A Timely Analysis of Legal Developments

ASAP®

In This Issue:

October 2008

New Massachusetts regulations effective January 1, 2009, mandate the development of a "written, comprehensive information security program" to safeguard the personal information of Massachusetts employees and consumers. These new regulations represent a new phase in efforts by states to combat identity theft. They should be a wake-up call to employers and their human resources departments to implement policies and procedures to safeguard employees' personal information.

New Massachusetts Regulations Impose Substantial Obligations on Corporate Human Resources Departments to Safeguard Employees' Personal Information

By Philip L. Gordon

New Massachusetts regulations, effective January 1, 2009, are a clarion call for corporate human resources departments to join the war on identity theft. The regulations mandate the development and implementation of a "written, comprehensive information security program" to safeguard the personal information of Massachusetts employees and consumers. Such a program rarely will be fully effective without the involvement of human resources professionals and in-house employment counsel.

While these regulations apply only to organizations with Massachusetts employees, even organizations without a Massachusetts presence should consider implementing a similar program. These regulations likely will be a model for other jurisdictions and could become the standard against which all information security programs are measured.

The Massachusetts Regulations' Potentially National Ramifications

The cornerstone of the new Massachusetts regulations is a mandatory, "comprehensive, written information security program" that encompasses all "personal information," whether in paper or electronic form, concerning Massachusetts residents. At first blush, these regulations appear to call for the attention only of Massachusetts-based IT professionals, but, in fact, they demand the attention of *every* human resources professional and in-house employment counsel.

Most immediately, these regulations will have an impact on every business with Massachusetts employees. The regulations define "personal information" to mean first name or initial and last name plus (a) Social Security number (SSN); (b) driver's license number or other state-issued identification number; and (c) credit or debit card number, or other financial account number, with or without any required security code. Information falling within the scope of this definition is present in virtually every human resources department, or held by third-party service providers on the organization's behalf.

Significantly, the regulations themselves do not expressly state that their reach is limited to personal information stored within Massachusetts' borders. Consequently, corporate human resources departments arguably will be required to apply these regulations to Massachusetts employees' personnel information imported into centralized HR databases located outside of Massachusetts. Because it will be burdensome, if not impossible as a practical matter, to comply with at least some of the regulations' requirements (described below) only with respect to the personal information of Massachusetts employees, many organizations may have no choice but to apply these regulations to all personnel information.

National employers with Massachusetts employees would be taking a risk by reading the regulations to apply only to personal information stored in Massachusetts. Under Massachusetts' security breach notification law, which included a provision mandating the promulgation of these regulations, any business responsible for a security breach involving the personal information of Massachusetts residents must notify not only the affected individuals but also the Massachusetts Attorney General. In other words, an organization with Massachusetts employees that does not apply the regulations to its extra-Massachusetts operations might be required, in the event of a security breach, effectively to admit to the Massachusetts Attorney General that the organization declined to give the Massachusetts regulations extraterritorial effect. In response to informal questioning on this issue, the Massachusetts Attorney General's Office declined to provide a definitive opinion, but recommended that employers "err on the side of caution."

Even employers with *no* Massachusetts employees should pay close attention to, if not comply with, these new Massachusetts regulations. Like California's groundbreaking security breach notification law enacted in 2002 that has now been followed by similar laws in more than 40 states, these regulations (in the absence of federal legislation) very well could become the national paradigm for regulating "personal information." Alternatively, the regulations may, in the future, be viewed by courts nationally as an appropriate standard of care for safeguarding personal information. As tens of millions of United States residents, including governors, state legislators, and judges receive multiple notices of security breaches of their own personal information, this prospect is not entirely remote.

The Massachusetts Regulations Demand the Attention of Human Resources Professionals and In-House Employment Counsel

While technology professionals most likely will take the lead in creating and implementing the mandated "comprehensive, written information security program," compliance with several aspects of that program most likely could not be accomplished in most organizations without the significant participation of human resources professionals and in-house employment counsel.

1. Information Handling Processes

To begin with, the regulations effectively call for a reexamination of all existing processes involving the collection, retention and use of personal information of Massachusetts residents. More specifically, the regulations require that an organization: (a) collect only the minimum personal information necessary to accomplish the purpose(s) for the collection; (b) retain the information only for as long as is necessary to accomplish that purpose; and (c) limit access to the information to those with a need to know. Applying these principles would, for example, require human resources departments to consider at what point in the hiring process should the SSNs of applicants be collected, for how long after the hiring decision should the SSNs of rejected applicants be retained, and which categories of employees should be permitted access to applicants' SSNs.

The regulations also require prompt deactivation of the user name and password of any terminated employee authorized to access personal information. While technology professionals will execute these tasks, the human resources professionals who track the ebb and flow of the organization's workforce will be at the hub of this process. Prompt termination of computer access is particularly critical when disgruntled employees or employees with system administrator privileges are involved.

