Data Breach Response Guide

By Experian® Data Breach Resolution
2013-2014 Edition

Experian®

Table of Contents

Legal Notice

The information you obtain herein is not, nor intended to be, legal advice. We try to provide quality information but make no claims, promises or guarantees about the accuracy, completeness or adequacy of the information contained. As legal advice must be tailored to the specific circumstances of each case and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent legal counsel.

Introduction

Preparation is the Best Defense

With 267 million records being exposed in data breaches in 2012, experiencing a breach may be inevitable*, but the bank-breaking costs often associated with them doesn't have to be. In fact, a Ponemon study reveals that organizations can greatly reduce the cost of a data breach by having an incident response plan, a strong IT security posture and a Chief Information Security Officer.** That's why this Response Guide is a vital tool that can be used in defense against data breaches.

Inside, you'll learn why it's important to have an incident response plan, how to create one and what to do during the first 24 hours of a breach. We'll explain what you need to know about notifying your customers, patients or employees. The guide also has the latest information on the HIPAA Omnibus Rule and upcoming federal legislation on breach notification laws. After you create your response plan, it's important to test and update it. Recommendations for updating your plan are included in this publication, along with some helpful resources.

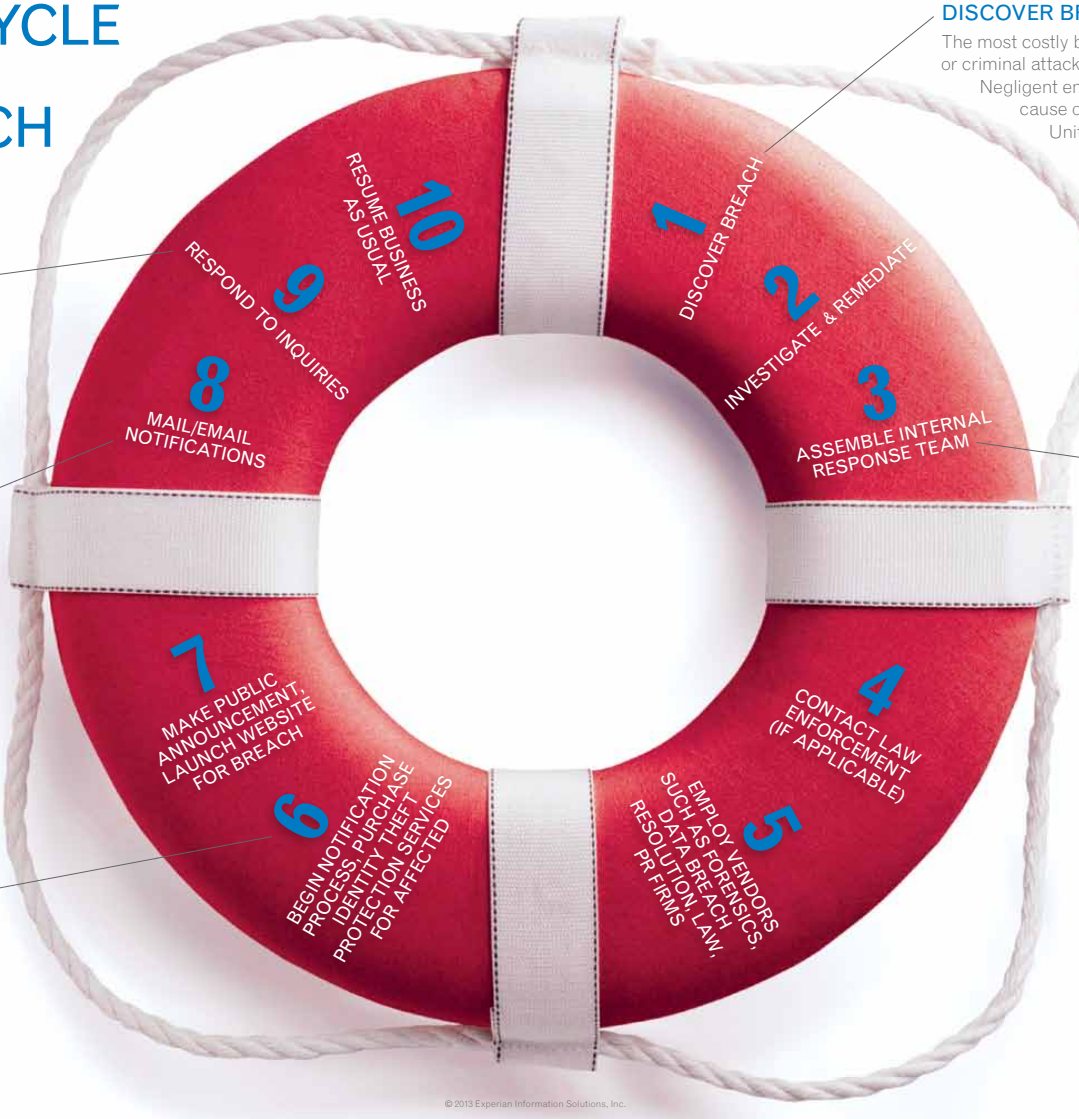
So please, take a little time to review this guide, and if you don't have an incident response plan, use this to help create one. It could mean the difference between a breach that causes a brief disruption and one that causes a major meltdown.

Sincerely,

Michael Bruemmer

Vice President, Experian Data Breach Resolution

LIFE CYCLE OF A BREACH



DISCOVER BREACH

The most costly breaches are malicious or criminal attacks, such as hacking. Negligent employees are the top cause of data breaches in the United States.[1]

ASSEMBLE INTERNAL RESPONSE TEAM

Organizations that employ a Chief Information Security Officer (CISO) with enterprise-wide responsibility can reduce the cost of a data breach by 35%.[2]

RESPOND TO INQUIRIES

During a recent breach, Experian® Data Breach Resolution handled about 6,000 calls for a client in a single day.

MAIL/EMAIL NOTIFICATIONS

Consumers want to see facts about the breach, information about the risks they may face, steps they can take to protect themselves and an offer for credit monitoring or identity protection included in a breach notice.[4]

BEGIN NOTIFICATION PROCESS

Did you know that 46 states, the District of Columbia, Puerto Rico and the Virgin Islands have laws requiring notification of data breaches?[3]

Experian

1 2011 Cost of a Data Breach Study: United States, Symantec Corp. and Ponemon Institute.

2 2011 Cost of a Data Breach Study: United States, Symantec Corp. and Ponemon Institute.

3 Congressional Research Service Report for Congress, 2012

4 Consumer Study on Data Breach Notification, Ponemon Institute, 2012

Footnotes

*2012 Data Breach QuickView Report, Open Security Foundation and Risk Based Security, Inc.

**2013 Cost of a Data Breach Study, Ponemon Institute, May 2013

Data Breach Preparedness

Why Create a Data Breach Preparedness Plan?

The average total cost of a typical breach is $5.4 million in the United States[1]. Some breaches cost much more than that, which is why it's so important to be prepared. Multiply that by the hundreds, thousands – even millions – of records that are typically compromised in one breach and you begin to realize just how costly a data breach is.

A data breach can take a toll on a company of any size. Having a breach preparedness plan in place can help you act quickly if one occurs. Acting quickly can help to prevent further data loss, significant fines and costly customer backlash.

Look to C-level executives to make data breach preparedness a continuing priority for the entire company.

