RUBERTO, ISRAEL & WEINER

Client Alert

NEW MASSACHUSETTS RULES REQUIRE INFORMATION SECURITY PLANS AND PROCEDURES.

Requirements are Effective Shortly

If your business has, in electronic or paper form, any personal information about any Massachusetts residents, you are required to draft, implement, and update a comprehensive written information security plan. You are also required to implement specified computer system security protections. Failure to do so will place your business out of compliance with state law. These regulations are among the most far reaching in the country. The official title of the regulations is "201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth." There are relatively short deadlines for compliance. Many of the requirements become effective on Friday, May 1, 2009.

Broad Coverage

The new regulations have a broad coverage – they extend to any company or individual that "owns, licenses, stores or maintains personal information." There is no exception for small businesses.

"Personal information" in the regulations means:

a Massachusetts resident's first and last name, or first initial and last name, *together with* his or her Social Security number, driver's license or state-issued ID number, bank or other financial account number, or credit or debit card number. Personal information may also include PIN numbers, passwords, or biometric information.

Personal Information Protection Obligation

The rules require covered companies to draft and implement a "comprehensive, written information security program." The program must include the following:

- Designate one or more employees to be in charge of information security.
- Assess the risk to the security, confidentiality, and/or integrity of electronic, paper or other records and the effectiveness of current risk mitigation procedures.
- Create security policies for employees that cover access and use of information.
- Impose disciplinary sanctions for employees who violate the program requirements.
- Reliably terminate access to records by former employees.
- If your business uses outside vendors that hold personal information, verify that service providers are capable of protecting personal information and are contractually obligated do so.

RUBERTO, ISRAEL & WEINER

Personal Information Protection Obligation Cont...

- Limit the amount of personal information that your business collects to that necessary to accomplish the purpose for which the data is obtained. Also limit the time the information is held to that reasonable necessary for its purpose.

- Identify systems and storage media, including devices and portable computers, that contain personal information.

- Secure records on physical media by locked storage and restrict access to personal information under written procedures.

- Monitor security procedures regularly and, as appropriate, upgrade them.

- Review the security procedures and measures for personal information at least once per year – or more frequently as necessary. Cure deficiencies revealed in the review.

- Document security breaches and measures taken in response.

Computer System Security Requirements

The new regulations also impose computer system security requirements on any business that owns, licenses, stores or maintains personal information about a Massachusetts resident. The requirements include the following:

- Authentication requirements, including:
  - ◊ Secure user authentication protocols, including passwords or other identification technologies, such as biometrics or tokens.
  - ◊ Data security passwords controls.
  - ◊ Access restrictions to insure use by active users and active user accounts only.
  - ◊ Access shut downs that block access to user identification after multiple unsuccessful attempts to gain access.
- Access control measures, including:
  - ◊ Restricting access to records on a need-to-know basis
  - ◊ Assigning unique (and non-vendor supplied) passwords to authorized personnel.
- Encryption of records that pass through public networks using no less than 128 bit encryption.

- Encrypted storage of personal information on portable devices and laptops.

- Use of firewall and keeping operation systems up-to-date with security patches.

- Use of malware and virus scanning software that regularly update virus definitions and security patches.

- Training for employees on the proper use of the computer security system and the importance of personal information security.

RUBERTO, ISRAEL & WEINER

Compliance is Important

All business should bring data policies and security systems into compliance with these regulations as soon as possible. Here is why:

- In case of non-compliance, the Massachusetts Attorney General can sue to terminate violations.
- Stakeholders, such as customer and employees, expect robust data security – and these regulations reinforce that expectation. Breach of security can harm your business.
- If your company is party to contracts that require your company to hold data and to "comply with applicable law," failure to comply with the regulations may constitute a breach of contract on your company's part.

In some cases, failure to comply with the regulations may be deemed evidence of negligence.

Compliance Deadlines

The original deadline for compliance was January 1, 2009, but due to many complaints about the short time for businesses to implement such comprehensive requirements, Massachusetts has set new deadlines:

Friday, May 1, 2009

- The compliance deadline for the regulation as a whole.
- The requirement that businesses ensure that their third-party service providers protect personal information and contractually bind them to do so.
- The deadline for ensuring encryption of laptops

Friday, January 1, 2010

- The requirement that businesses require that their third-party providers provide written certification of information security compliance.
- The deadline for ensuring encryption of other portable devices (such as smart phones, Blackberries, and memory devices.

Even with these changes, businesses that hold or manage personal data have a relatively short time to bring their data security plans and data systems into compliance.

Getting Assistance

If you need more information about these regulations, please let us know. Our law firm can help you create and assess the adequacy of your written plans, policies and procedures.

For more information, please contact Gene Landy at (617) 742-4200 or gkl@riw.com

100 N. Washington Street, Boston, MA 02114 • P (617) 742-4200 • F (617) 742-2355 • www.riw.com