insight

A LITTLER MENDELSON REPORT

SEPTEMBER 2007

An Analysis of Recent Developments & Trends

LITTLER MENDELSON, P.C.
THE NATIONAL EMPLOYMENT & LABOR LAW FIRM®

Employers Face New Compliance Challenges As Massachusetts Becomes the 39th State to Enact a Security Breach Notice Law

by: Philip L. Gordon and Martha M. Walz

Summary: New notice-of-security-breach laws can transform misdirected e-mail, stolen laptops, and other potential security incidents into a major legal compliance challenge for employers.

Misdirected e-mail, lost and stolen laptops, and security flaws in corporate websites, when they expose employee personnel information to unauthorized individuals, are now more than a potential embarrassment; they are a legal compliance challenge, especially for multi-state employers. With Massachusetts recently becoming the 39th state to pass a notice-of-security-breach statute, it is just a matter of time before all fifty states require notice of a security breach. While these statutes share a common thread, their requirements can materially vary, complicating the determination whether an employer has a legal obligation to notify employees and, if so, the steps that the employer must take to discharge its legal responsibilities.

Regrettably, it no longer is a matter of "if", but "when," human resources professionals and in-house counsel will be required to confront this legal compliance challenge. In a 2007 study conducted by the Ponemon Institute, a leading think tank on privacy and data protection, 85% of respondents had suffered a security breach within the previous 24 months, and 81% had been required to notify individuals of the breach. With the centralization and digitalization of employees' personal data into computerized human resources information systems (HRIS), security breaches involving personnel information are likely to become increasingly common and involve ever larger numbers of current and former employees, raising the stakes each time a security breach occurs.

Reviewing the provisions of the new Massachusetts notice law with reference to the thirty eight notices statutes which preceded it helps to highlight the most significant similarities and the most salient differences among these laws. With a full view of the variegated, legislative landscape, employers can more readily determine when and how they are required to provide notice.

The Extraterritorial Reach of the Notice Statutes

Like most other notice statutes, the Massachusetts law reaches beyond the state's borders by requiring any business which owns or licenses "personal information" (defined below) concerning a Massachusetts resident to notify that resident about a breach. In other words, a business that suffers a hack to its human resources database stored on a server at its California headquarters must comply with Massachusetts' notice law if the business employs any Massachusetts residents. If the hack were to expose the personal information of employees who reside in any state besides the eleven that have not yet enacted a notice statute,[1] the business would be required to comply with the notice statutes of those states as well. The fact that the security breach occurred only in California would not be controlling. Consequently, determining the state residency resident of affected employees is one of the first steps an employer should take when investigating a security incident.

Understanding the "Trigger Event" for Notification

All notice statutes (except those of Connecticut, New Jersey, and Vermont) define the *trigger event* for notice to require, *at a minimum*, the unauthorized acquisition of unencrypted, computerized, personal information. In Connecticut, New Jersey, and Vermont, unauthorized access to personal information (even without acquisition) is enough to trigger a notice obligation. In practical terms, this means that a hacker who is a voyeur, but not a thief, could trigger an obligation to notify in these states simply by, for example, perusing a payroll database.

[1] Alaska, Alabama, Iowa, Kentucky, Mississippi, Missouri, New Mexico, South Carolina, South Dakota, Virginia, or West Virginia are the only states that have not, thus far, enacted a security breach notice law.

continued...

continued from cover

Approximately one dozen states (including California, New York, and Texas) have adopted the "basic definition" of a security breach set forth above. The majority of states, however, have varied the basic definition in at least one of three significant ways.

First, Massachusetts, like only four other states (Hawaii, Indiana, North Carolina, and Wisconsin), requires notice to be given when a "paper breach" occurs. Thus, a business with employees residing along the entire East Coast whose human resources director had a briefcase full of paper files snatched at the airport might have a legal obligation to notify employees who reside in Massachusetts and North Carolina, but would have no legal obligation to provide notice to any of the business' other employees. While following such a course most likely would spawn an employee relations disaster, the hypothetical presented highlights the limited application of most notice statutes to security breaches involving "computerized" data.