Incident Preparedness

In the midst of a data breach is no time to decide how you're going to handle one or who's going to take care of what. So develop your response plan and build your response team before you need them.

Your team will coordinate efforts between your company's various departments and fulfill two primary functions:

1. The immediate function is to develop the data breach response plan and prep the entire organization on proper protocol during a breach.
2. Then, if a breach does occur, the team will implement the response plan, engage the proper resources and track the efforts.

Assemble Your Response Team

Incident Lead

Start by selecting your incident lead – think of someone from an internal or external legal department or a Chief Privacy Officer. Your incident lead should be able to:

- Manage and coordinate your company's overall response efforts and team.
- Act as an intermediary between C-level executives and other team members to report progress and problems.
- Identify key tasks, manage timelines and document all response efforts from beginning to end.
- Outline the budget and resources needed to handle a breach.
- Summarize the steps needed to assess the scope of a breach.
- Ensure contact lists remain updated and team members remain ready to respond.
- Analyze response efforts post-breach to better prepare the company and team for the next incident.

Your incident lead, as well as every response team member, needs a backup.

1 2013 Cost of a Data Breach Study: Global Analysis, Ponemon Institute

Data Breach Preparedness Continued

Outline a structure of internal reporting to ensure executives and everyone on the response team is up to date and on track during a data breach.

Here is a quick look at the other members you will want on your team and what their responsibilities might entail:

Executive Leaders

Include the company's key decision makers as advisors to your data breach response team to help ensure you have the needed leadership, backing and resources to properly develop and test your plan.

IT & Security

Your IT and security teams will likely lead the way in catching and stopping a data breach but not necessarily in investigating it. You'll want someone from IT and/or security on your response team to:

- Train personnel in data breach response, including securing the premises, safely taking infected machines offline and preserving evidence.
- Work with a forensics firm to identify the compromised data and delete hacker tools without compromising evidence.

Legal & Privacy

Rely on internal and/or external legal, privacy and compliance experts to shape your data breach response and help minimize the risk of litigation and fines. Your legal representatives will need to:

- Determine whether it's necessary to notify affected individuals, the media, law enforcement, government agencies and other third parties, such as card holder issuers.
- Establish relationships with any necessary external counsel now – not once a breach occurs.
- Review and stay up to date on both state and federal laws governing data breaches in your industry.

PR

Depending on the size of the data breach and your industry, you may need to report the breach to the media and/or notify affected individuals. Your response team member from PR or communications will need to:

- Identify the best notification and crisis management tactics before a breach ever occurs.
- Handle any information leaks regarding a breach.
- Track and analyze media coverage and quickly respond to any negative press during a breach.

Customer Care & HR

Data breaches may affect both your customers and your employees so appoint representatives from both customer service and HR to your response team to provide needed support. Your representatives should:

- Create simulation training for your customer service representatives that demonstrates how their roles would change during a data breach.
- Outline a plan for setting up a data breach hotline for customers and/or employees if a breach occurs. Determine in advance if you'll use internal or external resources.

Law Enforcement

Depending on the severity of a data breach, you may need to involve law enforcement. Take time to collect all of the appropriate contact information now so you can act quickly if a breach does occur.

- Identify which state and federal authorities, including the FBI and Secret Service, to contact in the event of a data breach involving criminal activity.
- During a breach, be sure everyone on the data breach response team is aware of any law enforcement directives so the investigation isn't interrupted.

Data Breach Resolution Provider

Contract with a data breach resolution vendor in advance of a breach to secure the best rates. Your vendor should be able to:

- Assign you a dedicated account manager to handle escalations, tracking and reporting.
- Handle all aspects of notification, including drafting, printing and mailing letters and address verification.
- Offer proven identity protection, comprehensive fraud resolution and secure call center services for affected individuals.

Clearly defined steps, timelines and checklists help keep everyone focused during the stress of a data breach.

Data Breach Preparedness Continued

Preparedness Training

In addition to a company-wide focus on data security and breach preparedness, department-specific training should trickle down from the data breach response team. Each member of the team has a unique responsibility to apply prevention and preparedness best practices to his/her own department.

- Work with employees to integrate data security efforts into their daily work habits.
- Develop data security and mobile device policies, update them regularly and communicate them to business associates.
- Invest in the proper cyber security software, encryption devices and firewall protection. Update these security measures regularly.
- Limit the type of both hard and electronic data someone can access based on job requirements.
- Establish a method of reporting for employees who notice that others aren't following the proper security measures.
- Conduct employee security training/re-training at least once a year.

While your data breach response team coordinates your preparedness and response efforts, everyone in your company plays a role in data security. Therefore everyone should be involved in data breach preparedness.

Prepare for the Worst So You Can Respond at Your Best

Be sure everyone on your data breach response teams understands their specific responsibilities –both in preparing for and responding to a breach. The contact forms in the back (See Page 22) will give you a starting point for organizing the contacts for your team. Be sure to update and distribute the contact list every quarter so everyone is always prepared to act.

Data Breach Incident Response

One out of five organizations do not have a formal incident response plan in place.[1]

Acting quickly and strategically following a data breach can help you regain your security, preserve evidence and protect your brand. Always collect, document and record as much information about the data breach and your response efforts, including conversations with law enforcement and legal counsel, as you can.

The First 24 Hours Checklist

Panicking won't get you anywhere once you've discovered a data breach. Accept that it's happened and immediately contact your legal counsel for guidance on initiating these 10 critical steps:

- ☐ **Record the date and time** when the breach was discovered, as well as the current date and time when response efforts begin, i.e. when someone on the response team is alerted to the breach.
- ☐ **Alert and activate everyone** on the response team, including external resources, to begin executing your preparedness plan.
- ☐ **Secure the premises** around the area where the data breach occurred to help preserve evidence.
- ☐ **Stop additional data loss.** Take affected machines offline but do not turn them off or start probing into the computer until your forensics team arrives.
- ☐ **Document everything** known thus far about the breach: Who discovered it, who reported it, to whom was it reported, who else knows about it, what type of breach occurred, what was stolen, how was it stolen, what systems are affected, what devices are missing, etc.
- ☐ **Interview those involved** in discovering the breach and anyone else who may know about it. Document your investigation.
- ☐ **Review protocols** regarding disseminating information about the breach for everyone involved in this early stage.
- ☐ **Assess priorities and risks** based on what you know about the breach.
- ☐ **Bring in your forensics firm** to begin an in-depth investigation.
- ☐ **Notify law enforcement,** if needed, after consulting with legal counsel and upper management.

1 IT Security and Privacy Survey, Protiviti Risk & Business Consulting, May 2013

Data Breach Incident Response Continued

Once you have begun or completed the 10 initial steps, stop briefly to take inventory of your progress. Ensure your preparedness plan is on track and continue with these next steps:

Fix the Issue that Caused the Breach

- Rely on your forensics team to delete hacker tools.
- Determine if you have other security gaps or risks and address them.
- Put clean machines online in place of affected ones.
- Ensure the same type of breach cannot happen again.
- Document when and how the breach was contained.

> Don't just document what steps you take. Document why you took them.

Continue Working with Forensics

- Determine if any countermeasures, such as encryption, were enabled when the compromise occurred.
- Analyze backup, preserved or reconstructed data sources.
- Ascertain the number of suspected people affected and type of information compromised.
- Begin to align compromised data with customer names and addresses for notification.

