ASAP™

A Littler Mendelson **Time Sensitive** Newsletter

in this issue:

MARCH 2006

Employers in twenty states, now including Ohio and Pennsylvania, are required to notify employees of a security breach that exposes them to identity theft, highlighting the importance of incident response planning.

Responding to Security Breaches Under Ohio's and Pennsylvania's New Notice-of-Security-Breach Statutes and Other States' Notice Laws

By Philip L. Gordon and Christa Fossee

Beginning in February 2005, the media reported a flood of data security breaches involving some of the nation's largest financial institutions, most respected corporations, and major universities. According to a chronology maintained by the Privacy Rights Clearinghouse, more than 125 security breaches were reported between February 2005 and February 2006, putting at risk the personal information of more than 50 million Americans. These security breaches exposed the affected individuals to identity theft and were very costly for many of the organizations that experienced them, resulting in disruption of business activities, loss of reputation, and damage to employee morale. While Congress debated many bills in response, it enacted none.

However, twenty states, most recently joined by Ohio and Pennsylvania, have enacted legislation mandating that all businesses in possession of "personal information" notify those affected by a security breach. The states that have enacted such notice laws, in addition to Ohio and Pennsylvania, include the following: Arkansas, California, Connecticut, Delaware, Florida, Illinois, Louisiana, Minnesota, Montana, North Carolina, New Jersey, New York, Nevada, North Dakota, Rhode Island, Tennessee, Texas, and Washington. While these statutes have some significant differences in their details, the new Ohio and Pennsylvania laws, which are described below, are substantially similar in their principal provisions to the other eighteen state notice laws.

The Principal Provisions of Ohio's and Pennsylvania's Notice Statutes

Under Ohio's notice law, effective February 17, 2006, and Pennsylvania's law, effective June 20, 2006, anyone who owns or licenses "personal information" must notify any state resident whose unencrypted personal information was, or reasonably is believed to have been, acquired by an unauthorized person. These laws, like the laws of most jurisdictions, define "personal information" to mean an individual's name accompanied by (a) a social security number, driver's license or state identification number, or (b) an account, credit or debit card number in combination with any security code or password that would permit access to the individual's financial account.

The laws include some limitations on the notice obligation. Notice is required only if the unauthorized acquisition causes, or if it is reasonably believed it will cause, a material risk of identity theft or other fraud. The theft or loss of personal information that is encrypted will not trigger the notice obligation.

Federally regulated financial institutions and healthcare-related entities subject to regulation under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) are exempt from the law, albeit such entities will be required to provide notice under other federal laws.

Ohio's and Pennsylvania's notice laws, like those of all other states except New York and North Carolina, do not prescribe the content of the notice, but these statutes do establish several procedural requirements. Notice must be provided without unreasonable delay after the discovery of the security breach unless a law enforcement agency determines that notice would impede a criminal investigation or jeopardize national security — for example, because the notice would tip off a hacker under criminal investigation. Notice may be provided by letter or by telephone. Ohio's notice law, like Florida's, is exceptional by setting a specific outside time limit — 45 days from the date of discovery — for providing notice. Notice may be provided in writing or electronically under certain circumstances. Ohio and Pennsylvania join Connecticut, Montana, and North Carolina as the only states that permit notice by telephone. If more than 1000 Ohio residents or more than 1000 Pennsylvania residents are affected by the security breach, the entity also must notify the major credit bureaus. The laws of Florida, Minnesota, New York, Nevada, North Carolina, Tennessee, and Texas have similar provisions.

State notice laws pose a particular challenge for multi-state employers. Security breaches involving employee information typically do not affect just employees who reside in one state. The theft or loss of a back-up tape containing payroll information, for example, generally will result in the unauthorized acquisition of personal information concerning employees in all of the employer's locations. In these circumstances, a multi-state employer will be required to comply with the notice laws of every state in which affected employees reside. Given the variations of these laws in their details, multi-state employers typically will need to confer with in-house or outside counsel who can ensure that the employer's response to the incident satisfies the varying requirements of each state that has enacted a notice law and in which employees reside. By way of illustration, an employer with employees in Ohio and California would need to determine whether notice to the national credit bureaus is required because California's notice statute includes no such requirements, but Ohio's statute does in the circumstances described above.

The Impact of State Notice Law on Employers

While none of the state notice laws are expressly directed to employers, these laws could potentially impose notice obligations on virtually all employers. Employers, as a matter of course, collect employee social security numbers. Employers with vehicle fleets generally maintain driver's license information on all employee-drivers, and many employees provide driver's license information as a means of identification for purposes of verifying eligibility to work in the United States.

Employers not only possess personal information subject to the notice law, they also are frequently forced to confront security breaches for a variety of reasons. Time Warner, for example, disclosed that a container of computer tapes containing the personal information of 600,000 current and former employees had been lost in transport to a data storage facility. Science Applications International Corporation (SAIC), one of the largest employee-owned companies in the United States, announced that stolen computers contained personal information for all 45,000 of SAIC's current and former employee-shareholders. The victims included former high-ranking military and intelligence officials with top secret security clearances, such as the former Deputy Director of the Central Intelligence Agency and the former Chief Weapons Inspector for Iraq. Boeing Corporation reported that a computer containing the personal information of approximately 161,000 employees was stolen, and Honeywell International recently discovered that the personal information of 19,000 current and former employees had been posted on an internet website.

Preparing For, and Responding To, a Security Breach

Given that security breaches can result in damaging publicity and out-of-pocket expense and undercut employee and customer loyalty, employers should prepare well in advance to respond to a reported breach. These steps typically should include the following:

Build an Incident Response Team: The team should include (a) information technology (IT) personnel who can investigate the source of the breach, determine the scope of the breach, identify necessary remedial measures, and act as liaison with law enforcement authorities if they are contacted; (b) human resources professionals who will manage employee relations issues, including the imposition of discipline on any employee who is responsible for the breach and helping victimized employees protect themselves from identity theft; (c) business unit leaders or marketers who will address customer relations issues; (d) in-house or outside counsel who can evaluate the entity's obligations, if any, under all applicable state notice statutes, draft the notice when necessary, and provide other related legal advice; and (e) public relations specialists who can respond to press inquires and work to

minimize damage to business reputation.

Prepare the Team For a Security Incident: Team members should be assigned specific roles and responsibilities. Contact information should be distributed. All team members should understand that they must be available "24/7" to respond to an incident.

Conduct Security Awareness Training: Employees should be trained on how they can help improve the security of information systems and how to identify suspicious activity indicative of a security breach. Employees also should be provided contact information for the person who will receive reports of suspicious activity.

When a security incident does occur, there are several steps that can be taken immediately to mitigate the potential harm of the breach.

1. Investigate the Breach. The investigation should focus initially on the cause of the breach and any measures that are necessary to prevent future unauthorized access to personal information resulting from the breach. The investigation also should determine the categories of information that were acquired by an unauthorized person, the state of residence of all affected individuals, and the total number of affected individuals.

2. Contact Law Enforcement. If the initial investigation suggests that the security breach involved criminal conduct, law enforcement authorities should be promptly notified, and a police report should be completed. The entity's liaison with the police should discuss the timing of notice.

3. Determine Notice Obligations. The state of residence of affected individuals will drive the determination of which states' notice laws apply. While state notice laws are substantially similar, as noted above, there can be material variations from state to state.

4. Prepare a Notice of Security Breach. The organization should assume that any notice of security breach will become available to the general public. Accordingly, a notice of security breach should be drafted with care. Such notices typically should include a brief explanation of the incident, a description of the measures taken to prevent a recurrence, the steps that affected individuals can take to reduce their potential exposure to identity theft, and a contact person at the organization who can provide additional information. The organization also should consider whether it will offer additional assistance to affected individuals, such as credit monitoring, and if so, the extent of the offer.

5. Take Appropriate Remedial Action. The steps that will need to be taken in the aftermath of a security breach will vary depending upon the nature of the breach. Issues that may need to be addressed could include repairing customer or employee relations, disciplining responsible employees, and implementing additional security measures.

Conclusion

No information security program can guarantee perfect security. Thus, the question for employers is not whether but when will a security breach occur. In light of the number of states that have enacted notice laws and their potential extra-territorial reach, all employers should consider taking proactive steps to prepare for a security breach.

Philip L. Gordon is a Shareholder in Littler Mendelson's Denver office, and Christa S. Fossee is an Associate in Littler's Columbus office. If you would like further information, please contact your Littler attorney at 1.888.Littler, info@littler.com, Mr. Gordon at pgordon@littler.com or Ms. Fossee at cfossee@littler.com.