | **E-Mail** |
| **IT Operations Team**  Primary  Alternate | | | | | | |
| **Information Security Team**  Primary  Alternate  **Information Privacy Team**  Primary  Alternate  **Network Architecture Team**  Primary  Alternate  **Operating System Architecture Team**  Primary  Alternate  **Business Applications Team**  Primary  Alternate  **Online Sales Team**  Primary  Alternate  **Internal Audit Team**  Primary  Alternate  **Customer Database Team**  Primary  Alternate  **Credit Payment Systems Team**  Primary  Alternate  **Legal Team**  Primary  Alternate | | | | | | |

# Appendix C - 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.

### A. U.S. Security Breach/Breach Notification Laws

In the event of a data breach, U.S. states and industry-specific laws and standards require notice to be provided to the affected individuals. Compliance with federal industry-specific requirements may satisfy state breach notification requirements. Laws are generally based on the state of residence of the individual whose data was compromised, not by the company’s place(s) of business.

Many states have enacted security breach/data breach laws and regulations. An updated list can be found on the web site of the National Conference of State Legislators

<http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>

For example, 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.

Contact the Office of the Attorney General of the appropriate state. Have the following information ready:

* Date(s) of breach.
* Date(s) of discovery of breach.
* Date(s) notice provided to consumers.
* If notification was delayed due to a law enforcement investigation.
* Type of personal information involved in the breach.
* Brief description of the breach including number of records, accounts, individuals compromised.
* Type of breach (e.g. unintended disclosure, hacking/malware, payment card fraud, insider, physical access, portable/mobile device, stationary device).
* Location of breached information (e.g. laptop, desktop, network server, e-mail, portable/mobile device).
* Law enforcement agency notified including the report number (if a police report was filed).

### B. 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.

### C. Health Insurance Portability and Accountability Act (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.

### D. Health Information Technology for Economic and Clinical Health (HITECH) Act

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

HITECH specifies the following notification requirements: The covered entity must notify each individual whose unsecured protected health information has been, or is reasonably believed to have been, accessed, acquired, or disclosed as a result of a breach:

* Written notice of the breach sent via first class mail or e-mail (if the individual’s preference).
* If more than 500 individuals have unsecured PHI disclosed, additional notice provided immediately to the Secretary of Health and Human Services and to prominent media outlets in the state where the individual resides.
* Business associates notify the covered entity if the associate experiences unauthorized disclosures of unsecured PHI. The covered entity notifies affected individuals within 60 calendar days after the unauthorized disclosure is discovered.

### E. General Data Protection Regulation (GDPR)

Article 33 – Notification of a personal data breach

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

The notification shall at least:

(a) Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) Describe the likely consequences of the personal data breach;

(d) Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34 - Communication of a personal data breach to the data subject.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

The communication to the data subject shall not be required if any of the following conditions are met:

(a) The controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;

(b) The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize;

(c) It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph above are met.

# Appendix D - Payment Card Standards

### A. Requirements

The PCI Data Security Standard 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.

The PCI Data Security Standard applies to all members, merchants, and service providers that store, process or transmit cardholder data. Failure to comply with the standards could result in a merchant being subjected to a fine or the loss of access to the credit card networks.

Refer to ABC Company’s PCI Policy for more information on PCI requirements.

### B. On-site reviews

Certain merchants, including e-commerce merchants, 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.

### C. Self-Assessments

The credit card companies recommend that a Self-Assessment be carried out on an annual basis. For a copy of the Payment Card Industry Self-Assessment Questionnaire, see https://www.pcisecuritystandards.org/pci\_security/completing\_self\_assessment

### D. PCI Data Security Standard Plan

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

### **E. 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 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.

### **F. 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://usa.visa.com/download/merchants/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.