> Any data breach could lead to litigation. Work closely with your legal and compliance experts to analyze risks and ways to mitigate them, such as proper documentation and notification.

Identify Legal Obligations

- Revisit state and federal regulations governing your industry and the type of data lost.
- Determine all entities that need to be notified, i.e. customers, employees, the media, government agencies, regulation boards, etc.
- Ensure all notifications occur within any mandated timeframes.

Report to Upper Management

- Compile daily breach reports for upper management.
- The first report should include all of the facts about the breach as well as the steps and resources needed to resolve it.
- Create a high-level overview of priorities and progress, as well as problems and risks.

> Never send sensitive information, such as SSNs, unnecessarily to vendors supporting the breach.

Identify Conflicting Initiatives

- Make the response team and executives aware of any upcoming business initiatives that may interfere or clash with response efforts.
- Decide whether to postpone these efforts and for how long in order to focus on the breach.

Alert Your Data Breach Resolution Vendor

- Contact your pre-selected vendor to choose business services for your company and protection products for individuals affected in the breach.
- Determine how many activation codes you will need for the protection products based on the number of affected individuals.
- Draft and sign a data breach resolution agreement if you do not have a pre-breach agreement in place.
- Engage your vendor to handle notifications (learn more in the next section: Breach Notification) and set up a call center so affected individuals have access to customer service representatives trained on the breach.
- Work closely with your account manager to review incident reporting and metrics.

Keep Your Response Efforts on Track

Resolving a data breach requires a coordinated effort between your response team members, executives, external resources, law enforcement, forensic firm and data breach resolution vendor. Staying organized and documenting every step and decision should be a top priority. Act quickly to minimize the damage but don't lose sight of your priorities or of the needs of affected individuals.

Data Breach Notification

Not all breaches require notification. If your data was encrypted or an unauthorized employee accidentally accessed but didn't misuse the data, you may not need to notify. Be sure to seek and follow legal advice before deciding to forgo notification.

Sixty days. That's generally the amount of time businesses have to notify affected individuals of a data breach, assuming notification is required by law. The countdown starts the moment a breach is discovered. Depending on varying circumstances, you may have even less time.

Notification Challenges to Consider

Your legal counsel can help you determine if any of these or other challenges may impact your notification process:

- Certain state laws and federal regulations shrink the timeline to 30 or 45 days, meaning there's no time to waste in verifying addresses; writing, printing and mailing notification letters; and setting up a call center and other services for affected individuals.
- Some states mandate specific content for you to include in your notification letters. This can include toll-free numbers and addresses for the three major credit bureaus, the FTC and a state's attorney general.
- Notification may be delayed if law enforcement believes it would interfere with an ongoing investigation.
- Multiple state laws may apply to one data breach because jurisdiction depends on where the affected individuals reside, not where the business is located.
- If some affected individuals live in a state that mandates notification and others live in a state that doesn't, you should notify everyone so you're not singled out for inequality.
- Keep in mind that some recipients will think the notification letter itself is a scam.

Mishandling notifications can lead to severe consequences, including fines and other unbudgeted expenses. It could also tarnish your brand reputation and customer loyalty, leading to potential revenue loss.

What you say, how you say it and when you say it are all important elements of data breach notification.

Organizations can improve the outcome of a data breach if they contract with vendors ahead of time. That way, if a breach does occur, you would already have a forensics partner, a privacy attorney and a breach notification partner in place and ready to hit the ground running.

Successful Notification

It is your responsibility to determine the deadlines for notification according to state law. The notification deadline is a heavy weight on top of the already burdensome and stressful ordeal of a data breach. One way to help eliminate some of that stress is determining how you'll handle notifications before a breach occurs. Lining up a data breach resolution provider in advance can help shave off both time and stress from your response efforts. In many cases, you can even save money by signing a contract with a provider in advance of a breach.

What to Look For in a Data Breach Resolution Provider

Above all, your data breach resolution provider should make security a top priority throughout the notification process. Unlike standard direct mail production, data breach notification requires critical service and quality assurance elements to ensure compliance. Look for one vendor that can seamlessly handle notifications from beginning to end and make a positive impact on your brand.

Data Breach Notification Continued

Account Management

Amid the stress of a data breach, you'll appreciate having an experienced account manager that streamlines and simplifies the notification process for you. Your account manager should know the ins and outs of your breach, your priorities and your deadlines. That can only happen if you have an assigned, dedicated account manager. Otherwise you'll waste valuable time working with a different account manager every time you call.

Be sure to double check and test phone numbers and URLs in all communications.

Critical Notification Services

A full-service data breach resolution vendor should offer a range of options, as well as strict security standards, to fit your business needs and the scope of your breach:

Comprehensive letter management

- Templates for you to customize to your company and breach
- Management of multiple letter versions based on state regulations, affected individuals (employee vs. consumer audience), etc.
- Four-color or black-and-white letters
- Professional printing with your company logo and electronic signature

Address validation & delivery

- Return mail management to securely handle and discard returned notification letters
- Certified address cleansing confirmed against USPS standards
    - Coding accuracy support system – address standardization
    - Delivery point validation – validate address exists
    - Locatable address conversion system – update address
- National change of address verified by USPS
- Deceased and criminal identification to minimize unnecessary mailings
- First-class postage

Quality assurance for printing and fulfillment

- Dedicated quality assurance personnel
- Robust integration controls to ensure 100% produced and mailed
- Tier-1 data security protocols with a secure/restricted access production area
- Ongoing training and certification of personnel
- 24/7 camera monitoring with secure archiving

Reporting for compliance

- Daily inventory reporting
    - Initial mailings
    - Address changes
    - Undeliverable and returned letters
- Electronic letter copies for proof of notification
- USPS postal delivery report

Notification letters may contain sensitive data and require secure handling through every stage of drafting, printing and mailing.

As dictated by state law, a notification letter may need to include:

- Clear language, not industry jargon, that the average person could understand.
- A toll-free phone number for individuals wanting additional information.
- Details about the type of data lost and how it was lost, unless prohibited by law.
- Next steps to help affected individuals regain their security, such as signing up for a complimentary identity protection product.

Legal Notice: Always check with your legal counsel in order to identify the notification requirements for your specific incident.

[Company Logo]
[Return Address]
[Date]

An example notification letter.

[Recipient's Name]
[Address]
[City, State, Zip (shows thru outer envelope window)]

Important Security and Protection Notification.
Please read this entire letter.

Dear [Insert customer name]:

I am contacting you regarding a data security incident that has occurred at [Insert Company Name]. This incident involved your [describe the type of personal information (of your client) that may be potentially exposed due to the breach incident (i.e., Social Security number, etc.)]. As a result, your personal information may have been potentially exposed to others. Please be assured that we have taken every step necessary to address the incident, and that we are committed to fully protecting all of the information that you have entrusted to us.

[Insert Company Name] takes this incident seriously and is committed to assuring the security of your data. To help protect your identity, we are offering a complimentary one-year membership of Experian's ProtectMyID® Elite. This product helps detect possible misuse of your personal information and provides you with superior identity protection services focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE That You Enroll By: [date]
2. VISIT the ProtectMyID Web Site: **www.protectmyid.com/enroll** or call **1-XXX-XXX-XXXX** to enroll
3. PROVIDE Your Activation Code: [code]

Once your ProtectMyID membership is activated, your credit report will be monitored daily for 50 leading indicators of identity theft. You'll receive timely Surveillance Alerts™ from ProtectMyID on any key changes in your credit report, a change of address, or if an Internet Scan detects that your information may have been found in an online forum where compromised credentials are traded or sold.

