DEBIX
The Identity Protection Network

Data Breach Notification and Responsibilities

Agency responses and credit monitoring options.

127,000,000

In 2007, personally identifiable information of over 127 million individuals in the U.S. was lost, stolen or compromised.

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. As public awareness and concern over the problem of data breaches grow, so do the questions for government agencies regarding the appropriate response.

How do we determine if affected individuals should be notified?

What should be included in a data breach notification?

Should credit monitoring be provided and if so, what type?

Elevated Risks and Reactions

While it was virtually unheard of just a few years ago, companies today routinely perform in-depth analysis to determine what valuable, private information was on a stolen laptop. In the private sector, it is common for businesses to establish an emergency hotline to allow employees to report all possible data breach incidences. Every effort is made to encourage reporting of these events and all information is taken seriously. And while more than thirty-eight states have enacted a variety of laws requiring businesses to notify consumers when their personal information has been exposed, many of these statutes are complicated and confusing.

Navigating a Jagged Landscape of Public Good

In this environment, Government agencies of all sizes and directives are facing enormous challenges regarding breach notification and responses.

How do we translate and apply notification laws?

How do we accurately weigh the potential risks of not notifying given the trend in litigation?

If we decide to notify, is it prudent to include a consumer protection option immediately?

A Presentation of Outstanding Issues, Not Legal Advice

This paper is not intended as legal advice and you are encouraged to seek legal advice regarding issues discussed here.

The purpose here is to identify relevant issues faced by government agencies charged with providing solutions to the problems of data breaches affecting their citizens. The goal is to present and explain processes and provide guidelines for developing appropriate resolutions.

Helpful Resources:

Answers to many questions on legal obligations regarding notifications are available from CSO Magazine.
http://www.csoonline.com/read/020108/ammap/ammap.html

For a summary of laws for specific states refer to the Consumers Union Website:
http://consumersunion.org/campaign/Breach_Laws_May05.pdf

Important Notification Decision Considerations

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.

Is your agency 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?

Always consider the attitude and possible response of constituents whose information has been breached. Fines, penalties and potential legal response by some constituents are a possibility.

Use this abbreviated list to measure notification risk value.

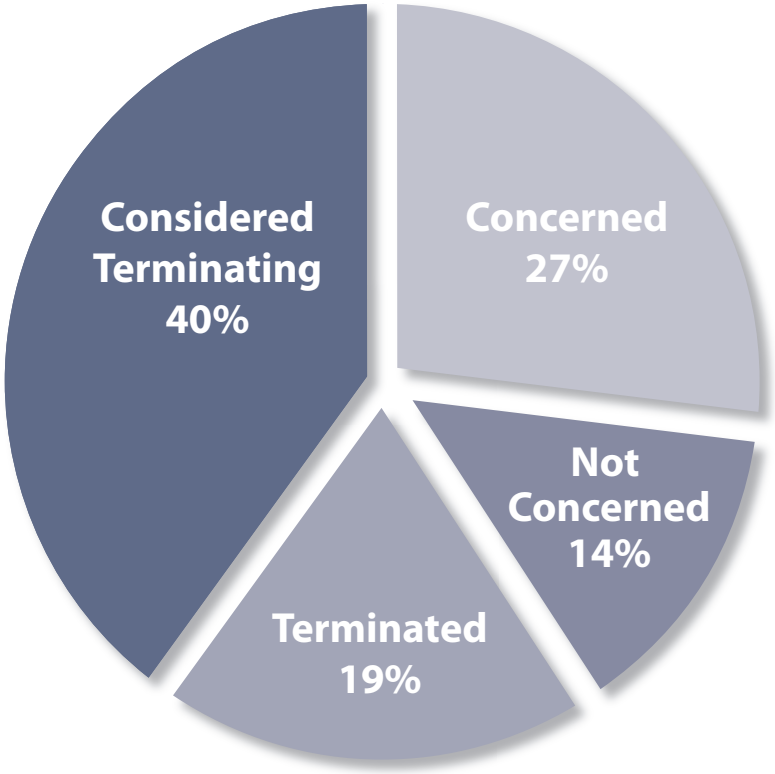
Is Your Agency Required to Notify?

Possible Exemptions to notifying:

- **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.**

NOT LEGAL ADVICE, seek legal counsel

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.



Notifying Affected Citizens

It is important to note that many state laws have established strict timelines for notifying consumers which include severe penalties for non-compliance.

In many cases, the faster the notification occurs, the faster press coverage declines and negative "buzz" dissipates.

Creating the 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 citizens 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.

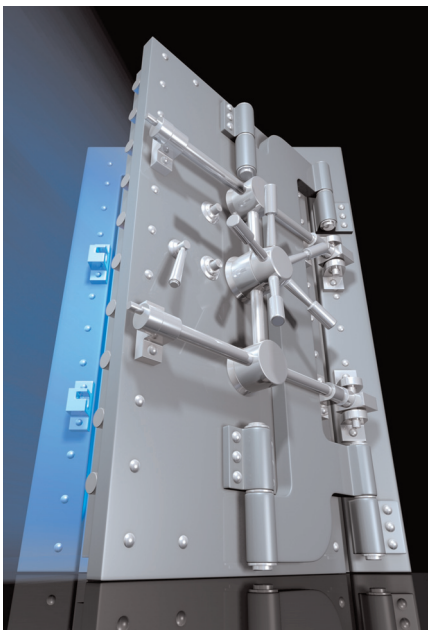
Helpful Resources:

Notification checklists and sample letters (also known as "disclosure letters") are available on many sites on the Internet.

For a free Notification Kit, including sample notification letters, please contact a Debix representative at 800-965-7564.

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 as many recipients are suspicious of notification letter authenticity.
- According to a Ponemon Institutes Study in 2007, the average per record cost of a data breach to businesses was $197.
- Expect twenty 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 agency provide credit monitoring or other ongoing credit protection service for citizens whose compromised information might be used to commit credit fraud?

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.

Consumer Protection Considerations

Weighing the answers to these questions is critical to making the right decision regarding consumer protection options.

1. What is the expected impact on your organization?
2. Will those affected change or cancel relationships with the organization?
3. What kind of public pressure will be placed on your agency from those whose information was compromised?
4. How will press coverage in this incident impact your organization?
5. Is your organization at risk for legal action?

Assessing the Risk of Credit Fraud

While it is virtually impossible to predict if and when stolen information will be used to commit fraud, determining the *level of risk* is essential. Criteria for doing so should include more than simply the nature of the information compromised. The circumstances surrounding the loss also play a vital role.

The Office of Management and Budget (OMB) has created a list to help determine the level of risk of identity theft to an individual.

1. How easy or difficult would it be for an unauthorized person to access the covered information in light of the manner in which the information originally was protected?
2. What was the means by which the loss occurred? Was it the result of a criminal act? Is it likely to result in criminal activity?
3. What is the ability of the agency to mitigate the identity theft; is there evidence that the compromised information is actually being used to commit identity theft?

Credit Monitoring and Credit Protection Guidelines

The OMB has also created guidelines to help you evaluate the need for credit monitoring or other consumer credit protection options.

> *In deciding whether to offer credit monitoring services and if so what type and for how long, agencies should consider the risk of identity theft arising from the data breach. Particularly important are whether incidents have already been detected and the cost of providing the service. Costs can be substantial, although rates are often subject to negotiation; bulk purchase discounts have been offered in many cases of large data breaches.*
>
> *The length of time for which the service is provided may have an impact on cost as well. In addition, the agency should consider the characteristics of the affected individuals. Some affected populations may have more difficulty in taking the self-protective steps described earlier. For example, there may be groups who, because of their location, may warrant special protection from the distraction of effort of self-monitoring for identity theft.*

Credit Monitoring Check List

Do I need to purchase credit monitoring?

1 check = Organization should consider purchasing credit monitoring.
2 to 5 checks = Organization should purchase credit monitoring.

- ☐ Data lost included SSN and DOB (Makes it easy for thieves to commit identity theft)
- ☐ If a thief has possession of/access to the data, could a reasonably savvy computer person view the data?
- ☐ The thief stole this data with the intent to use individual's information?
- ☐ There is already known fraud associated with the loss of this data
- ☐ The affected group will have difficulty taking measures on their own to prevent identity theft (military personnel stationed overseas; elderly population; those in long-term care; etc.)

Proactive vs. Reactive Credit Monitoring

There are many companies offering products that allow consumers to track activity in their credit files. With the explosion in identity theft crimes and a desire to fight identity theft, credit monitoring services have become extremely popular.

The primary limitation of many forms of credit monitoring is that the protection provided is **reactive** - allowing consumers to discover fraudulent activity *after it has happened.* Unfortunately, there is no preventative feature offered by these types of services.

A Comparison of Consumer Benefits

	Debix Proactive Credit Protection	Traditional Reactive Credit Monitoring
Prevents identity theft before it happens	✓	
Patent-pending technology lets you tell impacted citizens that their information is not being used by thieves	✓	
Identity theft attempts are identified as they are happening and can be reported to law enforcement	✓	
Consumer enrollment is simple, requiring no understanding of credit reports	✓	
Protection empowers customers delivering a high level of satisfaction	✓	

Emerging technologies have created an entirely new type of protection that is truly **proactive** - allowing consumers to know the *exact moment* a thief attempts to use their stolen information to commit fraud and to report the crime to law enforcement.

Debix has created the only proactive data breach solution on the market and has partnered with an extensive list of government and major, private-sector clients to protect consumers.

As the first company with an identity protection network, only Debix has the technology to link consumers, financial institutions and law enforcement to prevent and prosecute identity theft.

Debix Benefits to Agencies

- Dedicated data breach specialists to assist clients through the response process.
- Strongest available protection for consumers - prevents identity theft before it happens.
- Patent-pending technology allows clients to assure those impacted by the breach that compromised personal information is not being used by thieves to open new credit accounts.
- Fast turn-around time on setup.
- Daily or weekly reporting of fraudulent activity attempts.

Debix Benefits to Constituents

- Banks and creditors must request an Instant Authorization™ from the consumer before opening a line of credit
- Consumer can be contacted at up to three different phone numbers to authorize transaction.
- Consumer creates a unique Debix Voice Key to protect against phone scams.
- Non-stop protection is with a consumer during an attack, and continues following an incident
- When consumer reports fraud, they can be connected immediately to a Debix Fraud Specialist for help.
- Law enforcement organizations are engaged as appropriate.
- An Audit Trail is created to protect consumers' rights and aid prosecution

$3,500,000

Debix has already become the protection provider of choice for over thirty state and local agencies. And in just the last six months, Debix protection has saved customers and financial institutions over $3.5 million in identity theft losses.

A Final Word

For the foreseeable future, the problem of identity theft will continue to be a major threat and concern for consumers. Evaluating the problem from a government agency perspective requires an understanding of laws, responsibilities and public attitudes. Providing solutions in the public interest can best be achieved through awareness of all available resources and options.