DATA BREACH INCIDENT RESPONSE WORKBOOK

For Questions About a Data Breach and How to Respond, call the Data Breach Hotline.
800-965-7564

Notice to Readers
This paper is not intended as legal advice and Debix encourages all companies to seek legal advice regarding issues discussed in this document.

This document is a work in progress–Debix is continually seeking suggestions for improvement or areas where clarification is needed. If you have a suggestion for this publication, please email sales@debix.com. Your feedback is appreciated and important to us.

Version 1.0

Using this Workbook
This workbook is intended to provide general guidance and assistance in developing security standards appropriate for individual businesses. No one solution fits all businesses. Measures will vary depending on factors including the size and complexity of the business, the industry, and sensitivity of data.

The information in this workbook should not be regarded as a substitute for a company's self-assessment of security procedures or for legal advice.

Data Breach Incident Response Workbook

by Debix www.Debix.com/business

Table of Contents

1 The World We live In

In 2007, over 127 million individuals in the U.S. had their Personally Identifiable Information (PII) lost, stolen or compromised.

According to a Ponemon Institutes Study in 2007, the average cost of a data breach to a business was $197 per record lost.

Consumer awareness of identity theft and the security of personal information will only become more important in the future. With data breaches continuing to make daily headlines, publicity of large-scale breaches has caused an outrage among consumer advocacy groups, as well as adversely affected organizations such as banks and issuers. Some incidents have led breached institutions to be stricken with devastating class-action lawsuits.

Since 2005, there have been over 925 information security breaches, including:

- ChoicePoint
- Bank of America
- Lexis Nexis
- Card Systems
- Boston Globe
- Veterans Administration
- DSW
- TJX

(Source: Hunton & Williams, 2008)

Damage to the reputation of the breached institution may be even more difficult to prevent than any financial losses because it is heavily dependent upon the company's image, brand, and its relationships with customers. While data breaches can cost tens of millions of dollars to repair because of fines, security upgrades, and notification efforts, reputation is one asset that may not be guaranteed as fully restorable.

Key findings from a survey of breach victims highlight the implications that security breaches hold:

- 40% of consumers reported that security breaches changed their relationships with the affected institution or business.
- Confidence and buyer behavior are severely impacted by security breaches, with 55% of victims trusting the affected organization less, and 30% choosing to never purchase goods or services again from that organization. As a result, breached institutions must go beyond basic notification and take assertive action to mitigate the risk placed on victims.
- A recent study done by The Ponemon Institute reveals attitudes and actions of individuals after a private sector breach event. Nearly 60% terminated or considered terminating their relationship with the company involved.

Key findings on how consumers were affected by the way the organization responded to the security breach:

- 55% of breach victims who were offered a fraud protection solution were satisfied with the institution's handling of the incident, almost double the 31% of those who were satisfied without being offered any kind of restitution.
- The majority of breach victims (56%) prefer a solution that prevents fraudulent use of their information rather than detecting or resolving fraud after it has occurred.
- Breach victims are beginning to expect fraud protection assistance from the institution, with 36% already having been offered some kind of identity fraud protection service.

(Sources: Javelin, 2008; Ponemon, 2008)

Most identity security experts agree that while actual incidences of data breaches may not be increasing, identification and notification of data breaches are definitely on the rise.

Fraud prevention solutions are designed to avert new account fraud before it occurs. The strategic advantage of fraud prevention therefore lies in the ability to avoid losses to institutions and consumers, rather than dealing with them after the fraudulent applications have been made.

This *Data Breach Incident Response Workbook* is designed to address all these issues and will provide an outline and recommendations for planning a well-orchestrated response to a data compromise.

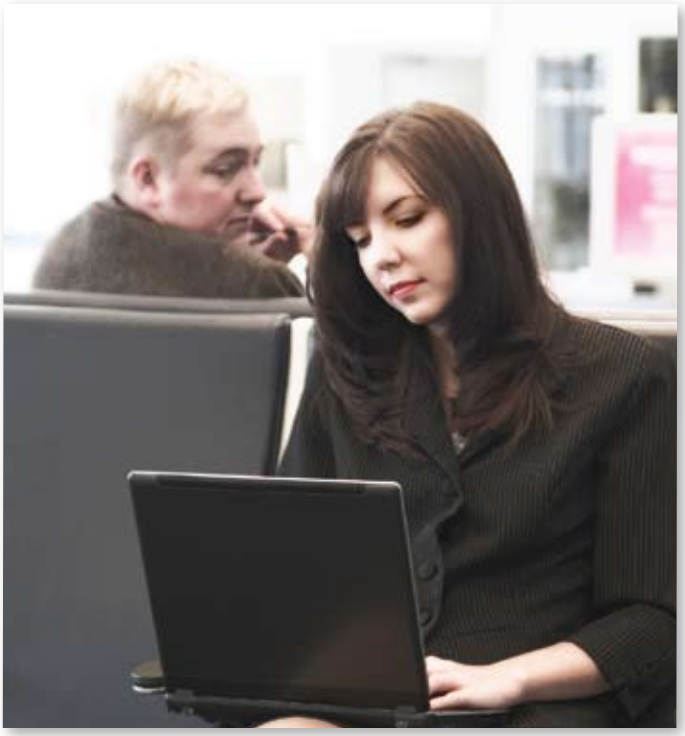
2 Anatomy of a Data Breach

These days, it is almost impossible to be in business and not collect or hold Personally Identifying Information (PII) that belongs to customers, employees, business partners, students or patients. PII includes (but is not limited to):

- Social Security Number
- Name
- Address
- Date of Birth
- Account Numbers (checking, credit card, etc)
- Email address
- Passwords

If this Personally Identifying Information falls into the wrong hands, it could put these individuals at risk for identity theft.

