MARCH 2006

SECURITY BREACH NOTIFICATION REQUIREMENTS: GUIDELINES AND SECURITIES LAW CONSIDERATIONS

THE RECENT WAVE OF SECURITY BREACHES

Hardly a week passes without a news story about the theft of personal data from a computer database of a major company or organization. In 2005 alone, the personal information of at least nine million people was compromised by database breaches at companies that keep such information.

Information security studies have indicated that the number of database breaches has increased recently, along with their frequency and severity, as well as the costs of responding. One recent survey found that nearly 80 to 90 percent of *Fortune* 500 companies and government agencies have experienced security breaches. In 2003, California, which leads the nation in privacy protection statutes, enacted a law to address this situation. The California Database Breach Notification Security Act gives individuals early warning when their personal information has fallen into the hands of an unauthorized person, so that they can take steps to protect themselves against identity theft or to mitigate the crime's impact. The first of its kind, the law has served as the catalyst for similar legislation enacted in 15 other states and for legislation proposals in the majority of other states and in Congress.

CALIFORNIA'S SECURITY BREACH STATUTE

Requirements. The California security breach statute requires public disclosure of computer security breaches in which unencrypted confidential information of any California resident may have been compromised. The law applies to any person or entity that does business in California, even if located out of state, and that owns or licenses computerized data that includes personal information.

Security Breach. A "breach of the security of the system" is defined by the statute as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business."

© 2006 Jones Day. All rights reserved. Printed in the USA.

Personal Information. The statute defines "personal information" as an individual's first name or initial and last name, in combination with either: the individual's Social Security number; driver's license or identification number; or account number, debit, or credit card number together with any required access code that would permit access to the individual's financial account.

Notification Obligations. A company that has been affected by a security breach must make the disclosure "in the most expedient time possible and without unreasonable delay." Notice may be delayed when a law enforcement agency determines that the notification will impede a criminal investigation.

Notification to affected consumers may be provided in writing or electronically if the electronic notice complies with the federal Electronic Signature Act. If a company can demonstrate that the cost of providing notice would exceed $250,000, that the affected class of subject persons to be notified exceeds 500,000, or that the company does not have sufficient contact information, then the company can rely on "substitute notice" to comply with its notification requirements. Substitute notice involves the following three actions: (1) e-mail notice when the company has e-mail addresses for the subject persons; (2) conspicuous posting of the notice on the company's web page, if it maintains one; and (3) notification in a major statewide medium.

STATE LEGISLATION OUTSIDE CALIFORNIA

At the time of enactment, California was the only state requiring disclosure of security breaches involving personal information.[1] Accordingly, companies that suffered database breaches notified affected individuals in other states voluntarily, amidst public pressure and threats from each state's attorney general. Since then, legislation has been proposed in almost every state and in Congress and enacted in 15 other states.[2] In some respects, the other states' legislation is very similar to the California version in that it: (1) covers electronic or computerized data only; (2) provides a safe harbor for encrypted data; (3) allows substitute notice in cases where the cost of direct notice would exceed $250,000 or where there are more than 500,000 affected individuals; and (4) provides a delay of notification if it would impede a law enforcement investigation. There are, however, several variations among each state's enacted legislation and additional provisions that are not part of the California bill.

Some of the states broadened the disclosure requirements to include not only persons or businesses that own or license computerized data, but also those that acquire, handle, collect, disseminate, or otherwise deal with nonpublic personal information. Several states, including Alabama, Connecticut, Delaware, and Florida, devised a risk-of-harm exemption, which releases a company from its disclosure obligations if, after an appropriate investigation and consultation with relevant federal, state, and local agencies responsible for law enforcement, the company reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired. Seven states included a requirement that companies notify all consumer reporting agencies in the event the breach affects a statutorily mandated number of people (ranging from 500 to 10,000). Connecticut also expanded the definition of a "security breach" to mean mere unauthorized *access to*, as opposed to *acquisition of*, computerized data. And Florida's version mandated a 45-day time period for a notification.

