DAVIS MALM & D'AGOSTINE P.C.

ATTORNEYS AT LAW

REGULATORY AND ADMINISTRATIVE LAW ALERT
JUNE 2015

CONNECTICUT EXPANDS DATA PROTECTION RULES

In early June 2015, Governor Malloy signed legislation making wide ranging changes to state laws that protect personal information of Connecticut residents (the Act). Key data security expansions and their impacts inside and outside of Connecticut include the following:

KEY CHANGES

1. **Shorter Reporting Time Frames and Minimum Consumer Remedies Are Now Required for All Computer Data Breaches.**

   Section 6 of the Act amends Connecticut data security laws to shorten the time period for mandatory notice to state agencies in the event of breach to 90 days following breach discovery (unless a shorter time is required by other law). Even more significantly, for breaches involving loss or hacking of computerized data, the breaching company must offer identity theft prevention and mitigation services for at least one full year. This represents a substantial increase from the three month minimum previously recommended by the Attorney General for offering credit monitoring, credit freeze and similar services.

2. **Expanded Data Protection Requirements for All Health Insurance Companies Required on or before October 1, 2017.**

   Section 5 also imposes significant obligations on health insurance companies, effective as of October 2017. Requirements will include:

   - Development of a written information security program (WISP), with designation of a responsible person for implementation and maintenance of the security program;
   - Computer and Internet user authentication protocols;
   - Access control measures;
   - Mandatory encryption of personal information transmitted over a public Internet network or wirelessly;
   - Laptop encryption;
   - Procedures for off-premises transport of information;
   - Implementation of disciplinary measures for security violations;
   - Post-termination employee security measures;

- Physical security measures;
- Robust security and anti-virus protections;
- Security training;
- WISP updates on at least an annual basis; and
- Mandatory post-incident review of actual or suspected breaches, with documentation of response measures.

Companies subject to these requirements also must annually certify compliance to the State Insurance Department under penalty of perjury and be required to provide the WISP to the Insurance Commissioner or Attorney General upon request.

3. **State Contractors Receiving Personal Information Also Must Implement Rigorous Data Security Programs.**

   Sections 1 and 2 of the Act require vendors receiving confidential information pursuant to state contracts to implement and maintain a "comprehensive" data security program that:

   - Covers data storage and transportation, access restrictions, annual review of policies and security measures, and mandatory employee awareness training;
   - Limits access to "authorized" agents of the contractor;
   - Requires retention of confidential information on secure drives and servers and behind firewalls protected by intrusion protection software;
   - Improves breach investigation procedures and notice obligations in the event of breach;
   - Imposes safeguards on storage and transportation of data; and
   - Imposes new remedies in the event of a breach, including the potential for a ban on the vendor issued by the State Department of Education.

4. **State Must Develop New Program to Coordinate Responses to Data Requests Across State Agencies and Protect State Agency Information.**

   Section 4 of the Act empowers the State Office of Policy and Management to develop a program that improves consumer access to data maintained by executive agencies and, in so doing, ensure the security, privacy and confidentiality of such information, including developing with the State Chief Information Officer a detailed "data security and safeguarding plan" for all data accessed or shared through the new access program.

5. **Smartphones Must Be Capable of Remote Wiping As of July 2016.**

   Section 7 of the Act prohibits retail sales of smartphones in Connecticut effective July 1, 2016 unless they contain hardware or capability to receive downloadable software upon activation that can render the phone inoperable to an unauthorized user.

IMPACTS ON BUSINESSES INSIDE AND OUTSIDE OF CONNECTICUT

Businesses inside and outside of Connecticut should consider the potential impacts of the Act in at least two principal respects.

First, all business, wherever located, should review their WISPs and related data security policies to see whether they are affected by the Connecticut-specific provisions in the Act. At minimum, (1) business with Connecticut offices, (2) non-Connecticut businesses with Connecticut resident employees or customers, and (3) especially health insurance companies and all companies seeking to do business as vendors with Connecticut state agencies should review existing policies and WISPs to determine whether changes are needed to reflect the new law. Wireless phone makers and retail outlets should pay particular attention to the July 2016 requirement of remote wiping capability for all smartphones.

Second, all businesses should consider the Act to be a potential "canary in a coal mine" sign of increasing state law level regulation of data security. Massachusetts lead this trend five years ago with implementation of its rules that require implementation of a WISP for all holders of personal information of Massachusetts residents, wherever the holder is located, and Nevada has followed by requiring tough new data encryption rules. The Act may serve as a third example that may well be followed by implementation of other state regimes in upcoming months and years. Businesses that have not implemented a WISP should consider getting ahead of this emerging trend and doing so as soon as possible.

CONTACT

If you have any questions about this alert, please contact the author, Robert J. Munnelly, Jr. , or a member of our Regulatory and Administrative Law Practice.

One Boston Place, Boston, Massachusetts 02108 | phone 617.367.2500 | fax 617.523.6215 | info@davismalm.com.