Not all personal information compromises result in identity theft, however, and the type of personal information compromised can significantly affect the degree of potential damage.



There are four fundamental ways data breaches occur:

1. **Theft or Loss of Physical Equipment**
   A data breach can occur with the theft or loss of physical equipment which stores data, such as laptop computers or memory storage devices.
2. **Illegal access to the systems or information** A data breach can occur through unlawful access to PII data by technological means such as hacking into existing computer systems or hijacking computers with viruses, worms, or trojans. Once inside a system, criminals can steal data, infect it, or overload computer systems.
3. **Insiders**
   A data breach can be committed by current employees, ex-employees, or even through social engineering where an employee is tricked into providing access or information (phishing is considered to be socially engineered fraud).
4. **Oversight**
   A data breach can occur when no one thought the information needed to be protected and no precautions were taken to safeguard the data in the first place.

3 Preparing For A Data Breach

While theft prevention should always be the primary goal of any organization, proactive planning can minimize the impact when a breach does occur. Most businesses tend to hope they will never fall victim to a security crime or disaster – but "hope" is not a good foundation for a business plan -- being prepared is.

There are two main things to keep in mind when the time comes to respond to a data breach –

1. it is important to move swiftly and follow your completed Data Breach Incident Response Plan, and
2. it is important to document all ongoing events, all people involved, and all discoveries into a timeline for evidentiary use.

The following is a list of actions that are going to need to be taken when a breach occurs:

- Identify how the breach happened, contain the breach, and implement a solution so it can not happen again
- Notify appropriate people within the company
- Notify External Agencies, within required time frames, such as:
  - Forensics Investigator
  - Law Enforcement
  - Affected vendors, suppliers
  - FTC
  - State Attorneys General (where applicable)
  - Consumers

The remainder of this workbook is designed to walk businesses through preparing for action on all of these points.

Be prepared for a data breach. The Number One recommendation of any company that has experienced a data breach is to have a response plan in place. The plan should include written emergency contact lists, a clear understanding of what law enforcement agencies must be contacted and involved, and a time frame for notification – internal SLAs should be established. Additionally, vendor contracts should be in place with a mail-house for notification letters, a call center (if your own in-house staff could not handle a major data breach), and finally, to have pre-negotiated rates for consumer fraud protection in the event your company needs to notify customers. It is very difficult to negotiate these contracts during an emergency situation.

Use the worksheets in this book to create a formal written plan of how you would respond to a data breach situation. Your incident response team should meet monthly to update contact information, discuss any changes in the organization, review any incidents that may have occurred, and evaluate the response process. The incident response team should practice responding to a data breach at least annually and preferably quarterly.

4 Build A Strong Internal Response Team

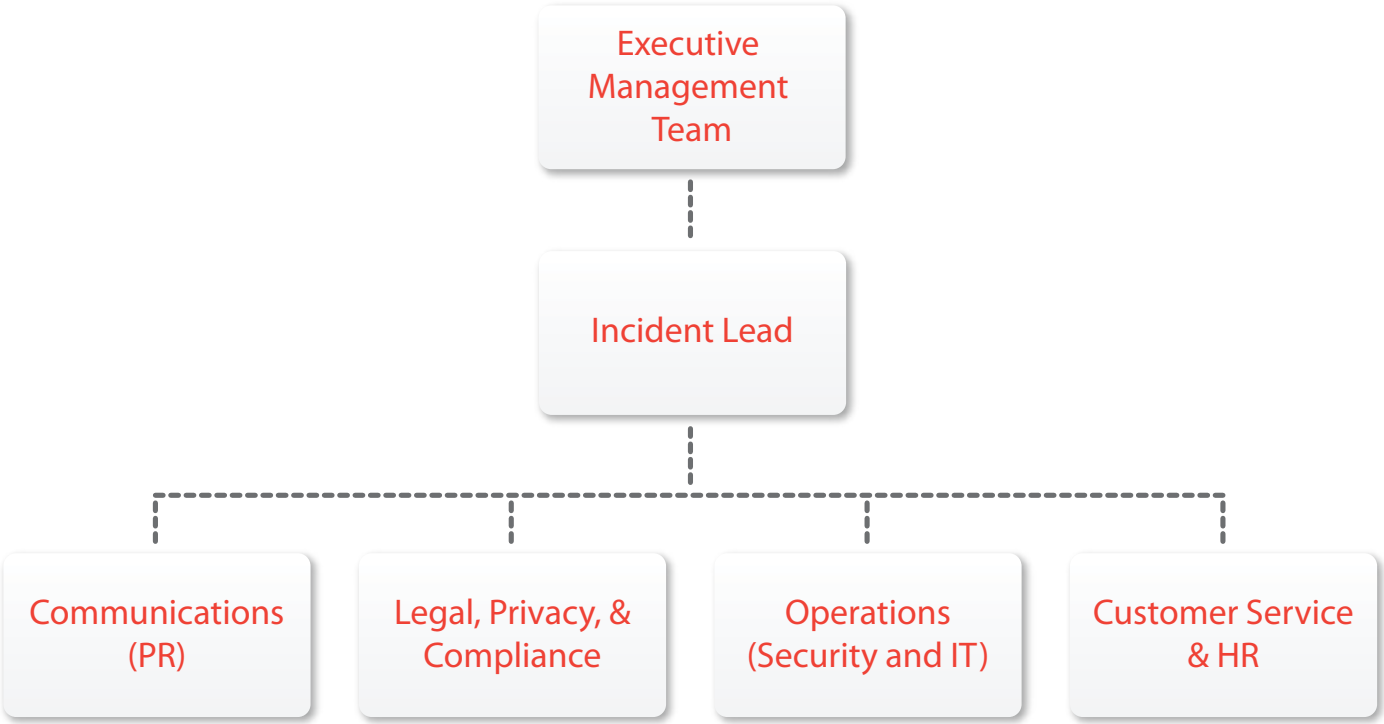
Build your team with the right mix of expertise with representation from:

- Executive Management
- Information Technology
- Customer Service
- Risk Management and Security
- Compliance and Audit
- Legal
- Privacy
- Public Relations

It is important to assign an **Incident Lead** to direct and manage the internal response team, as well as to act as the go-between for management and the response team. This individual (and their backup) should be considered to be the project lead for the breach incident. The other members of the response team have specific responsibilities to protect your company and customers, but all of them should report directly to the Incident Lead.

Executive Management needs to be kept up-to-date during a data breach incident. The **Incident Lead** will be running tactical, day-to-day operations of the data breach as well as regularly updating management. The Incident Lead is typically someone from the legal department or a chief privacy officer and their role is primarily that of a project manager. This person will coordinate efforts among all groups, notify all the appropriate people within the company and externally, and create the documentation and timeline of activities, identify key tasks, and estimate costs.

Response Team Structure



Communications personnel must be involved in the breach incident. A decision will need to be made very early in the event to determine whether or not it is appropriate to notify consumers of the incident. If consumers do need to be notified, it is critical to begin notification in a timely manner (see Chapter Seven: Notifying Customers and Affected Businesses). Every state has different notification laws based on the information that was breached, and communications groups must work hand-in-hand with legal counsel to determine the specific legal obligations and timeline for notification.

Legal, Privacy, and Compliance personnel will also work with counsel to find out what is required in the response. These individuals will be responsible for determining whether or not consumers should be notified and the legal requirements around what the notification must say (see Chapter Seven: Notifying Customers and Affected Businesses). Additionally, this team or person is also responsible for determining what external organizations should be contacted. For example, in the event of a data breach of credit card information, credit card associations (Visa, MasterCard, American Express, and Discover) should be notified, as well as the acquirer through which the merchant processes. If the company who suffered the breach loses client information, the client will need to be notified and involved in the plan.

Operations (Security and IT) teams will be critical in helping identify what information was actually compromised. A word of caution, though -- many IT individuals may be under the impression that they possess the skill set and training to do forensics on the data compromise (identification of how the breach happened, impact to any other systems, analysis of what was taken, ensuring the damage has stopped, etc). Unless specifically trained for this work, it is important to hire certified data forensics specialists, who possess a very specialized skill set. By having an untrained team working on the system, the chances of information being tampered with or corrupted are increased and make it significantly more difficult to investigate.

> **Recommendation:** Hire an outside certified data forensics team in every incident where a computer intrusion has occurred.

Customer Service and Human Resource (HR) personnel will play a critical role in the incident if employee or customer notification is determined to be a requirement. HR will be involved when the breach has impacted employee information and Customer Service will be called into action if the data breach impacts that of customers.

Because the notification of clients will create high volumes of calls, most companies will also create a telephone hotline dedicated to handling the breach incident.

A consumer website should also be created where a customer can enter their last name and last four digits of their social security number to see if they were impacted by the data breach. The website should also provide clear, detailed instructions about what consumers should do to protect themselves. Also include a Frequently Asked Questions section -- one of the most common questions consumers have when they hear about a data breach is, "Was I Impacted?" If this can be determined by visiting the website first, call volumes may be reduced.

Contacting the Team

Create and distribute an Incident Response Phone List that is updated at least quarterly. Include the employee's role on the Incident Response Team, their name, work/cell/home phone numbers, and e-mail address. Every person should have a backup contact as well.

Sample Incident Response Phone List:

Data Breach Contact List **Last Updated:** _____
(to be updated quarterly)

Role	Name	Work Phone	Home Phone	Cell Phone	Email
CEO					
CFO					
Legal Counsel					
Other Executives that will need to know					
PR					
PR Backup					
Incident Lead					
Incident Lead Backup					
Customer Service					
Customer Service Backup					
HR					
HR Backup					
IT					
IT Backup					
In-house Legal Counsel					
In-house Legal counsel backup					
External Legal Counsel					
External Legal Counsel backup					
Chief Privacy Officer					
Privacy Backup					

Some points to consider:

- In order for a company to have a strong data breach prevention plan, concern and focus on data security must come from top management so that fiscal and personnel resources are included in budget allowances year-round.
- Data breaches often must involve the CEO, CFO, CPO, CIO and General Counsel; you should include them in the Internal Response Team and Plan from the outset of the project.
- Upper management involvement in data breach preparedness is necessary in order to integrate the concern for information security as a core value in a company.
- Re-evaluation of security systems and policies should be done on an ongoing basis in order to remain up-to-date on the latest technologies and criminal trends.
- Training and practice of your Data Breach Incident Response Plan should occur on a regular basis.

