DAVIS MALM & D'AGOSTINE P.C.

ATTORNEYS AT LAW

REGULATORY AND ADMINISTRATIVE LAW ALERT
OCTOBER 2015

RHODE ISLAND EXPANDS DATA PROTECTION RULES

In June 2015, the Rhode Island General Assembly repealed its outdated ten year old Identity Theft Protection statute and enacted the Identity Theft Protection of 2015 law (the Act). The Act was signed by Governor Raimondo on June 26, 2015 and makes wide ranging modifications to state laws protecting "personal information" (i.e., names plus confidential numbers such as social security, debit/credit and driver's licenses) of individuals and businesses residing or operating in Rhode Island. **All program requirements take effect on June 26, 2016, one year from enactment**.

Key data security expansions and their impacts inside and outside of Rhode Island include the following:

1. **Risk-Based Written Security Plan Now Required for all Holders of Personal Information of Rhode Island Residents Effective in 2016.**

   New Section 11-49.3-2(a) of the Rhode Island General Laws includes a new requirement that every person (broadly defined to include individuals and all forms of businesses), municipal agency and state agency that holds or licenses personal information of a Rhode Island resident "implement and maintain a risk-based information security program." Such written, risk-based program must include reasonable security procedures and practices that "appropriate to the size and scope of the organization, the nature of the information and the purpose for which the information was collected."

2. **Personal Information is Subject to Retention Limits and Holders Must Properly Destroy Such Information.**

   Consistent with the policy that it is in the public interest for businesses and agencies to strive to limit potential harm from personal information breaches by becoming "lean information firms," Section 11-49.3-2(a) of the Act also imposes a new obligation on holders to limit their retention of personal information. Specifically, holders may not "retain personal information for a period longer than is reasonably required to provide the services requested, to meet the purpose for which it was collected, or in accordance with a written retention policy or as may be required by law."

   Holders are also required to destroy personal information properly "in a secure manner" upon disposal, "including, but not limited to, shredding, pulverization, incineration, or erasure."

3. **Holders Must Confirm Security Arrangements in All Vendor Contracts.**

   Similar to Massachusetts information security rules, Section 11-49.3-2(b) now mandates that holders providing personal information to unaffiliated third parties (i.e., vendors) must require "by written contract" that the other party maintain appropriate security protections consistent with the nature and importance of the personal information being transmitted. Existing contracts will be

"grandfathered," but all new vendor contracts entered into after June 2016 will need to include the required contractual security protections.

4. **Disclosure Rules in the Event of a Security Breach Have Been Updated.**

Sections 11-49.3-3 through 11-49.3-6 of the Act update and expand the obligation of holders to disclose unauthorized breaches of personal information and provide remediation to individuals adversely affected by such breaches. Sanctions for noncompliance are enhanced and include (but are not limited to) the ability to impose fines of $100 per record for each "reckless" violation of the Act and $200 per record for each "knowing and willful" violation. In addition to individual notices, breaches involving more than 500 Rhode Island residents must be reported to the State Attorney General and major credit reporting agencies.

IMPACT ON BUSINESSES INSIDE AND OUTSIDE OF RHODE ISLAND

Businesses within and outside of Rhode Island should consider the potential impacts of the Act in at least two principal respects.

First, all businesses with employees, individual customers or whose operations include transactions involving personal information located in Rhode Island should realize that they will be subject to the new requirement to implement and maintain a risk-based written security plan with appropriate risk protections for the business and information at issue. By its terms, the Act's obligation to implement a plan will apply irrespective of whether your business is based in Rhode Island.

Second, all businesses should consider the Act to be yet another "canary in a coal mine" sign of increasing state law level regulation of data security. Massachusetts led this trend five years ago with implementation of its rules that require implementation of a written information security plan (WISP) for all holders of personal information of Massachusetts residents, wherever the holder is located. Nevada has since implemented tough new rules requiring data encryption. As discussed in an earlier bulletin issued in June 2015, Connecticut amended its statutes to increase targeted state law data security protections in several respects. The Act may serve as another example that may well be followed by other states 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 questions about this alert, please contact 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.