

November 30, 2009

Murtha Cullina is pleased to provide clients and friends with information about topics of interest on identity theft regulations

If you have any questions about the issues addressed here, or any other matters, please feel free to contact the following attorneys:

Robert J. Munnely, Jr.
617.457.4062
rmunnely@murthallaw.com

Lissa J. Paris
860.240.6032
lparis@murthallaw.com

IDENTITY THEFT REGULATIONS: RECENT DEVELOPMENTS

Identity theft has cost consumers and businesses billions of dollars in recent years. These losses have triggered legislative and regulatory responses including:

1. Expansive federal requirements imposed on industries potentially vulnerable to identity theft under the Federal Trade Commission's "Red Flag" rules (16 CFR § 681.2);
2. Obligations on all employers of Massachusetts residents under new Information Security regulations (201 CMR 17.00), which implement Security Breach/Record Destruction statutes (Mass. G.L. c. 93H and 93I); and
3. Recently-enacted Connecticut limits on use of Social Security number and employment application information (Conn. Gen. Stat. §§ 42-470 to 472).

This bulletin highlights these developments and the steps businesses can take now to ensure compliance, especially when compliance dates are approaching for businesses subject to Red Flag and Massachusetts rules.

Federal Red Flag Rules

The Red Flag rules classify financial institutions and certain non-financial businesses which have ongoing and regular customer interactions as "creditors" under federal information protection laws and, as such, obligate them to implement a written, annually updated, information security program. Non-financial industries subject to the Red Flag rules include most cable television, telecommunications, energy and water providers, auto dealers, and health care providers, so long as services provided are not entirely pre-paid. While the level of federal compliance review and associated penalties are not yet precisely clear, noncomplying businesses are likely to face stiff sanctions and may face private litigation or class action suits.

Companies subject to the Red Flag rules must develop a written information security plan that identifies all personal information collected or maintained by the company (defined as a

person's name plus data elements such as social security number, driver's license or identification card number or credit/debit card and bank account information), review policies and practices against a lengthy list of "red flags" that signal possible opportunities for identity theft, have the final plan that reasonably addresses red flags approved by their Board or a subcommittee and establish a process for regular review of the written plan at least once per year. The Red Flag rules are now scheduled to become effective on June 1, 2010.

Massachusetts Information Security Rules and Statutes

In 2007, the Massachusetts legislature enacted General Laws chapters 93H and 93I to address identity theft security breach procedures and destruction practices for paper and electronic records containing personal information. Regulations that apply to all businesses employing Massachusetts residents have been issued, and we expect revised regulations to be issued by year's end. Again, while the scope of enforcement efforts remains unclear, Massachusetts statutory and regulatory requirements subject non-complying businesses at minimum to actions brought by the Attorney General under Chapter 93A (the unfair and deceptive trade practices statute) and may subject them to private or class action litigation.

The Massachusetts rules require each business to develop a written information security plan that is approved by the Board of Directors or designated committee with detailed compliance requirements, undertake an annual review/update process (similar to the Red Flag rules) and, in addition include numerous new computer security requirements. In particular, the rules require use of encryption with respect to all personal information that is taken out of the office on a laptop computer or is sent across public networks in electronic form. Employers must implement these procedures by March 1, 2010.

Connecticut Personal and Applicant Information Statutes

Connecticut has already required most companies to comply with narrower, but still robust, identity theft protection requirements.

First, in 2008, the Connecticut legislature passed the "Social Security Law" (or "SSN Law") that applies to all people and businesses (other than agencies or political subdivisions of the State) in possession of the "personal information" of another. The act was later codified into Conn. Gen. Stat. §§ 42-470 to 472. The SSN Law requires a person in possession of such personal information to:

- Safeguard the personal information from misuse by third parties; and
- Properly destroy the information prior to disposal.

It also requires that a person who collects Social Security numbers (as distinguished from other forms of personal information) in the course of business to create a written and displayed “privacy protection policy” that:

1. Protects the confidentiality of such Social Security numbers;
2. Prohibits unlawful disclosure of such Social Security numbers; and
3. Limits access to such Social Security numbers.

Each violation of the SSN Law is punishable by substantial civil penalties and may be used to support statutory or common law causes of action.

Second, in 2009, the legislature enacted the Safeguarding Employee Data Provision (“Safeguarding Act”) which amends and expands on the protections enacted in the SSN Act. Under the Safeguarding Act, employers (a term that is defined to exclude agencies and political subdivisions of the State) must securely maintain employment applications and take reasonable measures to destroy or make unreadable employment applications upon disposal. Disposal must “at a minimum, include the shredding or other means of permanent destruction of such employment applications in a secure setting.” Like its predecessor statute, the violators of the Safeguarding Act are subject to substantial penalties.

Conclusion

These acts and regulations require employers in Massachusetts, Connecticut and elsewhere to review their human resources practices and document handling, storage and disposal policies. Noncompliance might lead to serious penalties or private lawsuits. Massachusetts employers and those subject to the federal rules should make sure their workplace complies with requirements before the new requirements take effect. Connecticut employers should already be in compliance.

If you have any questions about the issues addressed here, please contact: Robert J. Munnely, Jr. at 617.457.4062 or rmunnely@murthalaw.com, Lissa J. Paris at 860.240.6032 or lparis@murthalaw.com or any of our individual attorneys in practice areas potentially affected by these new requirements.