2. Encryption

Massachusetts is the first state expressly to require encryption of employees' personal information (a Nevada law, effective October

1, 2008, requires encryption for the personal information of consumers). Under the regulations, encryption must be deployed for: (a) transmissions of personal information over the Internet, *e.g.*, e-mail; (b) all wireless transmissions of personal information, *e.g.*, wireless access to the corporate network; and (c) personal information stored on laptops and other portable storage media, *.e.g.*, compact disks, thumb drives, and Blackberries. While selecting and installing encryption software will fall to the technology professionals, human resources professionals will be responsible for ensuring that they actually use the encryption software for any e-mail containing the personal information of a Massachusetts resident in the body or in an attachment.

3. Portable Storage Devices

Given that the loss or theft of portable, electronic storage media has been an endemic cause of security breaches, the Massachusetts regulations mandate that organizations develop a policy to regulate when and how personal information of Massachusetts residents may be transported, stored and accessed off-site. In response to this mandate, the employer should decide, in the first instance, whether, and if so in what circumstances, employee personal information may be taken or stored off-site. Employers might consider, for example, a rule that prohibits the removal of any personal information off-site except when (a) there is a legitimate business need, and (b) the employee making the request would not be able to access the information through a secure, remote connection. By way of illustration, employees engaging in air travel would satisfy the exception because these employees would not be able to get a secure connection to corporate servers while on an airplane.

This policy also should identify the job categories authorized to take employees' personal information off-site, the process for obtaining approval for doing so, and the steps that an authorized employee must take to safeguard the information once off-site. These safeguards might include, for example, encryption, keeping the storage device with the employee at all times, and removing all stored personal information when the need for taking the information off-site has been accomplished. Another matter to consider is enforcement of the policy, such as by periodic audits of the hard drive of laptop computers to ensure that there has been no unauthorized storage of employees' personal information.

4. Vendor Management

Vendor management is another aspect of the regulations that will require the attention of any human resources department responsible for managing the personal information of Massachusetts employees. Under the regulations, the organization must conduct reasonable due diligence to verify that vendors will adequately safeguard personal information and also must obtain contractual assurances that each vendor will do so. While technology professionals most likely will need to take the lead in evaluating the information security programs of existing and prospective vendors, human resources professionals will need to identify and track these vendors, and in-house employment counsel should expect to be called upon to confirm that vendor agreements adequately address information security.

In addition to contractual safeguards, the regulations require the organization to obtain a written certification from each vendor that receives personal information of a Massachusetts resident. The certification should be a stand-alone document and must state that the vendor has a written, comprehensive information security program in compliance with Massachusetts' "Standards for the Protection of Personal Information of Residents of the Commonwealth."

Because the regulations do not expressly state that these vendor-focused requirements apply prospectively, employers should consider, at a minimum, obtaining a certification from each current vendor after January 1, 2009. Employers also should discuss with each current vendor the feasibility of amending existing agreements to address information security.

5. Training and Discipline

To prevent the "written, comprehensive information security program" from becoming an irrelevant paper tiger, the regulations mandate training on the requirements of the information security program as well as discipline for violating the program's rules. In most organizations, compliance with these requirements will require the cooperation of technology and human resources professionals. Human resources professionals generally will take the lead in administering and delivering training, with technology professionals

providing substantive assistance. When it comes to discipline, technology professionals often will originate reports of violations, but human resources professionals will be needed to ensure that discipline is imposed consistently with existing policies and procedures and in a uniform, non-discriminatory manner.

No One Right Answer

The regulations are not proscriptive; they do not identify specific hardware or software that must be used, nor do they provide specific policy language. To the contrary, the regulations acknowledge that information security programs will vary from organization to organization. While "every" written information security program must address all of the elements listed above (and several others), the regulations expressly permit for some flexibility. When evaluating compliance with the regulations, the Massachusetts Attorney General will be required to consider: (a) the size, scope and type of business in question; (b) the available resources; (c) the volume of stored personal information; and (d) the need for security and confidentiality of both consumer and employee personal information.

Conclusion

The Massachusetts regulations are a recognition that mere notification that a security breach has occurred is not enough to ensure information security. Rather, reducing the risk of a security breach in the first instance requires a programmatic approach that includes technical, physical and administrative safeguards. Successfully implementing these safeguards often will require the joint efforts of human resources and technology professionals.

Philip L. Gordon is a Shareholder in Littler Mendelson's Denver office, and Chair of Littler Mendelson's Privacy & Data Protection Practice Group. He maintains a blog on employment related privacy issues at http://privacyblog.littler.com. If you would like further information, please contact your Littler attorney at 1.888.Littler, info@littler.com, or Mr. Gordon at pgordon@littler.com.