FOR METRO AREA IN-HOUSE COUNSEL

ALM

GC New York

JULY 17, 2006

Sounding the Alert On Data Breaches

Panoply of state laws on individual notification puts companies in a difficult position.

ART BY ISTOCKPHOTO

BY LISA J. SOTTO AND AARON P. SIMPSON

DURING THE PAST YEAR, news headlines announced a steady stream of information security breaches. During this time, roughly 170 breach incidents have been subject to public scrutiny; countless other incidents have gone unreported. It is estimated that more than 81 million individuals have been impacted by the publicized security breaches alone, including 26.5 million individuals whose personal information was contained on a laptop computer lost by an employee of the Department of Veterans Affairs in late May. While security breach incidents certainly occurred prior to 2005, a little-known California law passed in 2002 brought about the sudden surge in news coverage of such incidents.

This law, known as the California Computer Security Breach Notification Act (SB 1386), requires businesses to notify California residents whose personal information has been the subject of a security breach.

Lisa J. Sotto, *a partner in the New York office of Hunton & Williams, heads the firm's privacy and information management practice. She also serves as vice chairperson of the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee.*
Aaron P. Simpson *is an associate in Hunton & Williams' New York office.*

Not to be outdone, 29 other states have jumped on the California bandwagon and passed breach notification laws of their own after witnessing the broad impact of the California law. With no federal law imminent, businesses that suffer security breaches are finding themselves in the unenviable position of having to comply with 30 state laws that require notification to affected individuals. Making matters more complex, many of these 30 state laws differ substantially, upping the ante on the need for a thorough understanding of the legal landscape in this ever-evolving area.

California and Other States

Under California's SB 1386, businesses are required to notify individuals if personal information about them maintained in computerized form was, or is reasonably believed to have been, acquired by an unauthorized person. "Personal information" means an individual's name in combination with a (i) Social Security number, (ii) driver's license or state identification card number, or (iii) account, credit or debit card number in combination with any required security code. The law provides a safe harbor for encrypted personal information such that notification is not required in the event of unauthorized acquisition.

If notification is required, businesses may satisfy the law's requirement by providing (i) written notice, (ii) electronic notice under limited circumstances, or (iii) substitute notice (consisting of e-mail notice, conspicuous posting on the business' Web site, and notification to major statewide media) if notifying customers will cost more than $250,000 or if more than 500,000 customers are impacted.

In the initial months following the effective date of SB 1386 on July 1, 2003, companies that suffered security breaches complied by providing notice to impacted individuals in California. If the breach impacted people outside of California, many companies chose not to notify these non-California residents, reasoning that the legal notification obligation was limited to residents of California. While this approach is correct from a strict legal perspective, companies that took this approach suffered significant reputational harm in the media firestorm that ensued following discovery of the breach. This media frenzy resulted in the passage of state security breach notification laws in a handful of other states in which state legislators feared businesses would continue to suffer breaches and not notify their state residents. This handful, which did not begin passing breach notification laws until 2005, quickly became 30 states by the beginning of 2006.

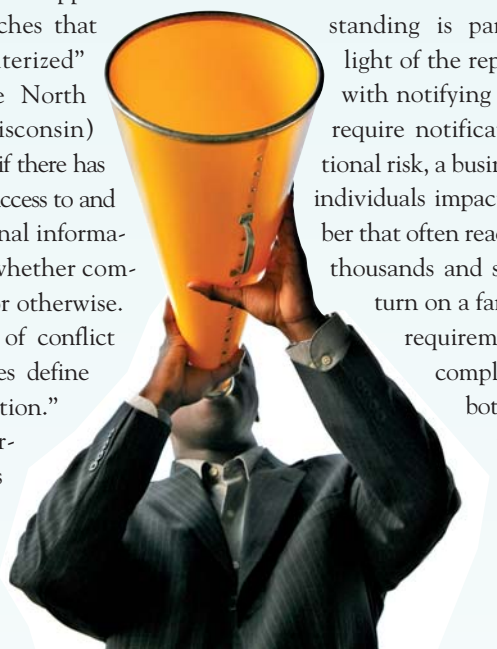
> *It is imperative that businesses fully understand, and prepare to address, each of the 30 state laws governing breach notification.*

The panoply of security breach notification laws at the state level has made compliance challenging for companies that have suffered national breaches in the past year. While the state laws are similar in many ways, they differ in four crucial ways, all of which bear on a company's notification obligations. First, the laws address different media. While most states follow California's approach and regulate breaches that involve "computerized" data, others (like North Carolina and Wisconsin) require notification if there has been unauthorized access to and acquisition of personal information in any form, whether computerized, paper or otherwise.

A second area of conflict arises in how states define "personal information." A significant percentage of states follow California's approach and define personal information to include name plus Social Security number, driver's license or state identification card number, or financial account number. Other states, however, use a more expansive definition of personal information. For example, personal information includes medical information in Arkansas, date of birth and mother's maiden name in North Dakota, and DNA profile in Wisconsin.