ProtectMyID provides you with powerful identity protection that will help detect, protect and resolve potential identity theft. In the case that identity theft is detected, ProtectMyID will assign a dedicated U.S.-based Identity Theft Resolution Agent who will walk you through the process of fraud resolution from start to finish for seamless service.

Your complimentary 12-month ProtectMyID membership includes:

- Credit Report: A copy of your Experian credit report
- Surveillance Alerts
  - o Daily 3 Bureau Credit Monitoring: Alerts you of suspicious activity including new inquiries, newly opened accounts, delinquencies, or medical collections found on your Experian, Equifax, and TransUnion credit reports.
  - o Internet Scan: Alerts you if your Social Security Number or Credit and/or Debit Card numbers are found on sites where compromised data is found, traded or sold.
  - o Change of Address: Alerts you of any changes in your mailing address.
- Identity Theft Resolution: If you have been a victim of identity theft, you will be assigned a dedicated, U.S.-based Experian Identity Theft Resolution Agent who will walk you through the fraud resolution process, from start to finish.
- Lost Wallet Protection: If you ever misplace or have your wallet stolen, an agent will help you cancel your credit, debit and medical insurance cards.
- $1 Million Identity Theft Insurance*: As a ProtectMyID member, you are immediately covered by a $1 million insurance policy that can help you cover certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Activate your membership today at www.protectmyid.com/enroll
or call 1-XXX-XXX-XXXX to register with the activation code above.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at **XXX-XXX-XXXX**.

[Insert a detailed explanation about the circumstances surrounding the breach incident (e.g., this information was contained on a computer that was stolen from our offices.), what investigative steps have been taken, if you are aware of any fraudulent use of the information, explain the steps your company has taken to ensure that this issue won't happen again, e.g., better secure our computers and facilities and include any and all other relevant facts]

We sincerely apologize for this incident, regret any inconvenience it may cause you and encourage you to take advantage of the product outlined herein. Should you have questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact us at [insert company phone number].

Sincerely,
[Signed by appropriate executive - president, CEO or VP HR]

* Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Legal Notice: Always check with your legal counsel in order to identify the notification requirements for your specific incident.

Data Breach Notification Continued

10 Steps of Working with a Data Breach Resolution Vendor

1

Client identifies affected individuals, determines notification requirements and contacts vendor

2

Vendor assigns a dedicated account manager and conducts kickoff meeting

3

Client selects products and services and signs a data breach resolution agreement

4

Vendor provides samples of notification letters and options for consumer protection products

5

Client provides final data files and letter materials

6

Vendor aligns affected individuals with addresses and generates product activation codes

7

Vendor preps call center using incident-specific FAQs

8

Client and vendor jointly approve final letter

9

Vendor oversees mailing, delivery and re-mailing from secure fulfillment center

10

Vendor provides regular reporting and metrics to client to track engagement

Legal Notice: Always check with your legal counsel in order to identify the notification requirements for your specific incident.

Healthcare Data Breach

Look for sizable spike in reported breaches under HIPAA Omnibus Rule

Perhaps the only thing certain about the healthcare industry these days is change. New technology, advanced procedures and innovative treatments keep the industry evolving, and along with all of the change, comes more regulation.

In addition to the complex web of state regulations, there are also new federal regulations imposed in the final HIPAA Omnibus Rule, which became effective in March 2013. Organizations have until September 2013 to comply. Plus, a new HIPAA audit program is scheduled to begin in 2014.

The purpose of the HIPAA Omnibus Rule is to strengthen the privacy and security of patients' Protected Health Information.

The purpose of the Omnibus Rule is to offer better protection to consumers. Specifically, the U.S. Department of Health and Human Services (HHS) designed it to strengthen the privacy and security of patients' Protected Health Information (PHI). So really, that's good news for patients and for the healthcare organizations that want to keep their business.

But along with the rewards, comes work. That means healthcare organizations and their business associates need to be more diligent about the way they secure – and handle – PHI or they will face stiffer fines. The rule also means there is likely to be a sizable spike in the number of reported breaches because the new regulations change the criteria; now more incidents will be considered breaches.

Here is a summary of the Omnibus Rule as it relates to healthcare data breaches:

Breach Redefined to Include More Incidents

The definition of a healthcare breach has been broadened to include more incidents. This was accomplished by eliminating the "harm standard" from the 2009 Interim Final Rule. The omnibus supersedes the 2009 rule. So what is the difference between the definition then and now?

Well in 2009, organizations had to assess whether a significant risk of "harm" would be caused to the affected individuals. This determined whether an incident qualified as a breach.

Now, organizations have to determine the probability of the PHI being compromised, regardless of whether it would cause harm to the affected individuals. So, if an organization determines there is a high probability of the PHI being compromised, then the incident would be considered a breach. If there is a low probability, it wouldn't be considered a breach. In order to make these determinations, organizations must conduct a comprehensive risk assessment. Organizations can forego the assessment if they notify all of the affected individuals.

HHS made these changes because it believed the language in the 2009 rule could be misconstrued and implemented incorrectly.

Directly Liable: Business Associates and Subcontractors

Business associates and their subcontractors are now directly liable under the new HIPAA Security Rule and various provisions of the Privacy Rule. These businesses will face the same civil and criminal penalties as healthcare organizations, if they violate the regulations.

Factors to Consider During a Risk Assessment

1) What was the nature and extent of the PHI involved (including the types of identifiers and likelihood of re-identification)?
2) Who was the unauthorized person who used the PHI?
3) Was the PHI actually acquired or viewed by an unauthorized person?
4) To what extent has the risk to the PHI been mitigated?

Healthcare Data Breach Continued

In addition, more types of businesses are being considered business associates. Basically any business that handles an organization's PHI is considered a business associate. This includes attorneys, accountants, third-party administrators, cloud providers and, sometimes, financial institutions. Financial institutions are exempt if they only do payment processing. However, if they provide back office services, help with accounts payable or provide other services in which they handle PHI, they will have to comply.

The new regulations not only require business associate agreements (BAAs) between the healthcare organization and business associate but also between the business associate and its subcontractor. In the past, BAAs were just required between the healthcare organization and business associate. It's important to outline your specific PHI handling policies in your BAAs.

Stiffer Penalties and How to Minimize Them

Along with the new regulations, come stiffer penalties, but only for repeat offenders. First-time violators will still face fines of up to $50,000 per violation, per year.[1] Those who have multiple violations, however, can face a devastating fine of $1.5 million.[1] The Omnibus Rule eliminates the lower tier of fines for repeat offenders.

If a violation does occur, organizations can save money by responding quickly. HHS may reduce penalties for organizations that work fast to resolve the problem. HHS will also look at other actions your organization takes to mitigate the damage. For instance, you may want to make changes to your policies to try to prevent a similar incident from occurring again.

If an employee's negligence causes a breach, then the organization needs to impose sanctions against that individual. And, obviously, organizations need to cooperate with authorities and respond accurately and timely to requests for information. Failure to cooperate can result in significantly higher fines.

Of course the best way to save money would be to avoid getting a fine in the first place. This can be done by having procedures to respond to a breach, policies to safeguard PHI and employee training so everyone understands the rules.

