Client Advisory

KELLEY DRYE

PRIVACY AND INFORMATION SECURITY PRACTICE NOVEMBER 4, 2008

# Massachusetts Releases Business Guidance on Compliance with the State's New Data Security Regulation

***In preparation for the January 1, 2009 implementation date, the Massachusetts Office of Consumer Affairs and Business Regulation (the "Office") recently published guidance on how companies can formulate the comprehensive written information security program required by its recently issued data security regulation (the "Regulation").[1] In addition, the Office has released a compliance checklist and a list of Frequently Asked Questions regarding the regulation. All three materials can serve as useful tools for businesses as they evaluate and update their current security policies to ensure compliance with the new Regulation.***

## APPLICABILITY

The Regulation requires that any person that owns, licenses, stores, or maintains certain sensitive "personal information" about a Massachusetts resident to develop, implement, maintain, and monitor a comprehensive, written information security program applicable to records containing such personal information. Thus, if a business outside of Massachusetts collects Massachusetts residents' personal information (whether customer, employee, or other personal data), under the terms of the Regulation, the business would be subject to its requirements. It remains to be seen whether the Massachusetts Attorney General or private litigants will attempt to enforce the Regulation against businesses with no operations in Massachusetts, but if they do (and succeed), businesses could be subject to civil penalties, as detailed below.

## GUIDE FOR FORMULATING A COMPLIANT INFORMATION SECURITY PROGRAM

On October 24, 2008, the Office released a *"Small Business Guide for Formulating a Comprehensive Written Information Security Program"* (the "Guide"). While intended to assist small businesses in their compliance efforts, the Guide can provide useful advice for businesses of all sizes. The Guide sets forth a template comprehensive written information plan (the "Massachusetts Plan" or "the Plan"), which businesses may use to adapt to the particular circumstances of their business, and which sets forth a recommended procedure for evaluating a business's "electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information of the residents of the Commonwealth of Massachusetts."

Similar to recommendations that the Federal Trade Commission has issued,[2] the Massachusetts Plan outlines methods businesses can apply to help secure personal information against anticipated threats, as well as against unauthorized access to or use of such information that creates a substantial risk of identity theft or fraud.

---

[1] Mass. Regs. Code tit. 201, § 17.00 (2008). Kelley Drye's previous client advisory on the Regulation is available at http://www.kelleydrye.com/resource_center/client_advisories/0373.

[2] The FTC's business guidance on developing an information security program is available at http://www.ftc.gov/bcp/conline/edcams/infosecurity/.

These include the following action items:

1) Identify risks to the security and confidentiality of the personal information it maintains;

2) Identify the likelihood and potential damage of these threats;

3) Evaluate existing security procedures in place to control risks;

4) Develop new safeguards to further minimize risks;

5) Regularly monitor effectiveness; and

6) Designate a Data Security Coordinator who will be responsible for implementing and maintaining the information security program and the business's security policies and procedures.

To help minimize ***internal*** threats to personal information, the Plan should ensure that a business:

- Provides all employees with a copy of the Plan;
- Obtains written acknowledgement from employees that they have received a copy of the Plan;
- Amends employee contracts to comply with the Plan;
- Limits the amount of personal information collected;
- Limits access to records;
- Annually reviews all security policies and procedures;
- Has in place specific secure user authentication protocols;
- Conducts a post-incident review after a security breach;
- Requires each department to develop rules that ensure reasonable restrictions on access to personal information are in place;
- Restricts visitor access to one entry point for each building; and
- Disposes of personal information in compliance with Massachusetts record disposal law.

To minimize ***external*** threats to the security and confidentiality of records containing personal information, the Plan should ensure that a business:

- Encrypts all personal information stored on laptops or other portable devices, and encrypts all records and files transmitted across public networks or wirelessly;
- Installs reasonably up-to-date firewall protection and operating system security patches on all systems processing personal information;
- Installs reasonably up-to-date versions of system security agent software, which must include malware protection and reasonably up-to-date patches and virus definitions on all systems processing personal information;
- Monitors all computer systems for unauthorized use; and
- Has in place specific secure user authentication protocols.

## COMPLIANCE CHECKLIST

In addition to the Guide, the Office has compiled a checklist to help businesses ensure that their written comprehensive information security programs comply with the Regulation. The checklist is available at: http://www.mass.gov/Eoca/docs/idtheft/compliance_checklist.pdf. Each point on the checklist highlights a required feature set forth in the Regulation.