A third key difference among the state laws turns on whether the law contains a harm threshold that triggers notification. In California, no such harm threshold exists—all California residents whose personal information has been acquired, or is reasonably believed to have been acquired, must be notified. That is not true in several states, where notification is required only if there is a reasonable likelihood that information acquired by an unauthorized person will result in harm. In addition, the state laws have different requirements about who should be notified by businesses that suffer security breaches. In California, businesses are required to notify only those individuals affected by the breach. In other states, state regulators and consumer reporting agencies must be notified. For example, in New York and North Carolina, businesses that suffer security breaches must notify the Attorney General's office, while in New Jersey the state police must be notified.

These substantive differences highlight the need for businesses that suffer a breach to understand all 30 state laws. This understanding is particularly important in light of the reputational risk associated with notifying only in those states that require notification. Given this reputational risk, a business' decision to notify all individuals impacted by a breach (a number that often reaches into the hundreds of thousands and sometimes millions) can turn on a faraway state's notification requirement. Thus, from both a compliance perspective and a bottom line perspective, it is imperative that businesses fully understand, and



prepare to address, each of the 30 state laws governing breach notification.

How to Respond

The first, and most critical, step any company that learns of a possible security breach must take is to determine whether personal information is reasonably believed to have been acquired or accessed by an unauthorized person. In making this determination, companies should look to several indicators, including whether the information (i) is in the physical possession or control of an unauthorized person (e.g., a stolen computer), (ii) has been downloaded or copied, or (iii) was used by an unauthorized person, such as having fraudulent accounts opened or reported instances of identity theft. Making this determination is often easier said than done. Depending on the complexity of the circumstances, determining whether a breach has even occurred could require working with a forensic investigator, at significant expense, to recreate activity on the database.

Once there is a reasonable belief that a security breach has occurred, the next step involves going to law enforcement (if necessary) and taking any internal measures necessary to restore the integrity of the affected system. As part of the report to law enforcement, companies should explain that they intend to provide notice of the breach to affected individuals in the most expedient time possible and without unreasonable delay. In certain situations, law enforcement authorities will ask companies to delay notification so as not to impede their investigation. Most of the state breach notification laws provide a safe harbor for these circumstances, but companies in this situation should make sure to ask law enforcement when it would be appropriate to send the notification and to be prepared to send the notices as soon as reasonably practicable after getting the go-ahead from law enforcement.

Once given the go-ahead to notify, companies should provide written notice to affected individuals in the most expedient time possible. In some states, such as Florida and Ohio, there is a time limit of 45 days after discovering the breach or receiving the go-ahead from law enforcement. Depending on the sensitivity of the circumstances, drafting breach notices can be an arduous task that requires significant assistance from counsel and public relations resources. At the very least, a breach notice should include (i) a general description of what happened, (ii) the nature of the personal information involved, (iii) a description of the steps taken by the company to protect personal information from further unauthorized acquisition or access, (iv) a description of how the company will assist affected individuals (e.g., by providing credit monitoring for the affected individuals), (v) information on how individuals can protect themselves from identity theft, including contact information for the three credit reporting agencies, and (vi) contact information for the Federal Trade Commission.

In addition to affected individuals, companies that suffer security breaches may be required to notify other stakeholders, including state and federal regulators, credit reporting agencies and credit card issuers. New York, New Jersey, North Carolina and Maine all require some form of notification to state regulators, typically the state Attorney General's office. New Jersey is unique in that it requires companies that suffer a security breach to notify the state police, and this notification must take place prior to notifying affected individuals.

The notification to state regulators should provide information as to (i) the nature and circumstances of the breach, (ii) the timing, content and distribution of the notices, and (iii) the approximate number of affected individuals. Because the credit reporting agencies will likely be inundated with calls from individuals affected by the breach who wish to sign up for credit monitoring or obtain a credit report, it is also a good idea, and a legal requirement in several states, to notify the credit bureaus. In Minnesota, this notification is required to occur within 48 hours of notifying affected individuals. Finally, if the breach involves personal information associated with a credit card, the company is likely contractually required to notify affected credit card issuers.

Planning Is Key

Given the panoply of state breach notification laws and their varying requirements, it is only a matter of time before Congress passes a federal security breach notification law. There are currently more than a dozen security breach notification bills that have been introduced in Congress. Most commentators agree that a law will not be passed by the end of this fall's congressional session. From a business perspective, the most important feature of any federal breach notification law is that it pre-empt state law. Because data often flows beyond state boundaries, a federal law that pre-empts state breach notification laws would ensure that affected residents of every state are notified of a data breach while at the same time easing the ability of companies to provide such notification by allowing them to adhere to a single standard.

Until a federal law is passed, companies that suffer security breaches across state lines find themselves in the difficult position of analyzing the law in 30 or more states to understand their compliance obligations. Given the reputational risks associated with security breaches, in addition to legal compliance exposure, it is imperative that companies not only understand these issues, but also have a plan in place to manage the notification process in the event they suffer a security breach.