Omnibus Clarifies Notification Issues

The Omnibus Rule clarifies some gray areas regarding notification. Covered entities, primarily meaning healthcare organizations and insurance companies, are responsible for notifying affected individuals, though they can delegate this responsibility to a business associate that causes a breach.

When HHS says a breach involving 500+ people needs to be reported "immediately," it means at the same time that companies notify the individuals whose PHI was exposed. The rule also states if an organization is required to publicize the breach, it has to send a press release to media outlets in the region where the affected individuals live. Organizations can't meet this requirement by posting a release on their website.

In a Nutshell

What all of this boils down to is that healthcare organizations and business associates need to become savvier about safeguarding PHI. You should take every precaution possible to try to prevent a breach. But if one does occur, you should have an incident response plan in place to respond quickly. Being prepared for a breach can help you keep patients or customers, avoid litigation and protect your brand.

With all of the new regulations, being prepared for a data breach can mean more than getting back to business quickly. It can also mean saving hundreds of thousands of dollars – perhaps even millions.

Snapshot of Omnibus Rule

Let's face it, the final HIPAA Omnibus Rule is complicated. So here is a checklist of the key provisions that will help keep you in compliance with the new regulations.

- ☑ The definition of a healthcare breach is broader now because of the elimination of the "harm standard." That standard meant organizations had to assess whether there would be significant risks of "harm" caused to the individuals whose Protected Health Information (PHI) were exposed. Now, organizations have to determine the probability of the PHI being compromised, regardless of whether or not it would cause harm to the affected individuals.
- ☑ A comprehensive risk assessment is required to determine if an incident is a data breach.
- ☑ Business associates and their subcontractors are directly liable for violations. They will face the same fines and penalties as healthcare organizations and other covered entities.
- ☑ Fines are stiffer for repeat offenders, meaning those with more than one violation can face a fine of $1.5 million.[1] The rule eliminates the lower tier of fines for repeat offenders.
- ☑ When the U.S. Department of Health and Human Services says a breach needs to be reported "immediately," it means simultaneously to notifying individuals that their PHI was exposed.
- ☑ If an organization is required to publicize a breach, it must send a news release to media outlets close to where the affected individuals reside. It cannot simply post a press release on its website.

Legal Notice: Always check with your legal counsel in order to identify the notification requirements for your specific incident.

1 U.S. Department of Health and Human Services, Federal Register, January 25, 2013

Legal Landscape

A work in progress

Courtesy of Tony Hadley, Sr. VP, Government Affairs and Public Policy, Experian®
Jeremy Hancock, Manager, Government Affairs and Public Policy, Experian
Last Updated: July 2013

National data breach legislation, despite some high-profile incidents, continues to languish on the federal level. But watch for that to change as the 113th Congress heads into the final stretch of its first session. The second session begins in January 2014.

Both Congress and the Obama Administration are increasingly interested in enacting a national data breach notification law to replace the current patchwork of state laws. Currently, there are 46 states that have notification laws, plus the District of Columbia, Puerto Rico and the Virgin Islands. In fact, only four states don't have such laws. They are Alabama, Kentucky, New Mexico and South Dakota.

In the previous legislative session, several bills were passed by Committee in both houses, but failed to gain enough support to be signed into law. In addition, attempts to include data breach amendments to cyber security legislation proved unsuccessful. It is expected, however, that data breach legislation will be a top priority for lawmakers in the upcoming year. Here's a glimpse of the landscape for data breach legislation.

House of Representatives

During the last session of Congress, the House Commerce Manufacturing and Trade Subcommittee passed the SAFE Data Act (H.R. 2577), but the bill was never taken up by the full Energy and Commerce Committee. Congressman Lee Terry (R-NE), who took over as Chairman of the Subcommittee, has signaled that he intends to propose a data breach bill again this session.

In addition, the House Judiciary Committee is currently working on cyber security legislation that would amend the Computer Fraud and Abuse Act. The bill is expected to:

- Establish a data breach notification requirement, requiring consumers to be notified no later than 14 days after the breach.
- The data breach sections would not apply to financial institutions subject to Title V of GLBA.

Senate

In the Senate there will be several measures introduced to establish a national data breach notification law.

On the Senate Commerce Committee, Chairman Jay Rockefeller (D-WV) is likely to introduce a data breach provision as part of a larger cyber security package, as he did in the last legislative session. Senator Pat Toomey (R-PA) has also signaled that he intends to reintroduce a data breach bill similar to the one he put forward in 2012. The Judiciary Committee passed data breach measures last year, but they failed to reach the full Senate. The committee will continue to hold hearings this session examining the issue.

No single federal law or regulation governs the security of all types of sensitive personal information. As a result, determining which federal law, regulation or guidance is applicable depends in part on the entity or sector that collected the information and the type of information collected and regulated. As a result, data breach notification requirements have largely been left to state legislatures.

Legal Considerations Continued

The Obama Administration

The White House also released a policy statement in April 2013 on H.R. 624, the Cyber Intelligence Sharing and Protection Act, which advocates for the inclusion of a national data breach reporting requirement in any cyber security legislation.

The White House's cyber security draft proposal released in May 2011 included a data breach provision, which in part stated the following:

- A Definition of Personal Information: PI, as proposed, is the same under H.R. 2577 and S. 1151, but this proposal authorizes the FTC to modify the definition of PI by rule.
- Notification requirements: Notice must be provided to consumers no later than 60 days, unless the entity can demonstrate that a delay is necessary. Federal officials would need to be notified if the breach exceeds 5,000 individuals or involves a database that is either owned by the federal government or includes the PI of 500,000 people nationwide. Credit bureaus must be notified in the event that more than 5,000 individuals are informed of a breach.
- Penalties: State attorneys general could bring civil actions to recover the penalties in the amount of $1,000 per day, up to $1 million per violation.

Definition of Sensitive Information

At the heart of all notification laws is the protection of personal information that can uniquely identify an individual and pose a risk for identity fraud. Generally, personal information is defined as a first name/initial and last name in addition to another piece of identifying information, such as a Social Security number, credit or debit card number or an account number. Over time, policy makers have begun to consider whether additional identifying elements should be considered sensitive information. Some states have expanded the law to include medical and health insurance and taxpayer identification numbers. There is also a blurring of the distinction between identifiable information and anonymous or de-identified information. This has led to the consideration of notification in the event of a breach of sensitive information independent of a name, such as email addresses that could be associated with a financial account.

Protection of Healthcare Data

The use and protection of patients' Protected Health Information (PHI) is regulated at the federal level under the Health Insurance Portability and Accountability Act (HIPAA). The law was modified in March 2013 when the HIPAA Omnibus Final Rule took effect.

The Omnibus Rule broadens the definition of a healthcare breach to include more incidents, increases penalties and makes more entities liable for violations. In addition, breaches affecting 500 or more individuals must be reported to major media outlets and the U.S. Department of Health and Human Services. States legislatures have also started looking at expanding their breach notification laws to also include sensitive health information. For more information on the HIPAA Omnibus Rule see page 13.

State Attorneys General Get More Involved

As state attorneys general have gotten more involved in the oversight of breach notices, a number of states have proposed a new requirement to report breaches to the attorney general's office. Proposals have ranged from notification in the event of any breach, no matter the size, to setting thresholds, such as the information of 500 individuals breached. State legislation also includes looking at the timing of when notices are sent out, from as soon as reasonably possible, to a more prescriptive number of days.