For example, the checklist covers whether the information security program contains appropriate safeguards for the protection of personal information; identifies the various types of personal information stored; identifies both internal and external risks to the security system; limits the amount of personal information stored and access to that personal information; and ensures that there is a method to ensure that third party contractors comply with the Regulation.

Additionally, the checklist calls attention to the additional requirements for electronic records, such as the

encryption of personal information stored on mobile devices; the encryption, to the extent technically feasible, of personal information transmitted wirelessly and transmitted across public networks; and up-to-date firewall protection and system security software; and specific secure authentication protocols.

## FREQUENTLY ASKED QUESTIONS

The Office also has identified Frequently Asked Questions ("FAQs") regarding the Regulation. The FAQs are available at: http://www.mass.gov/?pageID=ocaterminal&L=3&L0=Home&L1=Business&L2=Identity+Theft&sid=Eoca&b=terminalcontent&f=idtheft_201cmr17faq&csid=Eoca. These FAQs reiterate the Regulation's provisions that require that the information security program be in writing; that it is the duty of the business to ensure that any independent contractors it employs certify in writing that they are in compliance with the Regulation; and that the business is able to identify which records contain personal information.

The Office explains that compliance ultimately will depend on the size and nature of the business, as well as on the availability of an internal IT department, whether or not the business will need to hire an IT consultant, buy new computer equipment or new software, or limit the amount of personal information collected to be in compliance. Additionally, the business will have to determine how much employee training and security program monitoring are necessary, as well as, to whom the business will grant access to personal information in order to comply with the Regulation. Finally, the Office explains that both the statute and the Regulation require that compliance will be assessed taking into account the size and scope of the business, the resources available to the business, the amount of data the business stores, and the need for confidentiality.

## PENALTIES AND CIVIL REMEDIES

Violations of the Regulation are subject to enforcement under the Massachusetts Unfair Competition Statute.[3] The Massachusetts Attorney General may seek a temporary restraining order or a preliminary or permanent injunction against a business that it believes is in violation of the Regulation. If found to be in violation of the law, a court may require that the business pay a civil penalty of up to $5,000 per violation, as well as the costs of the investigation and attorneys' fees.

In addition, businesses also face the potential of a private action for noncompliance of the Regulation. Massachusetts residents can potentially bring a claim for unfair or deceptive practices under Chapter 93A of the Massachusetts Laws, or a negligence claim using the Regulation (or the statute under which it was issued) to prove that the business had a duty that was breached. Under Massachusetts law, a violation of the statute may constitute per se negligence. If such a case is successfully brought, the exposure is the amount of actual damages or twenty-five dollars, whichever is greater. Additionally, if the court finds that the practice was a willful or knowing violation, the court may order treble damages.

## CONCLUSION

The Massachusetts Guide, checklist, and FAQs indicate that the Office does *not* intend to extend the January 1, 2009 deadline for compliance. These three materials, however, can provide guidance to businesses on how to evaluate current business security policies and structure a comprehensive written information security policy that will be deemed compliant with the new Massachusetts data security law and corresponding Regulation. While the looming deadline of the Massachusetts Regulation may be the impetus for action now by businesses, the same or similar requirements are likely to be issued in other states as part of a trend on growing concern over information security

[3] Mass. Gen. Laws, ch. 93A.

practices and prevention of identity theft. Thus, efforts taken now will help position businesses for the national (and global) legal landscape going forward.

## KELLEY DRYE & WARREN

Kelley Drye & Warren's Privacy and Information Security Practice is a leader in advising clients on privacy and information security issues and has been at the forefront of developments in this growing area of the law. Our attorneys regularly counsel clients regarding all aspects of privacy and data security compliance, including drafting and amending privacy and information security policies, advising clients on interpreting their own policies, crafting data security programs for clients, performing privacy and/or data security audits of existing business practices, drafting agreements with third parties regarding their obligations in connection with handling clients' customer data, and representing clients in connection with federal and state regulator privacy investigations regarding their privacy and data security practices.

### For more information about this Client Advisory, please contact:

**ALYSA Z. HUTNIK**
**202-342-8603**
**ahutnik@kelleydrye.com**

**D. REED FREEMAN**
**202-342-8880**
**rfreeman@kelleydrye.com**