5 Data Breach Checklist

With a data breach, **timing is everything.** Document everything that happens, everything you discover, and turn it into a timeline!

Within the first few hours after discovering a potential data breach, it is important to begin running through the following checklist:

- Create a Data Breach Incident Plan that includes the following information (See Chapter 6: *Data Breach Investigations Log* will also assist you in creating this plan):
  - Date (and time)
  - Date/Time of discovery of data breach
  - Name of person reporting data breach (could be anonymous)
  - Details of how the data breach was reported
  - Type of data breach: theft, illegal access, insiders, oversight
  - Identify how the breach happened and describe what happened
  - Did you contain the breach (how and when)?
  - What did you implement so it can not happen again (time and date)?
  - How many consumers are affected?
  - What information was lost? (Be very specific with this list, for example, "Did every name lost include a social security number? Did the list include social security numbers of other family members?")
    - Name
    - Address
    - Social Security Number
    - Date of Birth
    - Account Numbers (checking, credit card, etc)
    - Email address
    - Passwords
- Keep a list of all external officials and individuals contacted and involved in the incident (See External Contact List Template in Chapter 6):
  - Forensics
  - Law Enforcement
  - Media
  - Customers
  - FTC
  - Card Processor
- Begin identification of the problem – what is the type of incident?
  - Network/server breach
  - Hardware loss, theft, or destruction
  - Software loss, theft, or destruction
  - Hacking/unauthorized third-party access to system
  - Unauthorized websites that publish sensitive corporate information not approved for public consumption
- What business rules and processes were affected?
- Assign an Incident Number
- Assign an existing incident number and reactivate it (if necessary)
- Assign new incidents their own numbers
- Alert the Incident Lead (use the Internal Contact List in Chapter 6)
- Activate Incident Response Team (use the Internal Contact List in Chapter 6)
- Main goal: Maintain and restore business continuity
- The team should:
  - Collect and/or review the incident documentation and event reports
  - Verify as facts
  - Help assign event severity (if necessary)
  - Alert appropriate external and internal contacts

- Maintain a complete chain of evidence
- Record any and all modifications

Don't get in hurry – thoroughness is more important than speed

- Restrict information – keep it on a need-to-know basis only
- Secure the area and record the information (gather names and contact information of everyone, restrict the area, notate all physical security controls)
- Begin collecting evidence
- Use the Data Breach Investigations Log (See Chapter 6)
- Protect the host servers (Consult with the chosen certified data forensics agency to perform or assist the investigation and disconnect if there is reason to suspect that it has been compromised)
- Restore the host servers (use appropriate monitoring)
- Maintain data integrity -- maintain baselines of normal activity to use for comparison
- Start forensic analysis – how, what, why did this happen?
- Keep detailed logs
- Be consistent with the way you collect and record information throughout the investigation
- Consult legal counsel at the beginning of an investigation
- Develop and record a hypothesis:

    › How does the evidence support/contradict it?
    › What did you do, what evidence did you find, and how did you test the hypothesis?
    › What important interactions took place?
    › Were there any other ideas at the time?
    › Record anything else that helps the company collectively remember things accurately

- Keep the evidentiary chain intact for all electronic and physical evidence
- Treat every incident as if it will lead to a court case (include the time and date for each entry in your notes and sign every page) – remember, all information can become available to lawyers through the information discovery and could become public.
- *Do not include confidential information unless necessary*
- Begin the process of reporting the incident
- Limit communication
- Use discretion when sharing information with employees, card members, card associations, law enforcement, vendors, business partners, etc.
- Be especially careful when communicating with breach victims and the media
- Notify law enforcement at the discretion of upper management. Consider these factors when deciding to contact law enforcement:

    › Severity of the incident
    › Scope of the compromise
    › Recommendations of your lawyer regarding disclosure

- If the data breach could result in harm to a person or business, contact the local police department immediately -- **if you need help identifying which law enforcement agency is the correct one to call, you can contact the Debix Data Breach Hotline at 800-965-7564 for assistance.**

    › Report the situation and be clear about the potential risk for identity theft
    › Contact the local FBI office or the U.S. Secret Service if your local police are not familiar with investigating data breaches
    › Mail theft: Contact the U.S. Postal Inspection Service

See Chapter Seven: *Notifying Customers and Affected Businesses* for more detailed information as well as a sample letter to customers

- Create an Executive-Level Report (approximately 1-2 pages) that includes:
  - High-level description of the incident and its scope
  - Impact on the company
  - Actions taken to prevent further occurrences
  - Recommendations for further action
- Create a Technical Report that includes:
  - Detailed information about the event
  - Detailed information about the investigation
  - All conclusions reached
  - Note: Data used in the report should reference collected evidence and must be verifiable

- Keep all evidence, logs, and data associated with the incident
- Put evidence the tamper-resistant containers and put in limited access, secure storage
- Give original records to Legal and save a copy for company security records
- Grant access to the storage facility only to incident investigators, executive management, and legal counsel
- Records should be kept of all access granted to the storage facility
- Create an itemized inventory of all the evidence, verify it with a law enforcement representative, and have that representative sign and date the inventory list for your records if and when evidence is turned over to law enforcement
- Legal counsel should be present in all meetings with law enforcement

Make sure to use the *Data Breach Investigations Log* in Chapter 6 to record the findings of each investigation – it helps create a useful record of events, which can help with court cases and can help future reactions and prevention of similar events.