---

1. On February 22, 2005, California State Sen. Debra Bowen introduced S.B. 852 to amend certain provisions of the statute and strengthen the existing breach notification requirements. First, the bill would cover not only businesses that *own* or *license* computerized data that includes personal information, but also businesses that *collect* such data as well. Second, the provision would include personal information that was not in computerized form at the time of the unauthorized transaction. The purpose of this change, according to Sen. Bowen, is to "require companies and public agencies to notify people anytime their personal information is lost, stolen, or accessed by the wrong person, regardless of the format of the data . . . ." Third, in order to delay notification for criminal investigation purposes, a law enforcement agency must make a written or electronic request. Finally, the definition of "personal information" is amended to include only an individual's last name in combination with at least one other data element. The proposed bill does preserve the safe harbor for encrypted data provided for in the original act. The latest major action on S.B. 852 occurred on June 28, 2005, when it failed passage in the Assembly Committee on Business and Professions but was granted reconsideration.

2. As of June 30, 2005, those states are Arkansas, Connecticut, Florida, Georgia, Illinois, Indiana, Maine, Minnesota, Montana, Nevada, North Dakota, Tennessee, Texas, and Washington.

In addition to the legislation enacted, approximately 80 bills have been introduced in the legislatures of all but 15 states related to database breach notification.[3]

FEDERAL SECURITY BREACH NOTIFICATION LEGISLATION

There are currently six bills pending in Congress with provisions requiring notification in cases where personal information is put at risk by a security breach.[4] A national preemptive notification law would create uniform standards for notification replacing the mélange of state law requirements that currently exists.

Taken as a whole, the proposed federal legislation sets forth more stringent notification requirements, broadens the scope of the disclosures, seeks to eliminate the encryption safe harbor, creates additional agencies within the federal government to combat identity theft and oversee statutory compliance, and requires companies to provide additional notices to credit reporting agencies and certain designated federal agencies. For the most part, the bills put the burden on law enforcement agencies to request a delay in notification, and only one of the proposed federal bills offers a risk-of-harm exemption. At this point, it is not known which version of the proposed bills will be enacted into law and which notification provisions will be adopted.

---

3. The following states did not introduce database breach notification legislation in 2005: Alabama, Hawaii, Idaho, Iowa, Kansas, Kentucky, Mississippi, Nebraska, New Hampshire, New Mexico, Oklahoma, South Dakota, Utah, Vermont, and Wyoming.

4. The first, Senate Bill 115, introduced by Sen. Dianne Feinstein (CA) on January 24, 2005, and entitled "Notification of Risk to Personal Data Act," is almost identical to the California statute.

   House of Representatives' Bill H.R. 1069, introduced by Rep. Melissa Bean (IL) on March 3, 2005, is a second version of the "Notification of Risk to Personal Data Act." It is structured like the California statute but also requires that the company affected by a security breach of personal information notify each consumer reporting agency and an information clearinghouse within the Federal Trade Commission of the security breach. The latest major action on H.R. 1069 occurred on May 13, 2005, when the bill was referred to the Subcommittee on Financial Institutions and Consumer Credit. The bill has 18 cosponsors.

   Senate Bill 751, introduced by Sen. Feinstein on April 11, 2005, as the third version of the "Notification of Risk to Personal Data Act," makes substantial departures from the California law. The bill applies to data containing personal information, *whether or not held in electronic form*, and there is no requirement that the personal information be *unencrypted*. Also, the safe-harbor delay in notification is allowed only if notification would *seriously* impede a criminal investigation. The onus is on the law enforcement agency to request in writing that notification be delayed. Notification via e-mail is allowed only if the individual has consented to receiving such notices by e-mail. Also, substitute notice is allowed if, among other things, the cost of direct notification exceeds $500,000—double the requirement in the California statute. The latest major action occurred April 11, 2005, when the bill was referred to the Senate Committee on the Judiciary. The bill has two cosponsors.

