Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Advisories

April Showers Bring May Flowers & Identity Theft Compliance Deadlines

02.19.09

By Charlene A. Brownlee and Ronald G. London

Finding it difficult to keep up with the growing body of federal and state privacy regulations? You are not alone. In fact, the deadline for compliance with the Massachusetts Standards for the Protection of Personal Information (the Regulations)[1] have been extended twice, recognizing organizations require more time to develop comprehensive identity theft prevention programs. The new compliance date, announced Feb. 12 by the Massachusetts Office of Consumer Affairs and Business Regulation, is Jan. 1, 2010.

If your business is subject to the Federal Trade Commission's (FTC) Red Flag Rules, your identity theft prevention program must be in place by May 1, 2009. As you finalize your Red Flag Program, keep in mind the requirements of the Massachusetts Regulations, which are more onerous than the requirements of the Red Flag Rules in certain regards. For example, the Regulations impose more specific data security requirements such as the encryption of laptops and portable media.

Let us know if you have any questions or would like us to assist you in creating or administering such a program.

Red Flag Rules

Is your organization a "creditor"[2] that maintains "covered accounts"[3]? The Red Flag Rules specifically refer to banks, finance companies, automobile dealers and mortgage brokers, as well as utility companies and telecommunications companies.

The Red Flag Rules require organizations to develop and implement an identity theft prevention program. There are four basic steps to designing such a program: (1) identifying relevant red flags; (2) detecting red flags; (3) preventing and mitigating identity theft; and (4) updating the program periodically.

Additional information about the applicability and requirements of the Red Flag Rules may be found in previous advisory bulletins issued by Davis Wright Tremaine LLP:

FTC Delays Enforcement of Red Flag Rules to May 1, 2009, by Rebecca L. Williams and Brent R. Eller, Oct. 2008

'Red Flag' Identity Theft Programs, by John D. Sevier and Ronald G. London, July 2008

Massachusetts Regulations

Your organization must comply with the Regulations if it owns, licenses, stores or maintains personal information[4] about a resident of Massachusetts. The Regulations require the establishment of a comprehensive information security program to safeguard personal information contained in both paper and electronic records, as described below.

Comprehensive information security program

The Regulations require the development and implementation of a comprehensive, written information security

RELATED PEOPLE

Randy Gainer

Ronald G. London

John D. Seiver

RELATED PRACTICES

Privacy & Security

program applicable to any records containing personal information of Massachusetts residents. The information security program must be consistent with industry standards, and contain administrative, technical and physical safeguards to ensure the security and confidentiality of personal information.

The Regulations do not adopt a “one size fits all” approach. Rather, much like the flexibility inherent in the Red Flag Rules, an organization's program can be tailored taking into account (i) the size, scope and type of business, (ii) the amount of resources available to the organization, (iii) the amount of stored data, and (iv) the need for security and confidentiality of both consumer and employee information.

The Regulations require every information security program to include the following components:

a. **Employee designate.** Designating one or more employees to maintain the program.

b. **Risk assessment.** Identifying internal and external risks to the security, confidentiality and/or integrity of any records (electronic and paper) containing personal information. Evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including: (i) ongoing employee training; (ii) employee compliance with policies and procedures; and (iii) means for detecting and preventing security system failures.

c. **Security policies.** Developing security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises.

d. **Disciplinary measures.** Imposing disciplinary measures for violations of the information security program rules.

e. **Terminated employees.** Preventing terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names.

f. **Verification of service providers.** Taking reasonable steps to verify that all third-party service providers with access to personal information have the capacity to protect such personal information. The organization should include data protection terms in its written agreement with such service providers.

g. **Limiting collection, retention and access.** Limiting the amount of personal information collected to that reasonably necessary to accomplish the purpose for which it is collected; limiting retention of such information to that reasonably necessary to accomplish such purpose; and limiting access to those persons who are reasonably required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements.

h. **Physical security.** Written procedures setting forth reasonable restrictions upon physical access to records containing personal information.

i. **Computer system security.** The establishment and maintenance of a security system covering the organization's computers, including any wireless system, that includes, at a minimum, the following elements:

    Secure user authentication protocols including: control of user IDs and other identifiers; a reasonably secure method of assigning and selecting passwords; control of data security passwords; restricting access to active users and active user accounts only; and blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.

    Secure access control measures that restrict access to records containing personal information to those who need such information to perform their job duties; and assign unique identifications and passwords.

To the extent technically feasible, encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data to be transmitted wirelessly.

Reasonable monitoring of systems, for unauthorized use of or access to personal information.

Encryption of all personal information stored on laptops or other portable devices.

Up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.

Current versions of system security agent software which must include malware protection and patches and virus definitions.

Education and training of employees on the proper use of the computer security system and the importance of personal information security.

j. **Annual review.** Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may impact the security or integrity of records containing personal information.

k. **Documenting security breaches.** Documenting actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in the organization's business practices relating to protection of personal information.

The Regulations, a compliance check list, and FAQs are available here.

FOOTNOTES

1 201 Mass. Code Regs. 17.00-.05

2 "Creditor" includes: Any person or entity that regularly, extends, renews, arranges or continues credit; any assignee or an original creditor who participates in the decision to extend credit; and essentially anyone that bills after providing service or allows customers to defer payment.

3 "Covered account" includes: an account maintained primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions; and any other account, including a business account, that poses "a reasonably foreseeable risk to customers or the safety and soundness of the . . . creditor from identity theft, including financial, operational, compliance, reputation or litigation risks."

4 "Personal information" is defined as a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.