THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp
Editor: Kirk J. Nahra, CIPP

Businesses nationwide continue to grapple with Massachusetts data privacy laws

October 23, 2012

By David M. Governo and Corey M. Dennis, CIPP/US

There were over 1,800 data security breaches affecting more than 3.2 million Massachusetts residents between November 2007 and September 2011, according to a recent report from the Massachusetts Office of Consumer Affairs and Business Regulation. These incidents, most of which were reported by companies in the healthcare, financial services and retail industries, involved both malicious hacking and unintentional breaches.

Data security breaches result in substantial monetary and reputational losses for businesses. The best way for a company to protect itself from these costs and liability is to establish policies and safeguards to reduce the likelihood of a breach. At a minimum, it is essential to comply with applicable data privacy laws. Achieving this minimum level of compliance, however, is a difficult task and does not eliminate the risk of a data security breach. Thus, cyber liability insurance is quickly becoming a popular way for companies to mitigate their financial exposure.

Overview of MA data privacy laws

The Massachusetts data privacy regulations became effective in March 2010 and are among the most burdensome in the country. The regulations were enacted to combat the increased threat of data security breaches following several high-profile incidents, most notably the TJX Companies breach, which resulted in 94 million customer accounts being compromised and a multibillion dollar loss to the company, including fines, legal fees, notification expenses and brand impairment. The regulations apply to every “person” or entity—including businesses both inside and outside of Massachusetts—holding, processing or otherwise accessing personal information of Massachusetts residents.

The regulations require such businesses to establish physical, administrative and technical information security measures to safeguard personal information and to develop a “written comprehensive information security program” outlining those measures. Businesses must also

take reasonable steps to ensure that their third-party service providers; i.e., payroll providers, outsourcers, contractors, comply with the regulations and must require such service providers to implement security measures by contract. Further, all records containing personal information transmitted over public or wireless networks, or stored on laptops or other portable devices, must be encrypted. The requirements of encryption and of ensuring third-party service provider compliance have been some of the more challenging aspects of the laws.

The regulations adopt a risk-based approach to information security, which takes into account the size, scope and resources of the business as well as its need for security. A company's compliance obligations do not end once the security measures are implemented; rather, the regulations require regular monitoring and reviewing security measures at least annually to ensure they are preventing unauthorized access to personal information. Failure to comply with the regulations could result in penalties of up to $5,000 for each violation affecting a Massachusetts resident, along with injunctive relief, attorneys' fees and the reasonable costs of investigation and litigation.

Massachusetts has enacted two additional laws designed to protect the personal information of its residents. Mass. Gen. Laws Ch. 93H requires businesses, in the event of a data security breach, to give notice to any affected Massachusetts residents, as well as to the Attorney General's Office and the Office of Consumer Affairs and Business Regulations. Mass. Gen. Laws Ch. 93I requires any business disposing of documents or electronic media containing personal information to redact, shred, or otherwise destroy the records so that personal data cannot practicably be read or reconstructed.

Data privacy laws of other states

Massachusetts is not alone in enacting laws governing data privacy and security. Over the past several years, 46 of the 50 states have enacted data security breach notification laws. The data privacy laws of California and Rhode Island, for example, require businesses holding unencrypted personal information of state residents to implement "reasonable security procedures and practices appropriate to the nature of the information" and require by contract third parties to whom they disclose such information to implement those safeguards. Further, in the event of a security breach involving such information, the laws of both states require notification to affected residents "in the most expedient time possible."

Under Connecticut's data privacy laws, any business holding personal information must safeguard it to prevent misuse by third parties, and any business that collects Social Security numbers in the course of its business must create a "privacy protection policy" establishing safeguards for those Social Security numbers. The laws also require those doing business in Connecticut to disclose any security breach involving unencrypted personal information to state residents and the state attorney general "without unreasonable delay."

A company's compliance with its own state's data privacy laws will not excuse it from complying with the laws of other states in which it does business. Thus, it is advisable for companies to establish policies and safeguards complying with the most stringent applicable data privacy laws, which in many cases—particularly for businesses operating in the Northeast—will be the Massachusetts data privacy laws. There are also a host of other industry-specific data privacy laws with which many U.S. businesses must comply, including HIPAA, the Gramm–Leach–Bliley Act, the federal Red Flags Rule, the Payment Card Industry Data Security Standard and the European Union Data Privacy Directive.

Recent data security breaches

Data security breach incidents are now making the news headlines on nearly a daily basis, and there is a growing trend of active enforcement by governmental authorities.

- In May 2012, a Massachusetts hospital agreed to pay $750,000 to settle a Massachusetts attorney general enforcement action based on a data breach involving the compromise of over 800,000 consumers' protected health information.

- In June 2012, a LinkedIn security breach involving the theft of more than six million customer passwords was reported. The breach resulted in the filing of a class-action lawsuit in the U.S. District Court for the Northern District of California seeking over $5 million in damages.

- In March 2011, a major Boston restaurant group agreed to a $110,000 settlement in connection with a Massachusetts attorney general enforcement action relating to a breach that put tens of thousands of customers' personal information at risk.

- In June 2012, the FTC filed a complaint against a large hotel chain in the U.S. District Court for the District of Arizona, charging that it repeatedly failed to safeguard consumers' personal information, which resulted in the compromise of several hundred thousand consumers' payment card data and $10.6 million in fraud loss.

- In June 2012, a subscription-based provider of geopolitical analysis agreed to settle a class-action lawsuit filed in the U.S. District Court for the Eastern District of New York, which was based on a hacking breach that resulted in thousands of customer credit cards and hundreds of thousands of subscriber e-mail addresses being published, for an estimated $1.75 million, based on the terms of the proposed settlement.

- In June 2012, the U.S. Department of Health and Human Services reported that the Alaska Department of Health and Social Services, the state's Medicaid agency, agreed to settle potential violations of the HIPAA Security Rule governing protection of electronic health information for $1.7 million.

While large companies, particularly those in the healthcare, financial services and retail industries, hold significant amounts of personal information that must be safeguarded, smaller businesses are not immune from data security breaches. A recent article from *The Wall Street Journal* reported that the majority of worldwide data breaches last year involved companies with 100 or fewer employees and explained that smaller businesses, due to their limited resources and budgets, are particularly vulnerable to cyber theft.

Enforcement of data privacy law violations is likely to increase in the future. In fact, the National Association of Attorneys General, comprised of the attorneys general of every U.S. state as well as the District of Columbia and several U.S. territories, recently announced a new initiative entitled "Privacy in the Digital Age," which will explore ways to protect online privacy and manage the risks associated with data breaches and emerging technologies. In light of these trends and developments, it is clear that compliance with applicable data privacy laws is not only good business but also an essential obligation of every company today.

David M. Governo *is the founding partner of Governo Law Firm LLC, an 18-attorney law firm in Boston, MA. For over three decades, he has advised companies on a range of risk*

management and compliance issues, and defended companies in complex litigation. He has attained Martindale-Hubbell's highest "AV" rating, is an active member of the Federation of Defense and Corporate Counsel, and has been voted a New England Super Lawyer for many years.

***Corey M. Dennis**, CIPP/US, defends companies in complex litigation, and advises companies on risk management and compliance issues at Governo Law Firm LLC. He has counseled businesses on compliance with data privacy laws, is a Certified Information Privacy Professional (CIPP/US) and has published numerous legal articles in the areas of data privacy, civil litigation, social media, toxic tort, and employment law.*

A fully annotated version of this report was first published in the LexisNexis® In-House Advisory.

Read more by David Governo and Corey Dennis:
FTC ramping up data privacy enforcement actions; Google fined $22.5 million