   The fourth, Senate Bill 768, introduced by Sen. Charles E. Schumer (NY) on April 12, 2005, creates within the Federal Trade Commission an Office of Identity Theft that will have "civil jurisdiction over any commercial entity that collects, maintains, sells, or transfers sensitive personal information, or attempts to collect, maintain, sell, or transfer sensitive personal information." The act defines "personal information" as any single data element listed (*e.g.*, Social Security number, medical condition, credit card number, and any information determined by the Federal Trade Commission). While the bill still requires that personal information accessed be unencrypted, it doesn't require that the data be computerized. The bill also mandates that the company notify the Office of Identity Theft if more than 1,000 individuals are affected by the breach. The latest major action on this bill occurred on April 12, 2005, when the bill was referred to the Senate Committee on Commerce, Science and Transportation. The bill has five cosponsors.

   The fifth, Senate Bill 1332, introduced by Sen. Arlen Specter (PA) on June 29, 2005, also does away with the encryption safe harbor. It requires that consumer reporting agencies be notified in the event of a breach. It also requires that the company inform the United States Secret Service of the breach if: (1) more than 10,000 individuals nationwide are impacted; (2) the security breach impacts a database, networked or integrated databases, or other system associated with more than one million individuals nationwide; (3) databases owned or used by the federal government are affected; or (4) sensitive personally identifiable information of employees and contractors of the federal government is involved. Along with notification of the breach, the company must also offer to cover the cost of monthly access to a credit report and a credit-monitoring service for one year. The bill also provides for a risk-of-harm exemption. Currently, the bill has two cosponsors. The last major action for this bill occurred on July 1, 2005, when it was placed on the Senate Legislative Calendar under General Orders.

   Finally, House of Representatives Bill 3140, introduced by Rep. Bean on June 30, 2005, applies only to consumer reporting agencies and financial institutions. It proposes to amend the Fair Credit Reporting Act and Title V of the Gramm-Leach-Bliley Act by requiring that consumer reporting agencies and financial institutions notify consumers of data security breaches involving sensitive consumer information. The bill currently has 13 cosponsors, and the last major action occurred on June 30, 2005, when the bill was referred to the House Committee on Financial Services.

MOVING TOWARD STANDARDIZED GUIDELINES

Given the number of bills enacted by state legislatures and without uniform national legislation in place, companies must comply with a patchwork of database breach notification requirements derived from various state statutes. But there are certain themes that can be derived from the plethora of notification requirements as to the guidelines a company should follow to fulfill its notification obligations:

Who Must Comply? The legislative trend appears to extend the security breach notification obligations to any person or company that acquires, maintains, handles, collects, disseminates, owns, licenses, sells, or otherwise deals with nonpublic personal information.

What Is Personal Information? The definition of "personal information" tends to include an individual's name in combination with at least one other data element (*e.g.,* Social Security number, medical information, credit card number, password, etc.).

What Constitutes a Breach? Most statutes require that an unlawful and unauthorized acquisition of personal information must occur to constitute a breach. Only Connecticut has expanded the definition of "breach" to mean mere unauthorized *access to* computerized data.

What Data Is Covered? While earlier bills limited the application of the law to computerized or electronic data, the latest trend is to extend the notification obligation to non-electronic documents as well.

When Should Notice Be Made? Most of the legislation requires that notice be made to the affected individuals in the most expedient time possible and without unreasonable delay. So far only Florida has mandated that notification be made within a specific time period (*i.e.,* 45 days).

Is Encryption a Safe Harbor? Currently all enacted and proposed state laws require that the personal information accessed be unencrypted. Two of the proposed federal bills do away with the encryption safe harbor.

Is There a Law Enforcement Delay for Notification? All enacted and proposed legislation provides for a delay if the notification would impede a criminal investigation. The newer bills put the burden on the law enforcement agency to request that the company delay the notification.