6 The Incident Response Workbook

Use this section to start developing a tailored Incident Response Plan. The worksheets serve as a guide to help you properly document events, actions, and timelines.

Maintain this workbook with other documentation so that the source of an incident can be identified and traced and so that the information is immediately available if needed.

IMPORTANT: Continuously update the information in the contact lists and other documents – don't get caught in an emergency with outdated information!

You should also maintain copies of the following:

- The company's written Incident Response Plan
- The company's Service and Operating Level Agreements
- The PCI Data Security standard document
- Notification responsibilities for all card associations (if relevant)
- Complete record of the company's software licensing information
- Current asset and hardware inventory

Internal Contact List Template — Use for Incident Team

Data Breach Internal Contact List (Pre-Incident)

Last Updated: _____
To be updated quarterly

Role	Name	Phone	Email
Executives		Work: Home: Cell:	
Incident Lead		Work: Home: Cell:	
Customer Service		Work: Home: Cell:	
Human Resources		Work: Home: Cell:	
Information Technology		Work: Home: Cell:	
Privacy		Work: Home: Cell:	
Audit		Work: Home: Cell:	
Legal		Work: Home: Cell:	
Security		Work: Home: Cell:	
Compliance		Work: Home: Cell:	

Signature	Date

External Contact List Template — use for all contacts outside the company that might need to be contacted during an incident

Data Breach External Contact List (Pre-Incident)

Last Updated: _____
To be updated quarterly

Role	Name	Phone	Email
Forensics		Work: Home: Cell:	
Police		Work: Home: Cell:	
FBI		Work: Home: Cell:	
Secret Service		Work: Home: Cell:	
Other		Work: Home: Cell:	
Media		Work: Home: Cell:	
Business Partners		Work: Home: Cell:	
Vendors		Work: Home: Cell:	
FTC		Work: Home: Cell:	
Card Processors		Work: Home: Cell:	

Signature	Date

Incident Log

Incident Number	
How was the incident reported?	
Date of Compromise (if known)	Time of Compromise (if known)
Date of Discovery of Compromise	Time of Discovery of Compromise

Incident Assessment					
❒ Suspected	❒ Confirmed				
Type of Data Breach					
❒ Theft	❒ Illegal Access	❒ Insiders	❒ Oversight		
Exposure dates					
Start Date _____	End Date _____				
Severity Level				Data Encrypted?	
❒ 1	❒ 2	❒ 3	❒ 4	❒ Yes	❒ No

	Organization	Contact Name	Phone	Date
Reported by				
Reported to (Incident Lead)				
Government Agency				
Other				

Signature	Date

Incident Log (cont.)

Data Breach External Contact List (Who did you talk to outside your company?)						
Last Updated: _____						
Role	**Contact Name**	**Work Phone**	**Alternate Phone**	**Email**	**Contact Date(s)**	**Contact Time(s)**
Forensics						
Law Enforcement						
Media						
Customers						
FTC						
Card Processors						

Describe how the breach happened
Actions taken to minimize exposure?
Total consumers affected?

Signature	Date

Incident Log (cont.)

Specific data compromised?			
❒ Account #	❒ Magnetic Strip Data	❒ DL	❒ Expiration Date
❒ Name	❒ SSN	❒ CID (4DBC)/CCV	❒ Passwords
❒ Address	❒ Email	❒ DOB	❒ Other

What specific applications/equipment were accessed (if known)?		
Is law enforcement involved?	❒ Yes	❒ No
Need to contact media?	❒ Yes	❒ No
Was extortion involved?	❒ Yes	❒ No
Need to contact customers?	❒ Yes	❒ No
Is computer forensics required?	❒ Yes	❒ No
Website operational?	❒ Yes	❒ No
Did you contain the breach?	❒ Yes	❒ No
How did you contain the breach?		
When did containment occur?	Date _____	Time _____
Describe how containment was implemented		

Signature	Date

Incident Log (cont.)

Forensics	
Computer forensics being completed by	Forensics lead
Forensics Company Contact Information	
What actions were taken?	
Steps taken to prevent recurrence?	

Evidence Collection — Record each piece of evidence you find

Description	Location	Date Found	Time Found	Cardholder Information Exposed (Y/N)	Estimated Exposure	Other Discoveries

Signature	Date

Incident Log (cont.)

Physical Evidence			
Hardware	**Asset/Serial No.**	**Handled By**	**Date**

Electronic Evidence			
Type	**Processing Applied**	**By**	**Date**

Crime Scene — Record all the people present when you first entered the area.	
Name	**Contact Information**

Signature	Date

Incident Log (cont.)

Physical Security Controls Currently in place — Record of all physical security controls in the area		
Type	**Functioning Properly (Yes/**	**Tampered with (Yes/No)**

Recommendations/requests for future event protection

Signature	Date

Incident Forensics — The goal of forensic analysis is to discover evidence that proves the What, Where, When, Who, and how behind an incident.

What happened? (Fact or Hypothesis)

Where did it happen?

When did it happen?

Who did it?

How did they do it?

