Maine's Data Breach Law: *What to do After a Breach*

By Elek Miller and Daina Nathanson May 2015

Data breaches are on the rise. Large and small organizations alike have been affected, and IT experts believe that it's a question of when, not if, an organization will experience a breach. So, what do you do when you discover that your organization has had a security breach and someone has gained access to personal information about employees, customers, clients, or others?

1 Determine Which Laws Apply

Unfortunately, there is no unified federal standard governing what you must do in the event of a data breach. Instead, most states have enacted their own laws, some of which have onerous and complex notice requirements. Which state law applies depends on where you do business and/or where affected employees live, as many state laws protect their residents' personal information, even if that information is maintained by an organization in another state. You may also have other obligations in the event of a breach, depending on the nature of the breach and the type of business you do. For example, a response to a data breach of a financial institution requires compliance with particular federal laws. In addition, you may also have contracts with individuals or other businesses that impose additional obligations related to data breaches and confidential information. Consequently, it is vital to determine which laws and other obligations apply so that you know how to properly proceed.

For organizations maintaining information about Maine residents, Maine's data breach notification law is an integral piece of the data breach response puzzle. The purpose of the remainder of this advisory is to give you the information you need about what Maine's law requires you to do in the event of a data breach, and to provide some suggestions about steps you might want to take before a breach happens.

2 Complying with Maine's Law

Maine's law related to data breaches is triggered when an organization's computer system is breached and personal information is acquired, released, or used without authorization. Most of the time, this happens when someone outside your organization (i.e. a hacker) infiltrates your system. But, unfortunately, sometimes a breach is caused by an absent-minded or disgruntled employee inside your organization who inadvertently or intentionally discloses personal information.

If you experience a breach, the law requires you to conduct a good faith and reasonably prompt investigation to determine the likelihood that personal information has been or will be misused. If personal information has been, will be, or is even likely to be misused, you must give written notice to those individuals who are Maine residents and whose information was compromised.

Under the law, "personal information" means unencrypted data related to a person's first name or first initial and last name in conjunction with any one or more of the following:

- Social Security Number;
- Driver's license or state ID number;
- Account number or credit or debit card number, if the number could be used without additional identifying information, access codes, or passcodes;

- Account passwords or personal ID numbers or access codes; or
- Any of the above when not connected to an individual's first name or initial and last name, if the information that is compromised is sufficient to permit a person to fraudulently assume or attempt to assume the person's identity.

Although the law does not require this notice to take any particular form, you may want to include the following in your notices:

- A summary of the nature and timeframe of the breach.
- The type of information involved (if known).
- Steps taken (or to be taken) to address the breach.
- Appropriate instructions to the recipient of the notice and contact information or a hotline for questions.

Under Maine law, you must provide notice as expediently as possible without unreasonable delay, consistent with the legitimate needs of law enforcement or with measures necessary to determine the scope of the breach and restore the integrity, security, and confidentiality of the data in your computer system. If notice is delayed because of a criminal investigation, you must provide notice within 7 days after a law enforcement agency determines that notification will not compromise a criminal investigation.

Also, if more than 1,000 people must be notified at one time, you must also notify consumer reporting agencies, and that notice must include the date of the breach, an estimate of the number of persons affected (if known), and the actual or anticipated date that affected people were, or will be, notified. If your organization is regulated by the Department of Professional and Financial Regulation, you must also notify them. All other organizations must notify the Office of the Maine Attorney General.

3 Take Steps Now to Help Minimize the Impact Later

Because the steps that you have to take in the event of a data breach are complex, and the law does impose penalties for noncompliance, you should strongly consider designating someone within your organization to take the lead on data breach issues and developing a data incident response plan so that you have a roadmap to follow in the event of a breach. Doing so can reduce the stress and anxiety that inevitably comes with responding to a breach and can help to eliminate potential legal issues down the road related to failure to comply with notice laws.

You should also consider whether it makes sense for your organization to acquire insurance coverage related to data breaches, which may help give you some additional piece of mind.

Elek A. Miller
207.253.0550
emiller@dwmlaw.com

Daina J. Nathanson
207.253.0508
dnathanson@dwmlaw.com