Expansion of Notification Content

State policy makers are considering expanding existing breach notification laws by being more prescriptive about what information must be included in a notice. This includes information such as the time of the breach and the type of data affected.

Focus on Penalties

As the number of data breaches and the impact on consumers increase, regulators are focused

Legal Notice: Always check with your legal counsel in order to identify the notification requirements for your specific incident.

Legal Considerations Continued

on the appropriate level of fines for organizations that are not compliant with breach notification laws. Some proposals set fines for each breach of an individual's information while others look at leaving the fines up to regulators with a large cap.

New State Notification Laws

In the last two years, at least 13 states have considered an expansion to the existing data breach notification laws and five approved new requirements.

Vermont

At the center of new requirements in Vermont is the timing of notification to consumers and the state attorney general. The law states that organizations must notify affected consumers no later than 45 days after they discover a breach, making Vermont the fourth state to impose a 45-day requirement – joining Florida, Ohio and Wisconsin. Organizations must notify the state attorney general within 14 business days of discovering the breach and include the dates and discovery of the breach and a description of what happened. Prior to a breach occurring, an organization may send the attorney general's office a statement that they are able to comply with the notification laws, making them exempt from the 14-day requirement and allowing them to notify the attorney general at the same time as the consumer notification.

Connecticut

Continuing the trend of notification, Connecticut added a new subsection to its breach notification statute. When organizations in the state are required to notify consumers of a data breach, they must also notify the state attorney general. Notification may only be delayed as a result of law enforcement investigations.

California

New laws took effect January 1, 2012 that require organizations to provide additional content in data breach notifications, including a general description of the incident, the type of information breached, the time of the breach and toll-free telephone numbers and addresses of the major credit reporting agencies in California. The notice must include the following information if such information is possible to determine before sending the notice:

- The date, estimated date or date range of the breach
- Whether notification was delayed as a result of a law enforcement investigation
- A general description of the breach incident

Further, the law requires data holders to send an electronic copy of the notification to the California attorney general if a single breach affects more than 500 Californians.

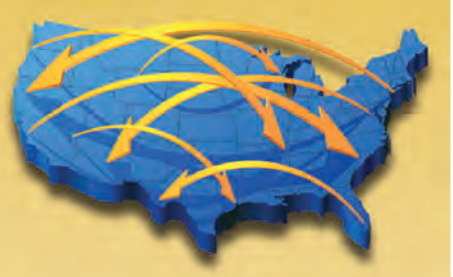
Illinois

In 2011, Illinois joined a growing number of states that dictate what content, at a minimum, must be included in notices to individuals regarding a compromise of their personal information. As of January 1, 2012, security breach notices to Illinois residents must include contact information for credit reporting agencies and the Federal Trade Commission, along with a "statement that the individual can obtain information from these sources about fraud alerts and security freezes." The law also expands the reach of the state's breach notice requirements to include service providers who maintain or store but don't own or license personal information.

Texas

Recently passed legislation focusing mostly on healthcare providers would require additional breach notification to residents outside of the state. Texas amended its breach notification law so that its consumer notification obligations apply not only to residents of Texas, but to any resident of a state that has not enacted their own notification law. Alabama, Kentucky, New Mexico and South Dakota are the only states that do not have breach notification laws.

Consensus has not yet fully emerged about the future of a comprehensive, national data protection framework. Policymakers still need to fully consider each approach and whether it fits into a national framework that protects consumers while facilitating innovation and competition. Meanwhile, commercial entities that are not already regulated should be prepared to engage in industry best practices and effective self-regulatory regimes in order to protect themselves from increased regulatory oversight and liability.



Legal Notice: Always check with your legal counsel in order to identify the notification requirements for your specific incident.

Preparedness Plan Audit

Preparedness Plan Audit

Once you've created your preparedness plan, you've cleared one of the major hurdles in setting up your organization for success if a data breach occurs. But your preparedness plan can only help you succeed if it's comprehensive and current. Each quarter, make it a priority to update, audit and test your plan. Consider the different scenarios that could occur and whether your plan would help address each one, including an internal breach, external attack, accidental data sharing and loss or theft of a physical device.

Most Overlooked Details

Here's a glimpse of a few commonly overlooked details that should be on your radar during a preparedness plan audit.

Call center

Getting your call center up to speed on a data loss incident or bringing external resources on board to help handle the high volume of calls is an important part of data breach preparedness. In the time following a data breach is not when you want to hide from or alienate your consumers. Instead, be readily available to answer their questions in order to reinforce the value of your brand and your commitment to their security.

Whether you plan to use internal or external resources, be sure you:

- Are prepared to swiftly pull together training materials, such as incident FAQs. Highly knowledgeable and emphatic call center representatives can make a positive impact on your brand during a crisis.
- Are able to scale the call center portion of your preparedness plan to fit any incident. In addition to identifying needed call center resources in advance of a breach, also create a call center script template specifically geared toward crisis management.
- Conduct ongoing crisis training for your regular call center, whether it's internal or external, so representatives are trained in handling sensitive information as well as emotional callers.
- Oversee several test calls to confirm the call center is ready to handle incident-related calls.

Vendor negotiations

With companies being plagued by data security breaches at the hands of their vendors, take steps to ensure your company isn't headed down the same road. Select vendors that have appropriate security measures in place for the data they will process. Then take it a step further by contractually obligating your vendors to maintain sufficient data safeguards. Assess whether they are meeting the contract requirements on a regular basis.

In general, it makes sense for companies to require that vendors:

- Maintain a written security program that covers the company's data.
- Only use the company's data for the sole purpose of providing the contracted services.
- Promptly notify the company of any potential security incidents involving company data and cooperate with the company in addressing the incident.
- Comply with applicable data security laws.
- Return or appropriately destroy company data at the end of the contract.

Always seek advice from legal and compliance when drawing up vendor contracts, especially ones involving data management or transfer.

Audit your preparedness plan immediately after a data breach so you can clearly remember what went wrong and what went right.

Operational challenges

So you've determined all of the steps and precautions you'll need to take if a data breach occurs. But, responding to one can take significant company resources. Does your preparedness plan address the operational challenges of managing a breach in conjunction with managing day-to-day business?

For example, if your head of security and/or IT is tied up with breach response, who oversees the department in the meantime? Answering questions like these truly helps to illustrate that data security, data breach preparedness and data breach response requires company-wide awareness and involvement.

As part of your preparedness plan, have every member of the response team prep their departments on what to expect and how to operate during data breach response. Everyone on staff should understand how their roles might change during a breach in order to maintain operations.

Preparedness Plan Audit Continued

Preparedness Audit Checklist

Auditing your preparedness plan helps ensure it stays current and useful. Here are several recommended steps you may want to take, but be sure to tailor your audit to fit the full scope of your company's individual response plan.

☐ **Update data breach response team contact list** • Check that contact information for internal and external members of your breach response team is current. • Remove anyone who is no longer with your company or with an external partner and add new department heads. • Re-distribute the updated list to the appropriate parties.	**Quarterly**
☐ **Verify your data breach response plan is comprehensive** • Update your plan, as needed, to take into account any major company changes, such as recently established lines of business, departments or data management policies. • Verify each response team member and department understands its role during a data breach. Create example scenarios for your response team and departments to address.	**Quarterly**
☐ **Double check your vendor contracts** • Ensure you have valid contracts on file with your forensics firm, data breach resolution provider and other vendors. • Verify your vendors and contracts still match the scope of your business.	**Quarterly**
☐ **Review notification guidelines** • Ensure the notification portion of your response plan takes into account the latest state legislation. • Update your notification letter templates, as needed, to reflect any new laws. • Verify your contacts are up to date for attorneys, government agencies or media you'll need to notify following a breach. • Healthcare entities need to ensure they have the proper Department of Health & Human Services contacts and reporting process in place.	**Quarterly**
☐ **Check up on third parties that have access to your data** • Review how third parties are managing your data and if they are meeting your data protection standards. • Ensure they are up to date on any new legislation that may affect you during a data breach. • Verify they understand the importance of notifying you immediately of a breach and working with you to resolve it. • Healthcare entities should ensure business associate agreements (BAAs) are in place to meet HIPAA requirements.	**Quarterly**
☐ **Evaluate IT Security** • Ensure proper data access controls are in place. • Verify that company-wide automation of operating system and software updates are installing properly. • Ensure automated monitoring of and reporting on systems for security gaps is up to date. • Verify that backup tapes are stored securely.	**Quarterly**
☐ **Review staff security awareness** • Ensure everyone on staff is up to date on proper data protection procedures, including what data, documents and emails to keep and what to securely discard. • Review how to spot and report the signs of a data breach from within everyday working environments. • Verify employees are actively keeping mobile devices and laptops secure onsite and offsite and changing passwords every three months.	**Yearly**

Resources

Staying up to date on best practices and legislation related to data privacy and data breach resolution is vital for every company. Because no business is immune to a data breach.

Experian Links

Experian Data Breach Resolution
www.Experian.com/DataBreach

Online Resource Center
www.Experian.com/databreachresources

HIPAA Omnibus Final Rule Resource Page
www.Experian.com/HIPAA

Perspectives Newsletter
www.Experian.com/DataBreachNews

Blog
www.Experian.com/DBBlog

Twitter
www.Twitter.com/Experian_DBR

Helpful Links

National Conference of State Legislatures
www.ncsl.org

Identity Theft Resource Center
www.idtheftcenter.org

Federal Trade Commission
www.ftc.gov/idtheft

Department of Health and Human Services
www.hhs.gov

Experian's Robust Online Resource Center

Data breach laws and risks are constantly changing. So is our online Resource Center, where you'll find the latest webinars and whitepapers created in partnership with some of today's top experts in privacy, data breach legislation and other key areas. Here's a quick look at some of the free resources we offer online:

Studies

- **Is Your Company Ready For A Big Data Breach?**
  Ponemon Institute, LLC
  www.Experian.com/Readiness

- **Securing Outsourced Customer Data**
  Ponemon Institute, LLC
  www.Experian.com/ConsumerDataStudy

Whitepapers and eBooks

- **Cyber Insurance 3.0: Risks, Rewards and Future Outlook**
  EXCERPT "Cyber Insurance, the fastest-growing speciality line in the commercial market, is rapidly becoming vital to the financial health of organizations."
  www.Experian.com/CyberReport

- **Navigating A Healthcare Data Breach eBook**
  EXCERPT "Data security can either make or break an organization... given HIPAA's stricter new regulations... This eBook provides five takeaways from lessons learned from the field."
  www.Experian.com/healthcareebook

Podcasts and Webinars

- **Podcast: How Cyber Insurance Can Help Organizations in the Event of a Data Breach**
  LISTEN to "Answer Man" Ozzie Fonseca, Senior Director of Experian Data Breach Resolution, interview Katherine Keefe from Beazely Insurance on what insurers can do to help organizations in the midst of a breach.
  www.Experian.com/CyberInsurancePodcast

- **Podcast: How To Accelerate Your Breach Response**
  LISTEN to "Answer Man" Ozzie Fonseca interview Privacy Attorney Miriam Wugmeister from the law firm of Morrison Foerster on the best way to respond to a breach.
  www.Experian.com/AcceleratedresponsePodcast

- **Podcast: Implications of the HIPAA Omnibus Final Rule**
  LISTEN to "Answer Man" Bob Krenek, Senior Director of Experian Data Breach Resolution, interview healthcare attorney Paula Stannard on what the Final Rule means to organizations.
  www.Experian.com/hipaapodcast

- **Podcast: Data Breach Readiness and Economic Impact**
  LISTEN to Experian Data Breach Vice President Michael Bruemmer discuss breach readiness and cost effectiveness with Dr. Larry Ponemon, Chairman of The Ponemon Institute.
  www.Experian.com/readinesspodcast

- **Webinar: How to Audit Your Incident Response Plan**
  This webinar provides a checklist of items to review when auditing your response plan. It also reviews how often you should audit, test, and update your plan.
  www.Experian.com/responseplanaudit

FAQs

What is a data breach?

A data breach occurs when secure data is released to or accessed by unauthorized individuals. The lost data may be sensitive personal data the company has collected on employees or customers or proprietary and confidential data regarding business operations and trade secrets. Data breaches can involve the loss or theft of digital media or physical data and devices, such as computer tapes, hard drives, mobile devices and computers. The incidents pose serious risks for organizations as well as for the individuals whose data has been lost.

How do data breaches happen?

Data breaches occur due to: accidental mishaps, such as an employee losing a mobile device or sending out sensitive data in an unsecured email; purposeful and malicious criminal attacks by someone inside or outside your organization; or a system failure or glitch that compromises security and leads to data loss.

How could a data breach impact my business?

A data breach has both direct and indirect financial consequences. First a business must allocate the budget and resources to resolve a data breach and address the underlying problem that led to the breach. Then a business must deal with the financial repercussions related to negative press, loss of customer loyalty, diminished brand reputation and possibly even litigation. In fact, 75% of the respondents in a recent survey say they've had or expect to have a data breach that results in negative publicity.[1]

How do I protect brand equity after a data breach?

In the face of a data breach, organizations have the opportunity to quickly implement sound decisions that will ultimately result in preserving brand equity and customer relationships. One way to preserve brand equity is to provide complimentary identity protection and credit monitoring services. Research shows that individuals affected in a breach who receive free credit monitoring are six times less likely to file a lawsuit against the breached company.[2] Experian makes it easy by offering a variety of consumer protection and credit monitoring products, backed with superior fraud resolution, to provide to your customers or patients.

What are my legal requirements regarding a data breach?

Working with internal and/or external legal counsel can help you determine your obligations, which is something you should explore before a data breach ever occurs. Your legal counsel will help you navigate the different state laws and determine whether they apply based on where the affected individuals reside, not where your business is located. Some industries, such as healthcare, have special considerations for reporting a data breach and notifying affected individuals. Be sure you work with a data breach resolution provider that can help you take all of the vital steps your legal counsel recommends. Even if your counsel determines you are not obligated by law to notify affected individuals, doing so can help preserve and even strengthen your relationship with consumers.

Do all data breach resolution vendors offer the same services?