When Is Substitute Notice Permitted? All enacted and proposed legislation permit the use of substitute notice. For the most part, substitute notice is permitted when the cost of providing notice exceeds $250,000 and the number of affected individuals is more than 500,000, but some legislation both raised and lowered the threshold amounts.

Is There a Risk-of-Harm Exemption? Some of the states and one of the proposed federal bills offer a risk-of-harm exemption, which exempts a company from its notification requirements if, after appropriate investigation, the company reasonably determines that the breach has not resulted, and is not likely to result, in harm to the individuals whose personal information has been acquired.

Who Else Should Be Notified? Some of the enacted and most of the proposed legislation requires a company to notify credit reporting agencies if the security breach affected a statutorily mandated number of people (ranging from 500 to 10,000). Certain proposed federal bills require that a company notify the specific federal agencies tasked with combating identity theft and overseeing statutory compliance (*e.g.*, the United States Secret Service, the Office of Identity Theft).

PRACTICAL SECURITY CONSIDERATIONS TO AVOID A SECURITY BREACH

While a company's information security system may be unique to its situation, there are recognized basic components of a comprehensive, multilayered program to protect personal information from unauthorized access. At the outset, companies should review their privacy and security policies and inventory records systems, critical computing systems, and storage media to identify those containing personal information. It is important to classify personal information in records

systems according to sensitivity. Based on those classifications, physical and technological security safeguards must be established to protect personal information, particularly higher-risk information such as Social Security numbers, driver's license numbers, financial account numbers, and any associated passwords and PIN numbers, as well as health information. This involves establishing policies that provide employees with access to only the specific categories of personal information their job responsibilities require, use technological means to restrict access to specific categories of personal information, monitor employee access to higher-risk personal information, and remove access privileges of former employees and contractors immediately.

Companies should promote awareness of security and privacy policies through ongoing employee training and communications. They should also require third-party service providers and business partners that handle personal information on behalf of the company to follow specified security procedures. This can be accomplished by making privacy and security obligations of third parties enforceable by contract. Internally, companies must employ the use of intrusion-detection technology to ensure rapid detection of unauthorized access to higher-risk personal information and, wherever feasible, must use data encryption, in combination with host protection and access control, to protect sensitive information. Data encryption should meet the National Institute of Standards and Technology's Advanced Encryption Standard. Companies should also dispose of records and equipment containing personal information in a secure manner, such as shredding paper records and using a program to "wipe" and overwrite the data on hard drives.

SECURITIES LAW CONSIDERATIONS

A company should take into account securities law considerations when dealing with a database breach.

Insider Trading. Knowledge of a database breach before notification may be material nonpublic information for purposes of Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5 promulgated by the Securities and Exchange Commission.[5] Rule 10b-5 prohibits the purchase or sale of a security of any issuer on the basis of material nonpublic information. A shorthand definition of materiality for insider-trading purposes, therefore, is any information the disclosure of which would be likely to result in a substantial change in the price of the security. A survey of stock prices following a string of losses of customer data by several *Fortune* 500 companies shows at least a moderate drop in a company's stock after such an incident. Thus, for insider-trading purposes, information related to a breach of database security is likely to constitute material information. It would seem, then, that a delay in notification of a breach in database security to affected individuals, or the general public for that matter, even at the request of investigating law enforcement agencies, does not provide reprieve from obligations against insider trading. The information is considered public only after the insider's informational advantage is neutralized vis-à-vis notification of the breach.

Public Company Reporting Obligations. There is also an issue of whether to disclose a database security breach in a company's SEC reports, or otherwise publicly comment on the breach, in light of a request to delay notification by a law enforcement agency. While a database security breach does not automatically trigger filing of a Form 8-K interim report, public disclosure of the breach may be required as a contingent liability in the company's financial statements, and as a "known trend, event or uncertainty" in the Management's Discussion and Analysis sections of the Form 10-K and Form 10-Q and in certain registration statements. Disclosure of a material database security breach may also be necessary to prevent other statements in these documents, or in other public statements such as earnings releases and quarterly investor conferences, from being found misleading by the omission of the potential impact of the breach. As a corollary, under Regulation FD, companies must avoid selective disclosure to investors about a material database security breach.

