A Guide to Data Privacy Compliance

**This article is for general information purposes only and does not constitute Eze Castle Integration operations or technology advice as to any particular set of facts.*

About Eze Castle Integration

Eze Castle Integration is the leading provider of IT solutions and private cloud services to more than 600 alternative investment firms worldwide, including more than 80 firms with $1 billion or more in assets under management. The company's products and services include Private Cloud Services, Technology Consulting, Outsourced IT Support, Project & Technology Management, Professional Services, Telecommunications, Business Continuity Planning and Disaster Recovery, Archiving, Storage, Colocation and Internet Service. Eze Castle Integration is headquartered in Boston and has offices in Chicago, Dallas, Geneva, Hong Kong, London, Los Angeles, Minneapolis, New York, San Francisco, Singapore and Stamford.

263,247,891.

It is the number of records involved in security breaches in the United States since January 2005, according to the Privacy Rights Organization. In reality, PRO states the number should be much larger; however, in many cases the number of records exposed is unknown.

Illuminating the risk of breaches, in 2007, TJX announced that up to 40 million credit and debit card numbers had been stolen, resulting in a $40.9 million settlement. In 2005, Bank of America lost the financial information for over one million government employees. This July, HSBC (UK) was fined $5.2 million for losing customer data in the mail – the largest penalty ever handed down by the UK's Financial Services Authority.

These and dozens of other noteworthy security breaches have prompted many states to enhance their data security protection laws, or in most cases, develop these laws for the first time. The law with the most force is from Massachusetts and, if passed, will be the strictest privacy law on the books. This article will examine the key facets of the Massachusetts regulation – 201 CMR 17 – and outline the requirements for compliance.

The Basics

Massachusetts is currently attempting to pass the most stringent data privacy law at either the state or federal level. Originally slated to take effect on May 1, 2009, the regulation was originally pushed to January 1, 2010 and then subsequently pushed to March 1, 2010 in order to give businesses time to comply. But which businesses are affected? According to the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR), any business that "receives, maintains or otherwise has access to personal information" of Massachusetts residents "in connection with the provision of goods and services or in connection with employment" must comply with the regulation.

In other words, it is not merely businesses that reside or operate in Massachusetts who need to comply. The geography does not apply to the business, but to the owner of the personal information that business stores. For example, an investment firm might operate out of California, but if even one investor resides in Massachusetts, that business must comply.

Now that we have identified the who, let's identify the what. The words "personal information" might mean a number of different things to different people. According to the OCABR, personal information is the combination of a person's first and last name with the following:

- A social security number, taxpayer identification number, or employee identification number
- Driver's license number or other state-issued identification card
- Financial account number of credit/debit card number
- An access code that would allow one to access that person's financial information

So what requirements does the law – 201 CMR 17 – specify? Let's take a look at the breakdown.

The Law

Several states currently have data privacy laws on the books, including Nevada, Connecticut, Texas and Michigan. It appears as though the Massachusetts regulation will far surpass the laws of these states in terms of its scope and severity.

MA 201 CMR 17 has six unique requirements. Each is designed to provide the highest level of security to Massachusetts residents in an effort to keep their sensitive, personal information protected and minimize the risk of a security breach.

Identify Risks

The law will require all Massachusetts businesses to identify and assess internal and external risks to employees' personal information as well as take steps to improve safeguards and minimize said risks.

Inventory Location of PI

Businesses will be tasked with identifying the specific locations where personal information is stored, including electronic, paper and other records, as well as on laptops and mobile devices.

Limit Collection of Data

This requirement includes limiting the amount of information that is available to employers, as well as the time that information is retained and the specific persons to whom it is accessible.

Routinely Evaluate and Adjust Program

Businesses should regularly monitor their security programs to ensure they are properly protecting information. Additionally, companies should review the scope of their security measures at least annually and update measures to reflect any changes in the business.

Encrypt Hardware and Data Transmissions

Businesses must encrypt all files and records containing personal information that are transmitted over public networks "to the extent technically feasible." In addition to transmitted information, the regulation also requires the encryption of information stored on laptops, flash or USB drives and wireless mobile devices.

Oversee and Obtain Written Guarantees of Adherence form Third-Parties

Companies with Massachusetts residents are also responsible for ensuring that any third-party service providers with whom they work are also in compliance with 201 CMR 17.

Developing a Written Information Security Policy

As part of the regulation, Massachusetts businesses will be required to develop a comprehensive written information security policy (WISP). This document will contain the written statements and specific information related to the protection of employees' personal information.

As part of the WISP, firms will need to:

- **Identify** where all personal information resides within the organization, including within reports, Microsoft Excel files, CRM systems, etc. Firms must also complete an assessment of internal and external risks.

- **Develop** the written document to protect all personal information. Include corporate policies and procedures as it relates to the protection of PI, including roles and responsibilities for managers and penalties for violations. **Implement** the policy, encrypting records "to the extent technically feasible." **Maintain and monitor** the policy, so as best to protect employee personal information and mitigate security risks.

- **Train and monitor** employee compliance and access to data, reviewing the scope of the security program at least annually. Ensure change control measures are in place and any changes of roles and responsibilities within the organization are captured and reflected in the security policy.

- **Ensure** third-party service providers (HR systems, CRM systems, etc.) satisfy all requirements of 201 CMR 17 and develop an action plan to work with these third-parties in the event of a security breach. Document actions that will need to be taken to resolve security breaches.

Computer System Security Requirements

In addition to the WISP, businesses will need to comply with certain technical requirements. For example, all user authentication protocols must be secured. In order to mitigate the chances of an internal breach, businesses must execute best practices such as controlling user IDs and passwords, restricting data access to authorized active users, blocking access after multiple unsuccessful attempts, and changing passwords frequently. In order to mitigate the chances of an internal breach, businesses must execute best practices such as controlling user IDs and passwords, restricting data access to authorized active users, blocking access after multiple unsuccessful attempts, and changing passwords frequently.

Businesses can secure access control measures by restricting records access to only “need-to-know employees” and assigning unique user IDs and passwords to each employee with computer access. Technical safeguards include mandatory encryption of all transmitted records with PI, “reasonably up-to-date” firewall protections, security patches, security software and updated anti-virus and anti-intrusion software.

After technical safeguards have been implemented and confirmed, it is essential that businesses monitor their networks and systems with careful eyes for unauthorized use. Employees should be trained on proper use of computer system security and record auditing processes.

Final Considerations

Massachusetts will not likely be the last state to implement such rigorous security protection measures. In fact, it may even act as a model for future federal data security regulations. Violators of 201 CMR 17 will face stiff monetary penalties – as much as $5,000 per violation – as well as the less calculable effects surrounding a business' reputation. It appears that the Massachusetts regulation will be the standard for data protection in the U.S. and is likely to change the way businesses operate. Even businesses outside of the state and without Massachusetts employees should take notice and be prepared to comply to similar regulations in the future. Careful analysis and strict compliance by all parties will ultimately create the safest environment for employee's personal information and help businesses avoid massive security breaches in the future.

**This article is for general information purposes only and does not constitute Eze Castle Integration operations or trading advice as to any particular set of facts.*