No. Among the different vendors, there are different levels of service and different solutions to consider. Plus, you need to think about the integrity and security standards of a vendor before aligning your brand with it. For example, Experian's 30 years of global leadership and experience reflect positively upon another brand, especially during a data breach. As the world's largest credit bureau, we offer superior business and consumer services that millions rely on. Our trusted identity protection products can help you meet the needs of affected individuals for credit monitoring and alerts of potential identity theft. We also back our products with proven fraud resolution services, offering consumers professional guidance in resolving identity theft. And, since we are the world's largest credit bureau, we can securely access your consumers' credit data (with their permission) and enact credit alerts to discourage new credit activity in their names. Your dedicated data breach resolution account manager can help explain the different options available to you. These options include: individual or family protection; 1-bureau or 3-bureau credit monitoring; length of membership in the protection product; advanced features, such as Lost Wallet to help consumers act quickly in the event of lost or stolen credit, debit and medical insurance cards and Internet Scan to monitor websites known for selling or trading compromised Social Security, debit and credit card numbers.

Credit monitoring can assist individuals in the early detection of instances of identity theft. Although it cannot guarantee that identity theft will not occur, it does allow individuals to take steps to minimize the harm.[3]

1 Is Your Company Ready for a Big Data Breach?, Ponemon Institute, March 2013
2 Empirical Analysis of Data Breach Litigation, Carnegie Mellon & Temple Universitites, 2012
3 Department of Homeland Security, Privacy Incident Handling Guidance, January 26, 2012

Data Breach Response Team Contact List

Incident Lead			
Incident Lead Primary ☐ Internal ☐ External		**Company:**	
Name:		**Title:**	
Work Mobile Phone:	**Mobile Phone:**	**Office Phone:**	**Email:**
Incident Lead Secondary ☐ Internal ☐ External		**Company:**	
Name:		**Title:**	
Work Mobile Phone:	**Mobile Phone:**	**Office Phone:**	**Email:**

"All victims share something in common: they never thought it would happen to them."

Christopher Pogue, Director of Digital Forensics & Incident Response, Trustwave's Spiderlabs

Data Breach Response Team Contact List Continued

C-Level Executives

Chief Executive Officer	☐ Internal ☐ External	Company:	
Name:		Title:	
Work Mobile Phone:	Mobile Phone:	Office Phone:	Email:

Chief Financial Officer	☐ Internal ☐ External	Company:	
Name:		Title:	
Work Mobile Phone:	Mobile Phone:	Office Phone:	Email:

Chief Information Security Officer	☐ Internal ☐ External	Company:	
Name:		Title:	
Work Mobile Phone:	Mobile Phone:	Office Phone:	Email:

Chief Privacy Officer	☐ Internal ☐ External	Company:	
Name:		Title:	
Work Mobile Phone:	Mobile Phone:	Office Phone:	Email:

Chief Compliance Officer	☐ Internal ☐ External	Company:	
Name:		Title:	
Work Mobile Phone:	Mobile Phone:	Office Phone:	Email:

Data Breach Response Team Contact List Continued

Response Team Members

IT Primary ☐ Internal ☐ External		Company:	
Name:		Title:	
Work Mobile Phone:	Mobile Phone:	Office Phone:	Email:
IT Secondary ☐ Internal ☐ External		Company:	
Name:		Title:	
Work Mobile Phone:	Mobile Phone:	Office Phone:	Email:
Security Primary ☐ Internal ☐ External		Company:	
Name:		Title:	
Work Mobile Phone:	Mobile Phone:	Office Phone:	Email:
Security Secondary ☐ Internal ☐ External		Company:	
Name:		Title:	
Work Mobile Phone:	Mobile Phone:	Office Phone:	Email:
Privacy Primary ☐ Internal ☐ External		Company:	
Name:		Title:	
Work Mobile Phone:	Mobile Phone:	Office Phone:	Email:

Data Breach Response Team Contact List Continued

Response Team Members

Privacy Secondary ☐ Internal ☐ External		**Company:**	
Name:		**Title:**	
Work Mobile Phone:	**Mobile Phone:**	**Office Phone:**	**Email:**
Legal Primary ☐ Internal ☐ External		**Company:**	
Name:		**Title:**	
Work Mobile Phone:	**Mobile Phone:**	**Office Phone:**	**Email:**
Legal Secondary ☐ Internal ☐ External		**Company:**	
Name:		**Title:**	
Work Mobile Phone:	**Mobile Phone:**	**Office Phone:**	**Email:**
PR Primary ☐ Internal ☐ External		**Company:**	
Name:		**Title:**	
Work Mobile Phone:	**Mobile Phone:**	**Office Phone:**	**Email:**
PR Secondary ☐ Internal ☐ External		**Company:**	
Name:		**Title:**	
Work Mobile Phone:	**Mobile Phone:**	**Office Phone:**	**Email:**

Data Breach Response Team Contact List Continued

Response Team Members			
Customer Care Primary ☐ Internal ☐ External		Company:	
Name:		Title:	
Work Mobile Phone:	Mobile Phone:	Office Phone:	Email:
Customer Care Secondary ☐ Internal ☐ External		Company:	
Name:		Title:	
Work Mobile Phone:	Mobile Phone:	Office Phone:	Email:
HR Primary ☐ Internal ☐ External		Company:	
Name:		Title:	
Work Mobile Phone:	Mobile Phone:	Office Phone:	Email:
HR Secondary ☐ Internal ☐ External		Company:	
Name:		Title:	
Work Mobile Phone:	Mobile Phone:	Office Phone:	Email:

Data Breach Response Team Contact List Continued

External Data Breach Resources Contact List

Resolution Partners			
External Legal Counsel		**Company:**	
Contact	**Mobile Phone**	**Office Phone**	**Email**
Public Relations/Crisis Management Firm		**Company:**	
Contact	**Mobile Phone**	**Office Phone**	**Email**
Forensics Firm		**Company:**	
Contact	**Mobile Phone**	**Office Phone**	**Email**
Notification Vendor		**Company:**	
Contact	**Mobile Phone**	**Office Phone**	**Email**
Customer Service Vendor		**Company:**	
Contact	**Mobile Phone**	**Office Phone**	**Email**

Data Breach Response Team Contact List Continued

Law Enforcement and Government Agencies

Police Department

Contact	Mobile Phone	Office Phone	Email

Secret Service

Contact	Mobile Phone	Office Phone	Email

FBI

Contact	Mobile Phone	Office Phone	Email

FTC

Contact	Mobile Phone	Office Phone	Email

State Attorney General

Contact	Mobile Phone	Office Phone	Email

Data Breach Response Team Contact List Continued

Third Parties

Business Partners

Company	Contact	Mobile Phone	Office Phone	Email

Vendors

Company	Contact	Mobile Phone	Office Phone	Email

Data Breach Response Team Contact List Continued

Third Parties

Regulators

Company	Contact	Mobile Phone	Office Phone	Email

Card Processors

Company	Contact	Mobile Phone	Office Phone	Email

Media

Company	Contact	Mobile Phone	Office Phone	Email

Experian® Data Breach Resolution
(1) 866-751-1323
www.Experian.com/DataBreach
databreachinfo@experian.com

About Experian Data Breach Resolution
Drawing on the global power of Experian®, the largest credit bureau in the world, Experian Data Breach Resolution helps business of all sizes navigate the stormy waters of a data breach. We have handled thousands of high-profile data breaches in nearly every industry, from medical to government. Our industry-leading service and consumer protection products help companies manage the stress of a data breach while mitigating damage to their reputations and customer loyalty. For questions or to provide feedback about this guide, please contact us at databreachinfo@experian.com.