### **G. Steps and Requirements for Compromised Entities**

1. Immediately contain and limit the exposure.
2. 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 be compromised).

1. Be on HIGH alert and monitor all Visa systems. 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.

1. 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.
2. 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.
3. 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

### **H. Steps for Merchant Banks**

1. Contact Visa USA Fraud Control Group immediately at (650) 432-2978. Canada merchants contact Visa Canada Risk Management at 416-860-3090.
2. Participate in all discussions with the compromised entity and Visa USA, or if we 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

### **I. 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.
2. Number of accounts at risk, identify those stored and compromised on all test, development, and production systems
3. Type of account information at risk
4. Account number
5. Expiration date
6. Cardholder name
7. Cardholder address
8. CVV2
9. Track 1 and Track 2
10. Any data exported by intruder
11. Perform Incident validation and assessment.
12. Establish how compromise occurred
13. Identify the source of compromise
14. Determine timeframe of compromise
15. 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.
16. Determine if compromise has been contained.
17. 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.).
18. If applicable, review VisaNet endpoint security and determine risk.
19. Preserve all potential electronic evidence on a platform suitable for review and analysis by a court of law if needed.
20. Perform remote vulnerability scan of entity’s Internet facing site(s).

### **J. 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”.

1. Executive Summary
   1. Include overview of the Incident
   2. Include Risk Level (High, Medium, Low)
   3. Determine if compromise has been contained
2. Background
3. Initial Analysis
4. Investigative Procedures - Include forensic tools used during investigation
5. Findings
   1. Number of accounts at risk, identify those stored and compromised
   2. Type of account information at risk
   3. Identify ALL systems analyzed. Include the following:
      1. Domain Name System (DNS) names
      2. Internet Protocol (IP) addresses
      3. Operating System (OS) version
      4. Function of system(s)

d. Identify ALL compromised systems. Include the following:

* + 1. DNS names
    2. IP addresses
    3. OS version
    4. 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.

1. Compromised Entity Action
2. Recommendations
3. Contact(s) at entity and security assessor performing investigation

### **K. 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.

### **L. 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 E - Incident Response Team Procedures

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.

### A. IT Operations Team

|  |  |  |  |
| --- | --- | --- | --- |
| Contacts | Office Phone | Hotline | E-Mail |
| Primary: | | | |
| Alternate: | | | |

1. The IT Operations Team will serve as a central point of contact for reporting any suspected or confirmed breach of personal information on an individual. The following information will be collected by the IT Operations Team  
   - Date and time reported  
   - Staff member reporting Incident

- Date and time of Incident

- Description of Incident (e.g. lost laptop, unauthorized access, virus, etc.)

- Steps taken by person/department reporting Incident

- Other relevant information

1. After documenting the facts presented by the caller and verifying that a privacy breach or suspected privacy breach occurred, the IT Operations Team will open a Priority Incident Request. This will begin an automated paging process to immediately notify the CSO.
2. The IT Operations Team will page the primary and secondary contacts in the Information Security Team. The IT Operations Team advises that a breach or suspected breach of personal information on an individual has occurred. After the Information Security Team 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 Incident”**.

### B. Chief Security Officer (CSO)

|  |  |  |  |
| --- | --- | --- | --- |
| Contacts | Office Phone | Cell | E-Mail |
| Primary: Chief Security Officer | | | |
| Alternate: Information Security Manager | | | |

1. When notified by the IT Operations Team, the CSO performs a preliminary analysis of the facts and assess 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 IT Operations Team 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 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 Legal Department, Information Privacy Team 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 Team 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 Legal Department, Information Privacy Team 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.
18. Identify the source of compromise, and the timeframe involved.
19. 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.
20. Document all internet protocol (IP) addresses, operating systems, domain name system names and other pertinent system information.
21. 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.
22. Do not access or alter the compromised system.
23. Do not turn off the compromised machine. Isolate the system from the network (i.e., unplug cable).
24. 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.
25. Monitor systems and the network for signs of continued intruder access.
26. 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.
27. Note: Visa has specific procedures that must be followed for evidence preservation.
28. 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.
29. If Protected Health Information (PHI) is involved, follow the additional steps outlined under Appendix C – U.S. Privacy Legislation, Health Information Technology for Economic and Clinical Health (HITECH) Act.
30. If credit cardholder data is involved, follow additional steps outlined under Appendix D – Payment Card Standards. 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.**
31. 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.

### C. Information Privacy Team

|  |  |  |  |
| --- | --- | --- | --- |
| Contacts | Office Phone | Cell | E-Mail |
| Primary: | | | |
| Alternate: | | | |

1. Coordinates activities with the CSO.
2. Documents the types of personal information that may have been breached.
3. Provides guidance throughout the investigation on issues relating to privacy of customer and employee personal information.
4. Assists in developing appropriate communication to impacted parties.
5. Coordinates with the Public Relations Team.
6. Assesses the need to change privacy policies, procedures, and/or practices as a result of a breach.