Second, eleven states (Arkansas, Delaware, Georgia, Maryland, Massachusetts, Montana, North Carolina, North Dakota, Nebraska, Oregon, and Wisconsin) have expanded upon the standard definition of *personal information* which forms part of the basic definition of a security breach. Under all notice statutes, *personal information* means, *at a minimum*, a resident's first name or initial and last name *plus*: (1) social security number; (2) driver's license number or state-issued identification card number; or (3) financial account, credit or debit card number with any required security code, or personal identification number (PIN) that would permit access to a financial account.

The states listed in the paragraph above have varied this definition in a number of ways with an impact on employers. Under Massachusetts law, for example, a credit card, debit card or financial account number *is* "personal information" even without a required security code or PIN. Thus, bank account information used for direct deposit purposes would constitute "personal information" under Massachusetts law even if the account could not be accessed without a PIN. Other additions to the standard definition of "personal information" include medical information (AK, DE); passport number (OR); unique biometric data, such as a fingerprint (NC, NE, WI); and date of birth (ND).

Third, in the majority of states, notice is not required if the security incident results in no reasonable likelihood of harm or identity theft to the individuals whose personal information has been exposed. Massachusetts has set an even higher threshold, excusing businesses from providing notice unless the security incident "creates a substantial risk of identity theft or fraud against a resident of the commonwealth." These "materiality" standards recognize that a business should not be required to undertake the potentially time-consuming and expensive task of providing notice of a security breach when the purpose behind the notice statute, to help protect affected individuals from identity theft, does not come into play.

Unfortunately, these materiality standards may be easier stated than applied. For example, when a laptop with a password is stolen, how can an organization evaluate the unknown thief's ability to crack or bypass the password and, therefore, the likelihood that personal information stored on the laptop might be used to commit identity theft. Faced with these difficult-to-answer questions, many organizations have chosen to err on the side of providing notice, trying to protect themselves against government investigators with 20/20 hindsight. In some circumstances, however, this conservative approach could be unfair to the notice's recipients who, once notified, must worry about being victimized by identity thieves (and take preventive action) despite the potentially low risk that the security breach would expose the recipient to identity theft.

One final caveat: encryption provides a safe harbor from the legal obligation to provide notice under all state notice laws. Many organizations have been reluctant to implement encryption in many of their information systems because of potential operational difficulties and lost computing speed. However, this safe harbor may be more inviting for discrete categories of "personal information," such as human resources data stored on laptop computers. According to a 2006 Ponemon Institute study, respondents reported that security breaches cost their organization $30 per exposed record in lost productivity and $54 per exposed record in direct costs, such as mailing costs and attorneys' fees. Given these figures, the potentially large number of employees whose information is at risk, and the significant possibility that a laptop with employees' personal information will be lost or stolen, purchasing disk-based encryption software for laptop computers issued to human resources professionals would appear to be a wise investment for many organizations.

Legal Obligations Upon the Occurrence of the Trigger Event

Massachusetts' notice law, like every other notice law, distinguishes between those who own personal information and those, like third-party service providers, who use personal information on the owner's behalf. The obligation of a service provider is limited to prompt notification of the owner. By way of illustration, if a rogue employee at a payroll administrator steals the personal information of a client's employees, the payroll administrator's legal obligation is limited to notifying the client (albeit the parties could impose additional obligations, such as an indemnification, on the service provider by contract), while the client maintains the ultimate legal obligation to provide notice to employees. Under Massachusetts' law, the service provider's notice must: (1) state when the security incident occurred; (2) describe the incident; and (3) list the steps taken or planned to address the incident. No other state prescribes the content of this type of notice.

Employers who are required to notify their workforce of a security breach should view the notice as an important employee relations communication. Employees who receive the notice (except perhaps IT personnel) will have had no control over the employer's actions in safeguarding their personal information. The notice's recipients very well may be angry that they now are at risk of identity theft and most likely will expect the employer to take full responsibility for righting this perceived wrong.

continued from page 2

In addition to adopting a tone that matches these circumstances, the employer should consider including the following information in the notice of security breach to its employees:

- A general description of the incident;
- The categories of personal information which were, and were not, compromised;
- The steps taken to end the security incident and to prevent a recurrence;
- The steps the employer is taking to help the employee, such as offering free credit monitoring or identity recovery service;
- The steps the employee can take to protect themselves, such as reviewing account statements for suspicious activity and obtaining a free copy of their credit report;
- A telephone number at the employer for additional information.

Because most state notice laws do not prescribe the content of the notice and most of those that do provide relatively limited requirements, a notice that addresses all of these points will satisfy most state notice laws with minor exceptions. Massachusetts, for example, requires that the notice inform recipients: (1) of their right to obtain a police report; and (2) on how to place a security freeze.

While notice to affected individuals is the data owner's primary notice obligation, Massachusetts also requires notice to the state's Attorney General and to the Director of Consumer Affairs and Business Regulation. Seven other states (Hawaii, Louisiana, Maine, Maryland, New Hampshire, New Jersey, North Carolina) impose similar requirements to notify state agencies although the requirement is triggered in Hawaii and North Carolina only if the breach affects more than 1,000 state residents. Most state agencies that are to be notified have developed forms for providing the notice. To date, state agencies typically have acted in response to such notices only when a very large number (several thousand or more) state residents are affected and the circumstances of the breach are particularly egregious.

Approximately two-thirds of notice statutes require a third type of notice, notice to the national credit bureaus — Equifax, Experien, and Transunion. This notice is intended to permit these credit bureaus to arrange for sufficient staff to handle a potential "bump" in the number of callers seeking to exercise their right under the Fair and Accurate Credit Transaction Act to receive a free copy of their credit report. In light of this purpose, notice to the national credit bureaus is not required in any state (except Massachusetts, Minnesota and Montana) unless the breach involves 1,000 or more state residents.

Timing of the Notice

Only three states (Florida, Ohio, and Wisconsin) impose a fixed deadline for notifying affected individuals — 45 days from discovery of the breach. All other states, including Massachusetts, require notice "without unreasonable delay." This standard permits an employer to conduct a reasonable investigation to determine whether a "trigger event" has occurred, to obtain the information needed to provide affected employees with a meaningful notice, and to make the necessary arrangements for distributing the notice. Even when operating under the more flexible standard, employers should consider using 45 days as a rule of thumb for the outside time limit for providing notice. In some circumstances, taking more than 45 days after discovery of a breach to provide notice could suggest to employees that the employer was trying to cover up the breach or was insufficiently concerned about its employees' interests.

While employers should notify affected employees with all due speed, every notice statute permits notice to be delayed at the request of law enforcement. Such requests might occur, for example, when law enforcement is attempting to track down a hacker and is concerned that public disclosure that the hack has been uncovered might "scare off" the hacker before he or she can be located. Employers relying on this exception should carefully document all communications with law enforcement concerning the timing of the notice and check for additional state law requirements. Under Massachusetts' notice statute, for example, an employer can rely on this exception only if law enforcement authorities have notified the Attorney General of the need for delay.

Delivery of the Notice

Notifying employees by letter is the most commonly used form of notice and is permitted under all notice laws. All notice laws also permit notice by electronic mail. E-mail notice, though potentially less expensive than notice by "snail mail," has several disadvantages. First, under most notice laws, an employer resorting to e-mail notice must comply with the Electronic Signatures in Global and National Commerce (E-SIGN) Act, 15 U.S.C. §7001. The E-SIGN Act requires that the employer, among other things, obtain the employee's consent to receive notice electronically before relying upon notice by e-mail, meaning that each affected employee must be sent two e-mails. Second, if former employees need to be notified, the employer may have only an outdated e-mail address or no e-mail address at all. Third, e-mail notices can be more easily distributed over the Internet, potentially increasing the public attention received by the security incident.

While more than one dozen states authorize notice by telephone, such notice cannot be accomplished by automated means because most notice statutes require that notice by telephone be given directly to the affected individual and that the telephone call be documented. Satisfying these requirements when more than a few dozen employees need to be notified generally would be a time-consuming and expensive undertaking.