5. Breaches in database security might also bring into play similar state laws that prohibit insider trading. Insiders must be mindful of the various state provisions governing insider trading and the obligations that arise therefrom.

DEALING WITH A SECURITY BREACH

Companies have a legal responsibility to inform individuals about incidents that have caused their personal information to be acquired by unauthorized persons. To ensure giving timely and helpful notice to affected individuals, the following practices are recommended:

Acquisition. At first, determine whether confidential personal information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person. Indications that the information is in control of another person include evidence of a lost or stolen computer or device containing unencrypted personal information, information that has been downloaded or copied, and information that was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Internal Investigation. Take necessary steps to contain and control the systems affected by the breach and conduct a preliminary internal assessment of the scope of the breach. Outside forensic investigators should be retained to conduct an analysis of the company's systems and databases to determine the source of the breach.

Contacting Law Enforcement. Immediately contact appropriate law enforcement agencies and notify them of the security breach. These include the Federal Bureau of Investigation, the United States Secret Service, and the local police and sheriffs' departments. If the law enforcement official tells you that giving notice would impede the investigation, ask for a written request from the law enforcement agency that the notification be delayed.

Insider Trading. Insiders at public companies who have knowledge of the database breach should avoid selling any securities until a public notification is made.

Notification. After the discovery of an incident involving unauthorized access to personal information, the company must notify affected individuals in the most expedient time possible.

Compliance With State Law Requirements. Determine whether state laws require any further action (*e.g.*, notifying credit reporting agencies), taking into consideration any applicable statutory minimum requirements concerning the number of consumers affected.

Contents of Notice. Include the following information in the notice: (1) a general description of what occurred; (2) the nature of the individual's personal information that was involved; (3) what the company has done to protect the individual's personal information from further unauthorized acquisition; (4) what your company will do to assist individuals, including providing an internal contact number (preferably toll-free) for more information and assistance; and (5) what individuals can do to protect themselves from identity theft.

Form and Style of Notice. Make the notice clear, conspicuous, and helpful. Use simple language and avoid using a standardized format which could undercut the purpose of the notice. To avoid confusion, the notice should be a stand-alone document, not combined as part of another mailing.

Whom to Notify. Notify all affected individuals whose personal information was acquired by an unauthorized person. If you cannot identify the specific individuals whose personal information was acquired, notify all those in the groups likely to have been affected, such as those whose information is stored in the files involved.

Means of Notification. Send the notice to all affected individuals by first class mail. You can notify by e-mail only if you normally communicate with the affected individuals by e-mail and you have received their prior consent to that form of notification. If more than 500,000 individuals are affected (100,000 in Delaware) or if the cost of giving notice to affected individuals is greater than $250,000 ($75,000 in Delaware), you may use substitute notice procedures: (1) send the notice by e-mail to all affected parties whose e-mail address you have; ***and*** post the notice conspicuously on the company's web site; ***and*** (3) notify a major statewide medium (television, radio, print, etc.).

Reporting Obligations. A public company should report the database security breach in its 10-K and 10-Q reports.

LAWYER CONTACTS

Jones Day has successfully counseled a number of clients through very complex database security breaches. For further information, please contact your principal Firm representative or one of the lawyers listed below. General e-mail messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Jeffrey M. Rawitz
1.213.243.2537
jrawitz@jonesday.com

Alexander Frid
1.213.243.2754
afrid@jonesday.com

Jones Day Commentaries are a publication of Jones Day and should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information purposes only and may not be quoted or referred to in any other publication or proceeding without the prior written consent of the Firm, to be given or withheld at its discretion. The mailing of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship.