[buck research]

fyi® for your information®

Volume 32 | Issue 61 | September 30, 2009

Massachusetts Takes on Identity Theft – Get Ready for the New Data Security Requirements

On August 17, 2009, the Commonwealth of Massachusetts issued new data security rules that will affect employers with workers who live in Massachusetts and businesses that serve Massachusetts residents. The rules, which are now scheduled to take effect on March 1, 2010, will require companies that touch personal information of Massachusetts residents to provide certain minimum safeguards to protect the information from unauthorized access, disclosure or misuse.

Background

In 2007, Massachusetts Governor Deval Patrick (D) signed into law comprehensive identity theft legislation, intended to protect the "personal information" of state residents. In September 2008, the Massachusetts Office of Consumer Affairs and Business Regulations (OCABR) issued regulations to implement the state's data security statute effective January 1, 2009. These data security regulations never took effect as revisions were made and effective dates were extended.

On August 17, 2009, OCABR issued revised regulations, extending the compliance deadline to March 1, 2010. The revised regulations establish minimum standards for businesses based in Massachusetts and outside the state with respect to safeguarding personal information about Massachusetts residents. Frequently Asked Questions (FAQs), which accompanied the latest regulations, clarify some of the new requirements and highlight important differences from earlier regulations.

Massachusetts Data Security Requirements

The OCABR regulations require organizations that "own or license" personal information about a resident of Massachusetts to take wide-ranging measures to protect that information from unauthorized access, disclosure or misuse. Among other things, the regulations generally require covered businesses to implement comprehensive information security programs, to encrypt all personal information stored on laptops or other portable devices (e.g., flashdrive, BlackBerry, cell phone) or data containing personal information that is sent over the Internet or by wireless connections, to take reasonable steps to select service providers capable of safeguarding personal information, and to contractually require service providers to protect personal information.

Personal Information Defined. The regulations define personal information as a Massachusetts resident's first and last name or first initial and last name in combination with one or more of the following –

- Social Security Number
- driver's license number or state-issued identification card number
- financial account, debit or credit card number (with or without PIN numbers or passwords).

Personal information is protected whether in paper or electronic form, but does not include information lawfully obtained from publicly available information, including federal, state or local government records.

Scope of Coverage. The regulations apply broadly to entities that own or license personal information, including any entity that "receives, maintains, processes or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment."

BUCK COMMENT. *Because employers that maintain personnel records or payroll information of Massachusetts residents would be subject to the new requirements, businesses with outside sales people and those with telecommuting policies must take extra care to ensure that they are familiar with and in compliance with the new regulations.*

Comprehensive Information Security Program Requirement. Covered businesses must develop, implement and maintain a comprehensive written data security program that meets certain minimum requirements for administrative, technical and physical safeguards, including –

- designating individual(s) to be responsible for the program
- determining where personal information is stored
- developing security policies for storing, accessing and transporting data with personal information off-site
- restricting physical access to records and storage of data in locked areas
- employee training and discipline
- routine monitoring of program effectiveness, with a review of the scope of security measures at least annually
- post-incident review of breach and corrective measures taken.

The regulations emphasize a "risk-based" approach to information security and allow covered businesses to tailor their data security programs to reflect their size, resources, amount of personal information, and need for security and confidentiality of consumer and employee information. Thus, these factors should be taken into account when designing a security program.

BUCK COMMENT. *Given these wide-ranging requirements, information security programs can be expected to impact many, if not most, functional areas of the corporation, As a practical matter, certain areas, such as HR, Benefits, Payroll and Legal, are more likely than others to receive, maintain, process or otherwise access personal information in connection with their jobs and tasks outsourced to their vendors.*

Thus, at a minimum, companies should ensure that these areas are working together with IT and other departments involved to develop appropriate safeguards, rather than in silos.

Computer Security Requirements. Covered businesses that electronically store or transmit personal information about a state resident must establish and maintain a security system covering their computers, including any wireless system. The regulations set forth minimum computer system security requirements, but limit them to steps that are "technically feasible." Although the regulations do not define what is technically feasible, the FAQs clarify that if there is a reasonable technological means to accomplish a desired result, it must be used. If, for example, it may not be technically feasible to encrypt cell phones, Blackberries or other similar devices, OCABR would look to other safeguards that can be implemented to protect personal information, such as secure websites and passwords.

Among other requirements, the security system must include secure user authentication protocols (e.g., passwords) and secure access control measures. In addition, firewall protection must be provided for files containing personal information on a system connected to the internet.

Contract and Oversight Requirements. The regulations require due diligence in overseeing third-party service providers, including taking reasonable steps to select and retain providers that are capable of taking appropriate security measures to protect personal information under state and federal law. The latest regulations reinstate a requirement that businesses contract with service providers to provide security measures consistent with Massachusetts regulations. As with the due diligence requirement, the new contract requirement extends to any applicable federal regulation.

Safe Harbor Provision. The regulations include a safe harbor for certain contracts – i.e., "any contract a person has entered into with a third party service provider prior to March 1, 2012, shall be deemed in compliance herewith, notwithstanding the absence in any such contract of a requirement that the service provider maintain such protective security measures, so long as the contract was entered into before March 1, 2010."

BUCK COMMENT. *Under this provision, covered entities with contracts in place prior to the effective date of the regulations would appear to have until March 1, 2012 to amend the contracts to require their service providers to implement and maintain appropriate security measures for personal information consistent with the new regulations and federal law. Because the language of the revised regulations is not entirely clear, and other states (e.g., Maryland) already require similar contract provisions, companies with personal information may want to consider amending their contracts sooner.*

Penalties. The Massachusetts Office of the Attorney General (OAG) is responsible for the enforcement of the state's data security regulations. The OAG may launch an investigation or file a claim against an entity that experiences a data security breach, regardless of whether the breach is reported by the entity. Severe penalties, up to $5,000 per violation, may be imposed when the entity is found to be in non-compliance with the regulations. A violation may be defined as broadly as $5,000 per individual record lost or stolen. These penalties are in

addition to the costs associated with notifying the individuals affected by the breach and any federal law mandates, e.g., credit monitoring, that may also be imposed against an organization.

Conclusion

As of March 1, 2010, companies doing business in Massachusetts or holding Massachusetts personal data, regardless of where the entity or the personal information is located, will have to implement certain measures to protect that information from unauthorized access, disclosure or misuse. Businesses that have not already done so should consider performing risk assessments and inventory personal information they receive, maintain, process or access. As they develop appropriate information security programs, companies should review and update policies, procedures and systems capabilities, and review their vendor operations to ensure compliance with the new regulations.

Buck's consultants are available to assist you in developing and implementing data security programs and vendor oversight programs that comply with the new Massachusetts requirements.