Signature	Date

Incident Chain of Evidence — Record any information recovered: who was involved, who handled physical and electronic evidence, storage or evidence and shipping records. Recording evidence is critical for any criminal investigation. To maintain a clear chain of evidence, record the following:

Where, when, and who discovered the evidence?

Location of breach	Time/Date	Discovered by	Entry point of breach (if different)

Who has handled or examined the evidence and when?

Evidence description	Handled by	Transferred to	Time/Date

Who has had custody of the evidence, during what time period and where it was stored/secured?

Evidence stored by	Location	Time submitted	Time released	Released to

Has custody changed? (Include how and when the transfer occurred, shipping numbers, etc.)

Evidence shipped by	Reference No	Ship Time/Date	To	Received Time/Date

Signature	Date

Incident Containment — There are certain steps that must be taken during the containment phase of an investigation. Follow the steps below and check off each item as you complete it. Sign at the bottom of the page when you have completed all the steps.

Before shutting down any computer system where an intrusion is suspected, several steps must be taken for collect evidence.
❒ Make a list of processes running on the system.
❒ Check the status of the network interface(s) to see if they are in promiscuous mode.
❒ List all listening ports and active network connections. If possible, include the processes that own the ports and network connections.

Even mundane commands on a host can destroy valuable, forensic evidence. Perform as few operations as possible that access or modify the file system prior to making a bit-for-bit copy of the file system on the compromised host. The preferred process is:
❒ Make two bit-for-bit copies of the compromised host's hard drive; one for restoration purposes and one for forensics.
❒ Remove the original hard drive from the system and secure it as evidence.
❒ Use one copy to aid the creation of a new system disk (copy only data that is known to be safe); then erase the disk using a secure wipe utility.
❒ Use the second copy for forensics.
❒ Use only executables with verified integrity for these tasks to avoid trojan horses and modified binaries.
❒ Create an Incident Response CD-ROM containing the appropriate binaries and documentation necessary for the system. If this is not possible, use binaries from the original installation media

Be aware that many utilities rely on shared object libraries that could be modified by an attacker, so sometimes just running "known good" copies of utilities may not be enough to protect from trojan horses and other malicious code.

Signature	Date

Critical Incident External Contact List

Activity Log							
Role	**Contact Name**	**Company/ Agency**	**Phone**	**Email**	**Contact Date**	**Contact Time**	**Nature of Contact/ Notes**
Forensics							
Law Enforcement							
Media							
FTC							
Card Processors							
Vendors							
Business Partners							

Signature	Date

7 Notifying Customers and Affected Businesses

Determining if notification is necessary and/or legally required is a complex issue impacted by confusing state laws governing jurisdictions where breach victims reside. The considerations below are presented as an overview and are not intended to be inclusive of all issues to be considered. Some examples of how State Laws differ include the definition of personally identifiable information, who must be notified (State Agencies, Law Enforcement, the Credit Reporting Agencies), the timing of the notification to the individuals, and the content of the letter (e.g. in Massachusetts you are not allowed to describe how the event occurred).

Not every incident is going to require the notification of customers and other businesses, depending upon the assessment of the severity, scope, and nature of data that was compromised. If the situation does warrant notification of customers and other businesses, the following information should be taken into consideration:

If you determine you are going to notify a set of individuals in one state because of a specific law, you should notify all individuals effected in the breach. There are many examples where individuals were not treated equally in a data breach and there were legal consequences to the organization. Additionally, even if the individuals identified are overseas, while there is little notification law, it is also recommended that overseas notification is included.

Notifying Individuals

Generally, early notification of individuals whose personal information has been compromised allows them to take steps to mitigate the misuse of their information. In deciding if notification is warranted, consider the nature of the compromise, the type of information taken, the likelihood of misuse, and the potential damage arising from misuse. For example, thieves who have stolen names and Social Security numbers can use this information to cause significant damage to a victim's credit record.

Always consult legal counsel -- most states require that consumers are notified. In some states, you must do so within 30 days. For a summary of the laws, visit www.breachprep.org. Several states also require notification of the Attorney General's office.

When notifying individuals, the FTC recommends that you:

- consult your law enforcement contact about the timing of the notification so it does not impede the investigation
- designate a contact person within your organization who will be in charge of releasing information (this should be designated by your Incident Lead). Give the contact person the latest information about the breach, your official response, and how individuals should respond. Consider sending letters (see example below), posting websites and toll-free numbers as methods of communication with those whose information may have been compromised.

It is important that your notice to consumers clearly describes what the company knows about the compromise. Include how the incident happened, what information was taken (if known), how the thieves have used the information, what actions the company has already taken to remedy the situation, and what responses may be appropriate for the type of information that was compromised. Explain how to reach the contact person within your organization (see Model Letter below).

Consult with your law enforcement contact on exactly what information to include in the consumer notification so your notice does not hamper the investigation. Provide contact information for the law enforcement officer working on the case (as well as your case report number, if applicable) for victims to use, as they can often provide important information about the crime. Be sure to alert the law enforcement officer working your case that you are sharing this contact information. Breach victims should request a copy of the police report and make copies for creditors who have accepted unauthorized charges. The police report is important evidence that can help absolve a victim of fraudulent debts.

The notification should also encourage those who discover that their information has been misused to file a complaint with the FTC at www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338). Information entered into the Identity Theft Data Clearinghouse, the FTC's database, is made available to law enforcement.