### D. Network Architecture Team

|  |  |  |  |
| --- | --- | --- | --- |
| Contacts | Office Phone | Cell | E-Mail |
| Primary: | | | |
| Alternate: | | | |

1. When notified by the CSO that the Incident Response Team 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.

### E. Operating System Architecture Team

|  |  |  |  |
| --- | --- | --- | --- |
| Contacts | Office Phone | Cell | E-Mail |
| Primary: | | | |
| Alternate: | | | |

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

### F. Business Applications Team

|  |  |  |  |
| --- | --- | --- | --- |
| Contacts | Office Phone | Cell | E-Mail |
| Primary: | | | |
| Alternate: | | | |

1. Monitors business applications and services for signs of attack.
2. Reviews audit logs of mission-critical servers for signs of suspicious activity.
3. Contacts the IT Operations Team with any information relating to a suspected breach.
4. Collects pertinent information regarding the Incident at the request of the CSO.

### G. Online Sales Team

|  |  |  |  |
| --- | --- | --- | --- |
| Contacts | Office Phone | Cell | E-Mail |
| Primary: | | | |
| Alternate: | | | |

1. The Online Sales Team will serve as the primary contact for the Online Sales Department. Online Sales Team support is available 24x7 and should be contacted using the above information.
2. When notified by Information Security Team that the Incident Response Team has been activated, the Online Sales Team will collect pertinent information regarding the Incident from the CSO and determine the appropriate systems involved. 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 IT Operations Team to begin the official Incident response notification process.
3. Online Sales Team, 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 event logs, looking at the network for abnormal connections, inspecting the 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, the Online Sales Team will only notify and communicate with the following management/groups: XXX.
5. Online Sales Team will keep persons informed until it can be confirmed or denied that the online sales systems were compromised.

### H. Internal Audit Team

|  |  |  |  |
| --- | --- | --- | --- |
| Contacts | Office Phone | Cell | E-Mail |
| Primary: | | | |
| Alternate: | | | |

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

### I. Customer Database Team

|  |  |  |  |
| --- | --- | --- | --- |
| IT Customer Database Contacts | Office Phone | Cell | E-Mail |
| Primary: | | | |
| Alternate: | | | |
| Data Owner Contacts | Office Phone | Cell | E-Mail |
| Primary: | | | |
| Alternate: | | | |

Notification Steps

1. If the Customer Database Team or Data Owners hear of or identifies a privacy breach, contact the IT Operations Team to ensure that the CSO and other primary contacts (e.g. CPO) are notified.
2. The Customer Database Team and Data Owner will assist the CSO as needed in the investigation.
3. IT Customer Database contact notifies the IT Contractor Liaison (if warranted).
   * 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).
   * Identify individuals whose information may have been compromised. An assumption could be “all” if an entire table or file was compromised.
   * Secure all files and/or tables that have been the subject of unauthorized access or use to prevent further access.
   * Upon request from the CSO, provide a list of affected individuals, including all available contact information (i.e., address, telephone number, email address, etc.).

### J. Credit Payment Systems Team

|  |  |  |  |
| --- | --- | --- | --- |
| Contacts | Office Phone | Cell | E-Mail |
| Primary: | | | |
| Alternate: | | | |

1. If notified of a privacy breach by a business area directly, open an Incident request with the IT Operations Team to activate the Plan for a suspected privacy breach.
2. When notified by Information Security Team that the Incident Response Team has been activated, perform a preliminary analysis of the facts and assess the situation to determine the nature of Incident.
   1. Determine the type of personal information breached.
      1. Current credit card customers
      2. New credit card applications
      3. Personal check authorizations
   2. Determine data sources and method of breach (hardcopy, electronic)
   3. Determine method of breach if possible.
   4. Identify additional resources needed to complete investigation
3. Determine the scope of the breach.
   1. Time Frame
   2. Specific Data Elements
   3. Specific Customers
4. Take necessary steps to prevent additional compromise of personal information about individuals.
5. Report all findings to the Plan Team.
6. Within 24 hours of notification of an account number compromise, contact the appropriate card companies:
   1. Visa Fraud Control Group
   2. MasterCard Compromised Account Team
   3. Discover Fraud Prevention
   4. American Express Merchant Services
7. Act as liaison between the card companies, CSO, and Legal.
8. Ensure credit card companies’ specific requirements for reporting

