

FEATURE

New Law Addresses Personal Information Breaches

By Maria Recalde

Massachusetts recently became the 39th state to enact a data security breach notification law, the "Breach Notification Law," to deal with security breaches of personal information of Massachusetts residents.

The law applies to any person (i.e., a natural person, corporation, association, partnership or other legal entity) or agency (i.e., any Massachusetts agency, executive office, department, board, commission, bureau, division or authority, or any of its branches, or of any political subdivision) that *owns, licenses, maintains or stores* data that includes personal information of Massachusetts residents.

"Personal information" is broadly defined to include a Massachusetts resident's first and last name or first initial and last name in combination with any one or more of the following data elements that relate to the resident:

- Social Security number;
- Driver's license number or Massachusetts identification card number;
- Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password that would permit access to a resident's financial account; or
- A biometric indicator.

Personal information does not include information that is lawfully obtained from publicly available information, or from federal, state or local



Maria Recalde

government records lawfully made available to the general public.

Own/License. A person or agency that *owns or licenses* data that includes personal information about a Massachusetts resident must provide notice, as soon as practicable and without unreasonable delay, to the Massachusetts Attorney General, the Director of Consumer Affairs and Business Regulation and to the Massachusetts resident, when such person or agency knows or has reason know:

- Of a breach of security (i.e., the unauthorized acquisition or unauthorized use of unencrypted data, or encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality or integrity of personal information, maintained by a person or agency that creates a substantial

risk of identity theft or fraud against a Massachusetts resident); or

- That the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose.

If the personal information involved was encrypted using 128-bit or higher algorithmic encryption and the encryption key was not compromised, notice of a security breach is not required.

The notice requirement, however, applies to *both* paper and electronic records.

The information furnished in the notices to be provided to the Attorney General and Director of Consumer Affairs and Business Regulation must include:

- The nature of the breach of security or unauthorized acquisition or use,
- The number of Massachusetts residents affected by such incident at the time of notification and
- Any steps the person or agency has taken or plans to take relating to the incident.

Proper notice to affected Massachusetts residents must include information regarding the resident's right to obtain a police report, how to request a security freeze on her/his credit report and the necessary information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting agencies.

The notice to affected Massachusetts residents should *not* include either the nature of the breach or unauthorized acquisition or use nor the number of Massachusetts residents affected by

FEATURE

the breach or unauthorized access or use.

Notice may be given in writing, by telephone or electronically, provided that such notice is compliant with federal and state electronic transaction laws.

Substitute notice (i.e., e-mail notice to the affected class of residents, conspicuous posting of the notice on the entity's website, if any, and notice to major statewide media) is permitted if the person or agency required to give notice demonstrates that the cost of providing written notice will exceed \$250,000, that the affected class of Massachusetts residents to be notified exceeds 500,000 residents, or that the person or agency does not have sufficient contact information to provide notice.

The notice to affected Massachusetts residents required under the Breach Notification Law may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. In such case, notice must be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.

Maintain/Store. A person or agency that *maintains or stores* (but does not own or license) data that includes personal information about a Massachusetts resident must provide notice to the owner or licensor of such data as soon as practicable and without unreasonable delay when such person or agency knows or has reason to know:

- Of a breach of security or
- That the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose.

In addition to providing notice, such person or agency is required to cooperate with the owner or licensor of the personal information at issue, by, among other things:

- Informing the owner or licensor of the breach of security or unauthorized acquisition or use,
- The date or approximate date of such incident and the nature thereof and
- Any steps the person or agency has taken or plans to take relating to the incident.

Such cooperation, however, *does not* require the disclosure of confidential business information or trade secrets, or the provision of notice to a Massachusetts resident that may have been affected by the breach of security or unauthorized acquisition or use.

Disposition of Records Requirements. Along with establishing the notice requirements discussed here, the Breach Notification Law heightens security procedures for disposing of records that contain personal information, whether in *paper or electronic* form.

When disposing of any such records, each agency or person must meet the following minimum requirements:

- Paper documents containing personal information must be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed and
- Electronic media and other non-paper media containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.

Any agency or person disposing of personal information may contract with a third party to dispose of such information. The third parties must

implement and monitor compliance with policies and procedures to prohibit unauthorized access to or use of personal information in the course of collection, transportation or destruction of the information.

Failure to comply with the requirements set forth above can be costly – improper disposition of records may result in a fine of \$100 per individual affected, up to a maximum of \$50,000 per event.

Implementation. Finally, the Breach Notification Law directs the Office of Consumer Affairs and the Division of Public Records to establish regulations to implement the law's objectives.

It is critical, therefore, that individuals or businesses handling personal information of Massachusetts residents become familiar with the new law and the associated regulations, and execute them effectively in order to avoid the potential for litigation and/or penalties over the loss or theft of protected information under the Breach Notification Law.

Despite the heightened burden and potential costs placed on persons or agencies owning, licensing, maintaining or storing personal information, overall the Breach Notification Law is an important step toward protecting Massachusetts residents from the serious consequences associated with misuse of their personal information.

The goals of the Breach Notification Law include decreasing instances of identity theft and providing Massachusetts residents with some vehicle for self-help, via notice requirements, police reports and credit freezes, so that victims may better control the outcome of such an experience.

Maria E. Recalde is a shareholder at Sheehan Phinney Bass + Green.