Is your organization exempt from notifying consumers?

Organizations may not have to notify affected consumers in the following situations.

Encrypted data - Some states (California and others) do not require notification if the compromised data is encrypted. State laws become very specific on this subject. For example, the exact level of encryption (128 bit) can affect compliance requirements. It is unclear if these current exemption requirements will remain in place or if increasing risks will push states to require organizations to notify even if information is encrypted.

To read the findings of a study on the security of disk encryption by researchers with Princeton University and the Electronic Frontier Foundation, visit: http://blog.wired.com/27bstroke6/2008/02/researchers-dis.html

Questionable Misuse - Some state laws do not require notification unless there is "reasonable belief" that the breached data has been misused.

Public Availability - if the breached information is already publicly available from a government agency, notification may not be required in some states.

Doubtful Use - In some cases where a breach was stopped and there is reasonable doubt that the information was accessed or used by criminals, some states do not require notification.

Is there a risk to your organization of fines, penalties and class action lawsuits if your organization chooses NOT to notify?

Possible Exemptions to notifying (NOT LEGAL ADVICE)

- Data was 128 Bit encrypted.
- There is no evidence or reason to believe the data has been or will be misused.
- The information compromised is already publicly available.
- There's reasonable belief the information was never accessed.
- There's no risk to the organization, such as lost
- business or law suits.

Once you have decided to notify, follow the best practices for notification.

Notification Hints and Tips

- Notification information should be well organized and presented in a way that is direct and concise. It should be obvious from whom the notification is coming and exactly what action is required of the citizen.

- All notification letters and documents should be printed on agency letterhead using high quality paper (60 pounds or better), as many recipients are suspicious of notification letter authenticity.
  - A security envelope should be used as well.
- Expect five - ten percent of consumers who receive notification letters to call the company or agency with questions. Typically, these phone calls last from five to fifteen minutes.
- Call center staffing costs can be minimized by sending notification letters in waves.

Providing Protection for Breach Victims

Once a breach has occurred and a decision to notify has been made, there is a final critical decision that can seriously impact the public's evaluation of how the breach response was handled: "Should your organization provide credit protection service for citizens whose compromised information might be used to commit credit fraud?"

A recent Javelin (June 2008) study stated, Providing a fraud protection solution makes a tremendous difference in customer approval of the breached organization's management and handling of the incident. Javelin data shows that 55% of breach victims that were offered a fraud protection solution were more satisfied with the institution's handling of the incident, compared to those who were not offered anything.

Javelin recommends the following measures that address consumer security concerns and expectations, to institutions in the event of a data breach:

- Given the wide variety of fraud protection solutions and varying features out in the market, engage in comprehensive research of the different services available to understand how they play a role in prevention, detection and resolution.
- Select a solution that is convenient and easy for the breach victim, in terms of enrollment and use, with an understanding of the impact on preventing new accounts fraud.
- Understand that offering a breach solution is a best practice from a customer service standpoint; in other words, do not create a situation in which your customers and/or employees have to request fraud protection assistance. Take a proactive approach by offering the assistance up front.

Avoiding common mistakes:

In recent months, many organizations who did not offer a consumer protection solution in their initial notification quickly found themselves facing an onslaught of negative press and threats of class action lawsuits. In this situation, most organizations reconsider their original decision and elect to offer some form of public protection. This requires the organization to absorb the considerable expense of issuing a second notification letter.

Once the decision has been made to notify, the notification letter is a critical element of communication. The fundamental rule of a successful letter is to be open, honest and direct with the consumer.

It is critical that the affected organization accept responsibility and explain all action being taken to protect their sensitive information.

It is also extremely important to include your website address to give individuals the option of getting additional breach information.

Establishing a toll-free phone breach resource line and publishing the number and hours of operation in the notification letter should also be a priority.

The Model Letter

The model letter below is provided as an example of how businesses might notify people whose names and Social Security numbers have been stolen. In cases of stolen Social Security numbers, it is important that individuals take action to prevent identity theft. For some victims, weeks or months may pass between the time the information is stolen and the time it is misused.

<Date>

<Employee's Name>
<Employee's Address>
<City, State Zip>

<Activation Code>

Dear <Employee's Name>:

Complete Property Management Group has confirmed that the names and social security numbers of <#> employees may have been exposed via <breach details>. We are doing everything possible to protect the personal information of our employees. We regret that the loss of this sensitive data has placed an undue burden of concern on employees and their families.

Complete Property Management Group has researched available options, and has selected Debix to provide you with their Identity Protection service at no cost to you for one year. If you are interested in this service, please enroll online via the following URL: www.debix.com/safe. You will need to go to the aforementioned web site and enter the Activation Code at the top of this letter. Once there, click on "Sign up now" and follow the web site's instructions.

Attached is a one page description of the Debix product. You will need access to the Internet, an e-mail address, and a phone to set up your Debix account.

If you do not have Internet access, you may complete the enclosed mail-in registration form and mail it into Debix.

Once your account is set up, all you will need to be able to use Debix is a telephone, preferably a cell phone. If you do not have a telephone, you will not be able to use Debix. We've chosen Debix since unlike traditional credit monitoring services which only notify you when credit has already been opened in your name, Debix will call you when a creditor is trying to open a new account. Using your phone, you can stop new accounts not initiated by you. Debix is preventative, instead of simply reactive.