### K. Legal Team

|  |  |  |  |
| --- | --- | --- | --- |
| Contacts | Office Phone | Cell | E-Mail |
| Primary: | | | |
| Alternate: | | | |

On-going:

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 office, 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 CSO 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, e-mail notice, and substitute notice (conspicuous posting of the notice on the online sales website and/or 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.
* Inform each individual about the availability of online guidance regarding measures to protect against identity theft. Encourage the individual to report any suspected Incidents of identity theft to the local law enforcement agency.

### L. Human Resources Team

|  |  |  |  |
| --- | --- | --- | --- |
| Contacts | Office Phone | Cell | E-Mail |
| Primary: | | | |
| Alternate: | | | |

1. If notified of a privacy breach affecting employee personal information, open an Incident request with the IT Operations Team to activate the Plan for suspected privacy breach.
2. When notified by the Information Security Team that the Incident Response Team 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 Operations Team, CSO, 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 CSO, CPO and Legal Department to determine if the Incident warrants further action.

### M. Public Relations Team

|  |  |  |  |
| --- | --- | --- | --- |
| Contacts | Office Phone | Cell | E-Mail |
| Primary: | | | |
| Alternate: | | | |

On-going:

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.
3. Vehicles for communicating include:
   1. News wire services
   2. Online Sales web site – Post statement on home page or conspicuous location of web site.
   3. Internal Website – If appropriate for breach of employee information
   4. E-mail
   5. News conference – If privacy breach should reach a national and/or crisis level, coordinate brief news conference at headquarters or appropriate location.
      1. Appoint appropriate spokesperson
      2. Prepare statement and, if necessary, potential Q & A.
      3. Coach spokesperson on statement and potential Q & A.
      4. Invite select media to attend and cover organization’s proactive message.
      5. 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
4. Prepare appropriate response to media, customer, and/or employee; and have the CPO and Legal Department approve prior to distribution.
5. Proactively respond to media inquiries, if necessary.
6. Monitor media coverage and circulate accordingly.

### N. Location Manager Team

|  |  |  |  |
| --- | --- | --- | --- |
| Contacts | Office Phone | Cell | E-Mail |
| Primary: | | | |
| Alternate: | | | |

1. If the Location Manager becomes aware of or identifies a privacy breach, contact the IT Operations Team to ensure that the CSO 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 CSO as needed in the investigation.
4. The Location Manager will keep the CSO updated on appropriate investigation information gathered.

# Appendix F - Security Breach/Data Breach Resources

### A. Data Breach Notification and Response Services

The following service providers help provide forensic investigation, notification, and call center services:

* AllClear ID (877) 441-3009
* CSIdentity (aka CSID) Data Breach Mitigation Services (855) 890-2743
* Equifax Data Breach Services (866) 510-4211 or psol@equifax.com
* Experian Rapid Response Hotline: (866) 751-1323 or databreachinfo@experian.com
* ID Experts (971) 242-4775
* Kroll Data Breach Response, forensics, call center (877) 300-6816

### B. Credit/Monitoring Services

ABC Company has chosen Experian’s ProtectMyID service that offers free credit monitoring and identity theft protection. Experian is a leading global information services company that helps individuals understand and keep track of their credit report, as well as monitor for and resolve identify theft. For more information visit <https://www.experian.com/consumer-products/protect-my-id.html>.

# Appendix G – Receipt and Acknowledgement

I have read ABC Company’s (Company’s) Incident Response Plan and agree to abide by it as consideration for my continued employment by Company. I understand that violation of the enclosed policies and guidelines may result in disciplinary action including, but not limited to, termination.

This document supersedes all prior electronic equipment policies, guidelines, understandings and representations. I understand that if any of the provisions of this manual are found null, void, or inoperative for any reason, the remaining policies and guidelines will remain in full force and effect.

If I am uncertain about any policy or procedure, I will check with my immediate supervisor or Company management.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_

Employee Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Name (Printed)