BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Since 2005, there have been reports of over 500 U.S. security breaches. Proactive incident response planning can help minimize the impact when and if a breach occurs. The authors provide advice on responding to and managing a data breach, including information on state law variations, relevant stakeholders, and tips on actual notification.

A How-To Guide to Information Security Breaches

BY LISA J. SOTTO AND AARON P. SIMPSON

Contrary to what the headlines suggest, information security breaches are not a new phenomena. What is new is that we are hearing about them in record numbers. While consumers are newly focused on information security due to the emergence of e-commerce, the reason security breaches now seem ubiquitous is a result of the development of a body of state laws requiring companies to notify affected individuals in the event of a breach. The differing requirements of over 35 state security breach notification laws make legal compliance a challenge for organizations operating on a national level.

Lisa Sotto heads the Privacy and Information Management Practice at Hunton & Williams LLP and is a partner in the New York office. She is also vice chairperson of the DHS Data Privacy and Integrity Advisory Committee. Sotto may be contacted at lsotto@hunton.com. Aaron P. Simpson is an associate in the Privacy and Information Management Practice at Hunton & Williams, New York. He may be contacted at asimpson@hunton.com.

Background

Since 2005, there have been reports of over 500 security breaches, many of which have involved the most respected organizations in the United States.[1] In fact, the number of reported incidents does not begin to define the actual number of breaches that have occurred in the United States during the past two years. From universities to government agencies to Fortune 500 companies, no industry sector has been spared. These breaches have run the gamut from lost backup tapes and laptops, to hacking incidents, to organized crime. The reported breaches are estimated to have exposed personal information contained in over 100 million records. Consequently, a significant percentage of the American public has received notification that the security of their personal information has been breached. Indeed, it seems that hardly a day goes by without a new press report of a significant security breach.

[1] *See* Privacy Rights Clearinghouse, "A Chronology of Data Breaches," available at http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited March 27, 2007).

State Security Breach Notification Laws

Public awareness was not focused in earnest on security breaches until 2005, fully two years after California enacted a law requiring organizations to notify affected Californians of a security breach.[2] At the time of enactment, few understood the enormous implications of that law. Since 2005, 35 other states, as well as New York City, Washington, D.C. and Puerto Rico, have jumped on the bandwagon and enacted breach notification laws of their own. In addition, numerous federal security breach bills have been proposed. With no clear frontrunner, it is hard to predict when a federal law might be passed, thought a federal preemptive law appears likely.

At the state level, the duty to notify individuals affected by a breach generally arises when there is a reasonable belief that unencrypted, computerized sensitive personal information has been acquired or accessed by an unauthorized person. Typically, the state laws define ''personal information'' to include an individual's first name or first initial and last name, combined with one of the three following data elements:

- Social Security number;
- driver's license or state identification card number, or
- financial account, credit or debit card number, along with a required password or access code.

Unfortunately, entities struggling with a potential breach must look beyond the language of the ''typical'' state law in the event of a national, or even multi-state, incident. The variations among state breach notification laws greatly complicates the legal analysis as to whether the breach laws are triggered with respect to a particular event. Because most breaches impact individuals in multiple jurisdictions, companies often must take a ''highest common denominator'' approach to achieve legal compliance.

Key areas of variation among state breach notification laws include:

- *Affected Media*: Under most state breach laws, notification is required only if ''computerized'' data has been accessed or acquired by an unauthorized individual. In some states, however, including North Carolina, Hawaii, Indiana and Wisconsin, organizations that suffer breaches involving paper records are required to notify affected individuals.
- *Definition of ''Personal Information''*: Breach notification laws in some states expand the definition of personal information to include data elements such as medical information (Arkansas, Puerto Rico), biometric data (Nebraska, North Carolina, Wisconsin), digital signatures (North Carolina, North Dakota), date of birth (North Dakota), employee identification number (North Dakota), mother's maiden name (North Dakota), and tribal identification card numbers (Wyoming).
- *Notification to State Agencies*: Many states require entities that have suffered a breach to notify state agencies. Currently, the states that require such notification include Hawaii, Maine, New Hampshire, New Jersey, New York, North Carolina and Puerto Rico. In Puerto Rico, organizations must notify the state government within ten days of detecting a breach. In New Jersey, the breach notification law requires entities to notify the state police prior to notifying affected individuals.
- *Notification to Credit Reporting Agencies*: While the threshold for notification differs among the state laws, many states require organizations that suffer a breach to notify the three national consumer reporting agencies (Equifax, Experian and Transunion). Among the states with this requirement, the state with the lowest threshold requires notification to the credit reporting agencies in the event 500 state residents must be notified in accordance with the notification requirement.
- *Timing of Notification to Affected Individuals*: Most state notification laws require notification to affected individuals within ''the most expedient time possible and without unreasonable delay.'' Some states, such as Ohio, Florida and Wisconsin, require notification within 45 days of discovering the breach.
- *Harm Threshold*: Some states (*e.g.*, Indiana, Michigan, Ohio, Rhode Island, Utah and Wisconsin) require notification of affected individuals only if there is a reasonable possibility of identity theft. Other states (*e.g.*, Colorado, Idaho, Kansas, Maine, New Hampshire, New Jersey and Vermont) do not require notification unless it has been determined that misuse of the information has occurred or is reasonably likely to occur. And in other states (*e.g.*, Arkansas, Florida, Hawaii and Louisiana) notification is not required unless there is a reasonable likelihood of harm to customers. For organizations that suffer multi-state security breaches, any harm threshold is irrelevant as a practical matter because many state breach notification laws do not contain such a threshold.

Federal Enforcement

In addition to the compliance maze at the state level, the Federal Trade Commission (FTC) has enforcement authority in the privacy arena pursuant to Section 5 of the FTC Act.[3] Section 5 of the FTC Act prohibits unfair or deceptive trade practices. The FTC recently has brought a number of enforcement actions pursuant to Section 5 stemming from security breaches. In fact, most of the enforcement actions brought by the FTC in the privacy arena have resulted from security issues. Some of the more noteworthy FTC enforcement actions stemming from security breaches have included those against BJ's Wholesale Club, CardSystems, ChoicePoint and DSW.

The CardSystems case highlights the significant reputational risk associated with privacy events generally, and security breaches in particular. In this case, over 40 million credit and debit card holders' information was accessed by hackers leading to millions of dollars in fraudulent purchases. In its enforcement action, the FTC alleged that the company's failure to take appropriate action to protect personal information about millions of consumers was tantamount to an unfair trade practice. As part of its settlement with the FTC, CardSystems agreed to implement a comprehensive information security program and conduct audits of the program biennially for 20 years. The real punishment, however, was the reputational damage the company suffered in the wake of the breach. Both Visa and Discover severed their relationship with CardSystems and

[2] Cal. Civ. Code § 1798.82 (2006).

[3] 15 U.S.C. § 45 (2005).

  PVLR ISSN 1538-3423

the company ultimately was sold to an electronic payment company in Silicon Valley.

As our society becomes increasingly information-dependent, it is likely that there will be an increase in FTC enforcement associated with security breaches. In fact, in response to heightened consumer concern and an increased need for regulatory oversight in this arena, the FTC recently established a new division of Privacy and Identity Protection. This signals a new FTC focus on data privacy and security, along with what will likely be a concomitant increase in enforcement.

Managing a Data Breach

If a possible breach occurs, it is critical to determine as quickly as possible whether the event triggers a requirement to notify affected individuals. To make this determination, organizations must be able to answer the following questions:

1. *What information was involved?* Does the compromised information meet the definition of ''personal information'' under any of the state breach notification laws? As discussed above, certain states have adopted expansive definitions of ''personal information'' for purposes of their breach notification laws. These broader definitions must be considered in analyzing the information involved in the event.
2. *Was the information computerized?* In most states, only incidents involving computerized information require individual notification. But special attention should be paid to the laws in those states in which notification is required for incidents involving personal information in any form, including paper.
3. *Was the information encrypted?* Encryption is available as a safe harbor under every extant state security breach notification law. Importantly, all of the relevant laws are technology-neutral, meaning they do not prescribe specific encryption technology. If the information is maintained in an unreadable format, then it may be considered encrypted for purposes of the state breach laws. Encryption does not, however, include password-protection on equipment such as desktop computers, laptop computers and portable storage devices. As a result, many organizations have been required to notify affected individuals when laptop computers subject to password-protection have been lost or stolen.
4. *Is there a reasonable belief that personal information was accessed or acquired by an unauthorized person?* If an entity has a reasonable belief that the information was compromised by an unauthorized person, notification is required. Note that a number of state breach notification laws contain a harm threshold whereby notification is not required unless there is reasonable possibility of harm, misuse or identity theft (*see above*). Organizations should be wary of relying on harm thresholds, however, because they are not included in many state breach laws and thus may not be available in the event of a multi-state breach.

Because breaches come in all shapes and sizes, many of them require significant technical analysis to answer these questions. Organizations often must enlist the assistance of highly skilled forensic investigators to assist with the evaluation of their systems.

Recognize the Stakeholders

Once an organization has determined that the breach notification laws have been triggered, it is important to understand the panoply of stakeholders throughout the breach process. Depending on the type of organization involved, the potential universe of stakeholders is extensive and may include:

- *Affected individuals*: Individuals affected by a security breach are the primary focus for every organization during the notification process. Although the breach may not have occurred as a result of any misdeeds by the organization suffering the breach, in the eyes of consumers, employees and other affected individuals, the organization is responsible for the data it collects and maintains. As a result, regardless of the circumstances, an organization suffering a security breach should be appropriately helpful and respectful to individuals whose data may have been compromised.
- *Board of Directors/Senior Management*: Information security is no longer an area of a company that is relegated to the dusty basement. Front-page headlines and stock drops stemming from early security breaches made sure of that. It is often advisable to involve the Board of Directors (or its equivalent) and senior management soon after learning of a security breach affecting the organization.
- *Law Enforcement*: Depending on the nature of the event, it may be important to report the security breach to law enforcement authorities for purposes of conducting an investigation. The state security breach laws allow organizations to delay notifying affected individuals pending a law enforcement investigation. New Jersey's breach notification law makes it a legal requirement to notify law enforcement prior to notifying affected individuals.
- *State and Federal Regulators*: In addition to the laws' requirements to notify state regulators, organizations should give serious consideration to notifying the FTC in the event of a significant security breach. Proactively notifying the FTC, while not a legal requirement, provides an organization with the opportunity to frame the circumstances of the breach and provide appropriate context. Because the FTC will undoubtedly learn about every significant security breach, organizations are well-advised to tell the story themselves rather than have the FTC learn about the breach from unfavorable media reports.
- *Financial Markets*: For publicly-traded companies, some security breaches rise to the level of reportable events. In these cases, it may be necessary to notify the Securities and Exchange Commission and the relevant exchange of the breach.
- *Payment Card Issuers*: To the extent payment cards are involved, it is often essential to consult the card issuers as early as possible in the process. Organizations should review their contractual obligations with the card issuers because there are likely to be provisions relevant to a security breach. In addition, the card issuers may require organizations suffering breaches to file formal incident reports. Depending on the scope of the breach, the card issuers also may require that an

independent audit be conducted by their own auditors.

- *Employees*: In some cases, employees of the organization should be notified of an incident affecting customers. Many employees care deeply about the entity for which they work. To the extent the organization's reputation may be tarnished by the event, employees will not want to be left in the dark about the incident.

- *Shareholders*: Public companies that suffer breaches must consider their shareholders in the aftermath of a breach. The investor relations department should be mobilized in the event of a significant breach to respond to investors' concerns.

- *Auditors*: In some cases, security breaches may need to be reported to a company's auditors.

- *Public*: Security breaches often ignite the passions of the public at-large. In managing the process of notification, organizations should give careful consideration to the anticipated public response to the incident. In many cases, it is helpful to work with experienced public relations consultants. The risk to an organization's reputation stemming from a security breach far exceeds the risk associated with legal compliance. Thus, it is imperative in responding to a security breach to consider measures that will mitigate the harm to an organization's reputation.

Timing of Notification

Once the extent and scope of the incident have been defined and it is determined that notification is required, the next step is to notify affected individuals. Most state security breach laws require organizations that suffer a breach to notify affected individuals ''in the most expedient time possible and without unreasonable delay.'' In several states, notification is required within 45 days of the date the incident was discovered. Under both timeframes, the date of actual notification may be delayed by the exceptions available in most states for law enforcement investigations and restoring system security.

Pursuant to the law enforcement exception, notification may be delayed if a law enforcement agency determines that notification would impede a criminal investigation. Thus, if law enforcement has requested such a delay, the clock does not start ticking on notification until after the agency determines that notification will not compromise the investigation.

As to the exception for restoring system security, notification to affected individuals may be delayed to provide the affected organization time to take any security measures that are necessary to determine the scope of the breach and to restore the ''reasonable integrity of the system.'' Organizations should not take this exception lightly—notification to consumers of a system vulnerability may tip off copycat fraudsters to a system weakness they can exploit. Thus, prior to notifying affected individuals, it is essential for organizations suffering security breaches to restore the integrity of their systems.

Entities that rely on either the law enforcement or system security exception should document such reliance. In Hawaii, such documentation is a legal requirement.

Notification to Individuals

Letters to individuals notifying them of a possible compromise of their personal information should be simple, free of jargon and written in plain English. Entities would be well-advised to avoid legalistic phrases and any attempt to pin blame elsewhere. Organizations that have been most favorably reviewed by individuals following a breach are those that have accepted responsibility and provided useful information to recipients. (A breach notification letter is not the place for marketing!)

Organizations should keep in mind that, in addition to impacted individuals, the notification letter will likely be scrutinized by numerous interested parties, including regulators, plaintiffs' lawyers and the media. As a result, it is essential to strike the appropriate tone while at the same time providing a meaningful amount of substance.

There is a growing de facto standard, depending on the information breached, for the types of ''offerings'' companies are making to affected individuals in their notice letters. These offerings typically include:

- *Credit Monitoring*: In the event a Social Security number or some other form of identification that may contain a Social Security number (such as a driver's license number or a military identification card number) has been compromised, it has become standard to offer affected individuals one year of credit monitoring services. Depending on the size of the breach, this can be a significant cost for companies.

- *Free Credit Report*: Separate and apart from credit monitoring, organizations should inform affected U.S. individuals that they are entitled to one free credit report annually from each of the three national credit reporting agencies.

- *Fraud Alert*: Organizations also may want to recommend that affected individuals place a fraud alert on their credit file for additional protection. There is no charge for this service. Because fraud alerts can have a significant impact on a consumer's day-to-day purchase habits, most organizations simply suggest to consumers that this is an option rather than insist they take such action.

In addition to the standard offerings, the letter should describe the details of the security breach. For obvious reasons, these details should never include the specific affected payment card or Social Security numbers impacted by the breach. Instead of providing this detail, it is most effective to explain what happened and what the organization is doing to help individuals affected by the breach. In many cases, this means providing the individual with information about credit monitoring and other information about how they may protect themselves. Also, it may be necessary to establish a call center (with trained agents) to handle consumer response to the incident.

As a general rule, if an organization is required to notify in a few jurisdictions, it is recommended that it notify in all jurisdictions (often this includes foreign countries). With few exceptions, this has become standard in the privacy realm. A few companies that suffered early security breaches after California passed its law were torched by the media and subjected to severe criticism by irate state attorneys general for notifying affected Californians but not affected residents of other states without breach notification laws. The collective experi-

  PVLR ISSN 1538-3423

ence of these companies highlights an important, but often misunderstood, concept: technical compliance with law is necessary but not sufficient in the privacy arena. Privacy events are hot button social issues that often transcend mere legal compliance. Indeed, the risk to an organization's reputation and revenues often far exceeds the risk associated with non-compliance with breach laws. As a result, organizations responding to a breach should focus on doing the right thing as opposed to doing only those things that are required by law.

Lessons Learned

Security breach notification laws have brought information security issues into the spotlight. While no information security is perfect, proactive incident response planning can help minimize the impact when and if a breach occurs. Such planning includes inventorying the entity's databases that contain sensitive personal information, understanding how sensitive personal information flows through the organization, conducting ongoing risk assessments for internal and external risk to the data and responding to reasonably foreseeable risks, maintaining a comprehensive written information security program, and developing a breach response procedure. Given that a recent survey of 31 breaches ranging in size from 2,500 records to 263,000 records conducted by the Ponemon Institute found that the average cost of responding to a security breach was $182 per lost customer record with an average total cost of $4.8 million, the stakes are higher than ever for companies to focus on their information security programs.[4] Most importantly, concern and respect for information security should be integrated into the organization's core values. A breach response plan alone, without demonstrable organizational concern for information security generally, exposes the organization to significant risk. With the stakes as high as they are, all organizations should be taking a closer look at their information security practices.

---

[4] *See* Ponemon Institute, ''2006 Annual Study: Cost of a Data Breach'' (October 2006).