PretiFlaherty

What to do after a Data Breach:
A Primer on Maine's Security Breach Law

By Sigmund D. Schutz
Preti Flaherty
February 6, 2012

Your company just discovered a security breach resulting in the disclosure of personal information concerning customers, vendors, employees, or other individuals. What now? The purpose of this primer is to provide an introduction to what you need to know about notification requirements under Maine's Notice of Risk to Personal Data Act, 10 M.R.S. §§ 1346-1350-B (the "Act").

The essential purpose of the Notice of Risk to Personal Data Act is informational -- to ensure prompt notification to persons at risk of identity theft. The Act prohibits use of personal information acquired through a security breach, imposes prompt notification requirements in the event of a security breach, provides for enforcement and penalties, and requires that law enforcement provide a police report in connection with any reported misuse of personal information.

In the absence of a uniform federal law governing notice requirements in the event of a data breach, the states have enacted a patchwork of notice requirements. At present 46 states plus the District of Columbia, Puerto Rico and the Virgin Islands (and New York City) have enacted security breach notification laws. The holdouts are Alabama, Kentucky, New Mexico, and South Dakota. Maine law applies to Maine residents. Notification to residents of other states is governed by the law of the state of residence.

The Act is a key part of the legal puzzle when it comes to notification of data breaches involving Maine residents, but it is not the whole story. A response to a data breach by financial institutions involves federal law. State law tort claims (e.g., negligence) and unfair trade practices acts at the state and federal level provide incentives to respond thoughtfully to security breaches. Relevant contracts may also address data breach, confidentiality, or related requirements. As in any risk management situation – data breaches are no exception – insurance should also be top of mind.

1. How does the Act define a security breach?

A security breach means the unauthorized acquisition, release or use of an individual's computerized data that includes personal information such that the security, confidentiality or integrity of that personal information is compromised.

The good faith acquisition, release or use of personal information by an employee or agent of a person on behalf of the person is not a security breach if the personal information is not used for or subject to further unauthorized disclosure to another person. 10 M.R.S. § 1347(1)

2. Who is subject to the Act?

Any person, except for financial institutions. A person is broadly defined to include any business, as well as state agencies and state universities. 10 M.R.S. § 1347(5). Requirements differ for information brokers (and that difference is discussed below), but information brokers are a subset of "persons." Financial institutions are exempt because they are subject to substantially similar requirements under federal law. 10 M.R.S. § 1349(4).

3. How is "personal information" defined?

The term "personal information" means an individual's first name, or first initial, and last name in combination with any one or more of the following data elements:

A. Social security number;
B. Driver's license number or state identification card number;
C. Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords;
D. Account passwords or personal identification numbers or other access codes; or
E. Any of the data elements contained in paragraphs A to D when not in connection with the individual's first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

However, data that is encrypted is not included within the definition of "personal information." 10 M.R.S. § 1347(6).

4. Does the Act apply to paper records?

No. A security breach is defined, in relevant part, as the acquisition, release or use of an individual's *"computerized"* data. 10 M.R.S. § 1348. To trigger notification, there must be a breach of the security of a system, which is defined as "a computerized data storage system containing personal information." 10 M.R.S. 1347(7). The Maine Bureau of Insurance issued guidance confirming that the Act "only covers electronic records." A number of other states, however, do require notification of security breaches involving paper records.

5. Do I have to investigate once I become aware of a security breach?

Yes. An investigation must be conducted in good faith and must be a "reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused." 10 M.R.S. §1348.

6. What triggers the duty to notify?

For "information brokers," as defined by the Act, the standard for notification is acquisition of personal information by an unauthorized third-party. Notification is required upon discovery that information has been or is reasonably believed to have been acquired by an unauthorized person. The likelihood of misuse is irrelevant.

For "any other person," the standard for notification is misuse of personal information by an unauthorized third-party. Notification is required upon discovery that misuse of personal information has occurred or if it is reasonably possible that misuse will occur.

10 M.R.S. §1348.

7. Who has to be notified?

All Maine residents. For residents of other states, the security breach notification law of the state of residence should be consulted.

If a third party is maintaining data on behalf of a person but does not itself own the data, the owner of the data must be notified.

If more than 1,000 persons must be notified at a single time, consumer reporting agencies must be notified.

If the entity involved in the security breach is a state-licensed entity, the Department of Professional and Financial Regulation must be notified. All other persons must notify the Attorney General. The contact person at the Maine Office of Attorney General is Linda J. Conti.

10 M.R.S. §1348.

8. Does Maine have a notification form?

No. Some other states do require that notification be made by completing a state-specific form.

9. What are the required contents of the notification?

The Act does not specify the contents of required "notice," except that notice must be written (with certain exceptions for substitute notice) and where notification to consumer reporting agencies is required. The Act requires that notification to consumer reporting agencies contain the date of the breach, an estimate of the number of persons affected by the breach, if known, and the actual or anticipated date that persons were or will be notified of the breach. 10 M.R.S. §§ 1347(4), 1348.

As a matter of good practice, notice to Maine residents may include a summary of the nature and timeframe of the breach, the type of information involved, 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.

Many states outside Maine do require that notices of a data breach include specific information, such as the number of residents affected, information on credit reporting agencies, and notification of the right to request a credit freeze.

10. How quickly do I have to notify?

If Maine residents must be notified, notice "must be made as expediently as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement . . . or with measures necessary to determine the scope of the security breach and restore the reasonable integrity, security and confidentiality of the data in the system." 10 M.R.S. § 1348(1). If notice is delayed as a result of a criminal investigation, notice must be provided within 7 days after a law enforcement agency determines that notification will not compromise a criminal investigation. 10 M.R.S. § 1348(3).

If persons maintaining personal information on behalf of others must be notified, notice must be provided "immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." 10 M.R.S. § 1348(2).

If a consumer reporting agency must be notified, notice must be made "without unreasonable delay." 10 M.R.S. § 1348(4).

The Act does not say how quickly notification must be given to state regulators. 10 M.R.S. § 1348(5).

11. Are there penalties for non-compliance with the Act?

Yes. A person that violates the Act is subject to a civil violation and, if that person holds a state license, to enforcement by the Department of Professional and Financial Regulation. The fine for a civil violation is not more than $500 per violation up to a

maximum of $2,500 for each day the person is in violation. The State is exempt from any fine. The Act may also be enforced by court order requiring certain action or preventing further violations. 10 M.R.S. § 1349.

12. Does the Act create a private right of action?

No. The Act does not create a private right of action for damages. It is enforceable only by the State. However, the Act does not affect or prevent other claims available under state or federal law.

For further information about security breach reporting requirements and related privacy or confidentiality issues, please contact Sig Schutz at Preti Flaherty's Portland, Maine office at sschutz@preti.com or 207-791-3000. Sig and other attorneys at PretiFlaherty have advised numerous companies in responding to security breaches and the firm has served as defense counsel in security breach litigation.