Debix will identify new attempts to obtain credit in your name from the date that you set up your account. Debix will not identify any credit accounts that have already been set up in your name.

Please let me take this opportunity to confirm that Complete Property Management Group takes the protection of your personal information very seriously. We apologize for the inconvenience to you of having had your information stolen. We hope that by using Debix you will have the peace of mind of knowing that your credit is being proactively protected, and that you will be able to stop any new accounts that are not authorized by you.

If you have any difficulties opening new accounts, feel free to contact Debix Customer Support. Their normal hours of operation for phone support are Monday - Friday, 9am - 5pm Central, at 888-DEBIXME (1-888-332-4963). If I may be of assistance, please do not hesitate to call me at <XXX-XXX-XXXX.>

Sincerely,

<Name>
<Title>
<Division>
<Company>

What Fraud Prevention Solution to provide the breached individuals.

It is important to note that the FTC and other non-profit organizations do not recommend purchasing Credit Monitoring for individuals but in fact recommend providing consumers a protection that prevents identity theft, such as fraud alerts or an easy to use solution such as Debix.

- The majority of breach victims (56%) prefer a solution that prevents fraudulent use of their information rather than detecting (credit monitoring) 20% or resolving fraud after it has occurred (19%).
- Typically 25%-35% of consumers take advantage of a free offering. This number may increase or decrease depending on:
  - How the individuals are notified: i.e. email, letter, phone call
  - The population of individuals: employees, customers, ...
  - Amount of press the incident receives and timing of the press
  - How the data was compromised: stolen laptop, hack, …
  - Has the data been used by the crooks to steal identities

Other Notification Tips

Cleanse the mailing addresses; typically only 80–90% are deliverable without extra investigation.

- Match against a Delivery Point Validation databases (DPV)
- Match against the Postal Service Change of Address database
- Determine what you intend to do to track down the rest of the addresses and notification
  - Use 3rd party services to find the consumers
    - Use your customer service for outbound calls
- Asses the risk of not notifying this group (not recommended)
- Discuss what to do when you know that individuals' information has been compromised, but you don't yet know exactly what was exposed
- Put an end date on your letter of when the free offer will end
  - Be firm and consistent on end date
- Mail-in registrations must be post-marked no later than the published deadline date. Typically allow 10 days for receipt after post-mark date.
- Plan for those consumers who state they never got a notification but insist on you providing protection

Notifying Affected Businesses

Information compromises can have an impact on businesses other than the one currently breached, such as banks or credit issuers. If account access information (e.g. credit card or bank account numbers) has been stolen from a company that does not maintain the actual accounts, it is important to notify the institution that does maintain that information so that it can monitor the accounts for fraudulent activity. If personal information is collected or stored on behalf of other businesses, notify those businesses of any information compromise, as well.

If the information compromise resulted from the improper posting of personal information on the company website, immediately remove the information from the website. Be aware that Internet search engines store, or "cache," information for a period of time. Contact the search engines to ensure that they do not archive personal information that was posted in error.

8 Data Breach Preparation Checklist

- ☑ **How is an incident reported and documented in your company?**
  - Plan in place to document everything
  - Forensic Integrity, treat a data breach like a crime scene
  - Who contacts law enforcement
- ☑ **Do you know who you are going to call?**
  - Internal Response Team Created
  - Internal Response Team Emergency Contact List
  - External Response Team/Notification List
- ☑ **Vendor contracts in place?**
  - Forensic investigator
  - Mail-house for notification letters
  - Call Center
  - Consumer Fraud Protection
- ☑ **Process for determining if notification is required?**
  - Legal counsel understands laws
  - Timeline obligations and specific state laws (based on where individual lives not the company)
- ☑ **If notification is required is your organization prepared?**
  - PR – what will be said to the public
  - Who authors and approves the notification letter
  - How will it be sent
  - What will be provided to protect the individuals
  - Call Center Scripts
  - Website with FAQ and additional information
- ☑ **How will this effort be funded?**

For More Information

This publication provides general guidance for a company that has experienced a data breach. For more individualized guidance, you may contact the Debix Data Breach Hotline at 800-965-7564. To order re-prints of this publication email sales@debix.com.

Other Valuable Complimentary Resources:

Replay of a Javelin Webinar, When a Data Breach Occurs What do Consumers Expect, www.debix.com/webinar and a copy of the research report can be downloaded at www.debix.com/javelin

Replay of a presentation by Hunton & Williams and Tenet Health Care: The Legal Implications of a Data Breach www.debix.com/legalwebinar

Interactive Map of Notification Laws http://www.csoonline.com/article/221322/CSO_Disclosure_Series_Data_Breach_Notification_Laws_State_By_State

Identity Theft Study, May 2008 www.debix.com/research

Identity Theft Resource Center, www.idtheftcenter.org

Sources:

Consumer Survey on Data Breach Notification, Javelin Strategy and Research, June, 2008

Data Breach Notification and Responsibilities: Agency Responses and Credit Monitoring Options White Paper, Debix, Inc., 2008

Incident Response Workbook, American Express Travel Related Services, Inc., 2006

The Legal Implications of a Data Breach and Building an Optimal Breach Response Plan Web Seminar, Debix, Inc, Hunton and Williams, Tenet Healthcare, 2008

Ponemon Institute, Consumers Report Card on Data Breach Notification March, 2008