When a breach implicates the personal information of former employees who have not worked for the employer for one year or more, or who are relatively transient, the employer may have difficulty providing notice by mail, e-mail or telephone for lack of current contact information. In those circumstances, all of the notice laws provide for "substitute notice." This form of notice typically entails clear and conspicuous posting of the notice of security breach on the business' home page and publication or broadcast in statewide news media.

continued from page 3

All of the notice laws also permit substitute notice when the cost of individual notice would be high or when the number of affected individuals is particularly large, although the thresholds vary among the states. Massachusetts, for example, permits substitute notice when the cost of individual notice would exceed $250,000 or the number of affected individuals exceeds 500,000. In Wyoming, by contrast, those thresholds are $10,000 and 10,000 affected individuals for Wyoming-based business, but the thresholds are the same as those in Massachusetts for businesses based outside of Wyoming.

Ten Key Questions to Ask When Investigating a Security Incident

To address the statutory requirements described above, those charged with investigating and responding to a security incident should obtain responses to the following ten questions:

1. What happened?
2. Was law enforcement contacted and, if so, was there a request to delay notice?
3. Was "personal information" acquired, or only accessed, by an unauthorized persona?
4. What categories of "personal information" were and were not compromised?
5. Was the personal information in paper or electronic form?
6. Was the personal information encrypted or subject to any other security measures?
7. What is the likelihood that the compromised information will be used to commit identify theft?
8. How many individuals were affected and in which state(s) do they reside?
9. What steps have been taken to prevent additional "leakage"?
10. What steps have been taken to prevent a recurrence?

Recently Enacted Data Protection Legislation

Employers should note that data protection legislation aimed at reducing the risk of a security breach often accompanies a notice-of-security-breach law. While not directed expressly at employers, these laws, like the notice laws, typically encompass any business which owns or licenses "personal information" and necessarily encompass all employers who, at a minimum, collect employees' social security numbers.

The legislative act containing Massachusetts' notice law, for example, also requires that businesses dispose of "personal information" in a way which renders the information irretrievable, regardless of whether the information is in paper or electronic form. More than one dozen states have enacted similar legislation. The Texas Attorney General recently has demonstrated that these document disposal laws can have teeth, instituting administrative proceedings against several businesses which exposed thousands of pages of paper records to "dumpster divers." The Texas law authorizes recovery of a penalty of $500 per violation, *i.e.*, for each page containing personal information which is not properly destroyed.

More than two dozen states now impose limits on certain disclosures and transmissions of social security numbers. More specifically, these statutes typically prohibit (1) the public display of SSNs, such as on an identity badge; (2) the printing of SSNs on cards used to obtain goods or services, such as insurance cards; (3) requiring an individual to transmit an SSN over the Internet — for example, in an on-line job application — unless the transmission is secure or the SSN is encrypted; and (4) mailing a document which contains an SSN unless the document by law is required to include the SSN (*e.g.*, a Form W-2) and in certain other limited circumstances.

These data protection laws, when coupled with the potential cost and embarrassment associated with security incident response, should encourage employers to review their information-handling processes and to take steps to reduce the risk of a security breach before they are required to provide notice.

Conclusion

Given the variations in these state notice laws, 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. Counsel will first need to determine whether there is a legal obligation to provide notice and, if so, whether that obligation requires notice only to affected individuals or to state agencies or the national credit bureaus as well. Even when no law requires notice — for example, in the case of a "paper breach" involving only residents of California, New York, and Texas, the employer still should consider providing notice for employee relations purposes. Once the decision to notify has been made, the employer will need to prepare and distribute a notice that contains all of the required information and, at the same time, communicates to the workforce the employer's regret over the inconvenience caused by the incident and the employer's commitment to minimizing that inconvenience for its workforce.

Philip L. Gordon is a Shareholder in Littler Mendeson's Denver office. Martha M. Walz is Of Counsel in Littler Mendelson's Boston office. She is also a member of the Massachusetts House of Representatives. 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. Walz at mwalz@littler.com.