

OPINION

Corporate obligations under the state's new data breach law



SCHREIBER



YOUNG



ECKSTEIN

By Mark E. Schreiber, Robert G. Young and Diana C. Eckstein

The new Massachusetts data breach law, effective Oct. 31, 2007, adds additional compliance obligations for companies evaluating their duties when customer, credit card, financial account, insurance or employee information is improperly accessed and disclosed.

The Act Relative to Security Freezes and Notification of Data Breaches requires entities to adopt measures to safeguard personal information of Massachusetts residents. It also contains new Chapter 93H, which mandates notice be given to specified parties in the event of a data breach involving personal information of state residents.

Any analysis of data breach duties is often complex because the data may cover individuals in various states, and Massachusetts is now the 39th state with a data breach law.

While noteworthy in many respects and in its goal to provide Massachusetts residents with such notice, in practice Chapter 93H creates several potential compliance issues. This is because of a lack of key definitions and inclu-

Mark E. Schreiber is a litigation partner in Edwards, Angell, Palmer and Dodge's Boston office. He is chairman of the firm's privacy group, as well as co-chair of the Boston Bar Association's Privacy Committee. Robert Young is a senior litigation associate at Edwards Angell. Diana C. Eckstein is an associate at Manchel & Brennan in Newton.

sion of a notice provision that forbids the description to affected individuals of the "nature of the breach or unauthorized acquisition or use."

The end result may be that a notice given in Massachusetts will be markedly different from those in other states, and corporate counsel will spend time crafting separate notice versions in major breaches where residents of different states are involved.

Fortunately, the statute provides a safe harbor if a company has procedures for responding to breaches under federal laws, rules or guidelines and gives notice to Massachusetts residents according to those rules.

Following FTC identity theft guidance or complying with Gramm Leach or HIPAA security rule follow-up directed at a particular industry may suffice under Chapter 93H for entities in that industry (i.e., a retailer may not be able to rely on federal guidelines directed, for example, at another industry), if a breach policy is in place.

Best practices are already emerging where corporations are adopting data breach procedures. These consist of a combination of existing incident response and data security protocols, along with breach issue identification, internal team selection and escalation steps, i.e., who is assigned what tasks in the event of a possible data breach so as to avoid the crisis environment that often accompanies such events.

The Department of Consumer Affairs and Business Regulation (CABR) recently issued, and held a hearing on, draft regulations under Chapter 93H broadly requiring companies to develop and maintain a "comprehensive, written security program," including numerous technology safeguards, encryption for covered wireless communications, audit trails and documented response measures to a breach of security.

The attorney general, the secretary of state and other state agencies are also tasked with



In practice, Chapter 93H creates several potential compliance issues.

adopting implementing regulations, and perhaps forthcoming regulations or legislative amendments will clarify the statutory ambiguities.

The near-term consequences are unclear, but Chapter 93H does authorize the attorney general to bring an action pursuant to section 4 of Chapter 93A for violation of the new statute. The statute does not provide a private right of action for affected individuals.

• **Who is subject to the statute?**

Chapter 93H applies to any legal entity (including government agencies, individuals and corporations) that owns, licenses, maintains or stores "personal information" of any Massachusetts resident, regardless of where the entity or personal information is located.

Thus, out-of-state businesses are subject to this act if Massachusetts residents are affected. Although the statute defines "personal information," there is, for example, no specific defi-

inition of the terms “own,” “license” “maintain” or “store.”

These words are critical because the statute imposes greater notice obligations on an entity that owns or licenses personal information (a “data owner”) than on one that only maintains or stores such information (a “data storer”).

Presumably, common law definitions are applicable to these terms in Chapter 93H. Concepts of “own”/“license” versus “maintain”/“store” also are terms of art in technology fields, which seem to be understood in IT departments and in some state agencies. According to some, they are akin to a “data controller” or “data processor,” respectively.

• What is “personal information”?

Under Chapter 93H, “personal information” includes a person’s first name and last name (or first initial and last name) in combination with any one or more of the following: (1) a Social Security number; (2) a driver’s license number or other state-issued identification card number; or (3) a financial account number, or credit or debit card number, with or without any required security code, access code, or PIN that would allow account access.

While this may seem like a straightforward, specific definition, and in most cases it is, the term “financial account number” is not defined. If read broadly, this term sweeps a number of record categories within its reach. For example, besides bank, brokerage or related accounts, other data have a financial or billing component, including health care, insurance and other employee-benefit information.

Strangely, the Chapter 93H definition of “personal information” differs from, and is more narrow than, the definition of “personal information” in new Chapter 93I, which was enacted as part of the same bill and which governs the disposition and destruction of records.

Chapter 93I is effective as of Feb. 3 and defines “personal information” to include biometric indicators, where Chapter 93H does not.

The Chapter 93H definition of “personal information” also differs from similar statutes in other states, some of which have a longer list of what constitutes “personal information” and others of which take a more holistic view of “personal information.”

• What is a breach of security?

A “breach of security” under Chapter 93H is an unauthorized acquisition or unauthorized use of unencrypted data that includes personal information of Massachusetts residents (or encrypted

electronic data along with the confidential process or key that would compromise the security of the data) that creates a substantial risk of identity theft or fraud against a Massachusetts resident.

The term “data” includes hard copy documents in addition to electronic information. Accordingly, Chapter 93H applies regardless of whether the data was stored on a laptop computer, in paper files, in a filing cabinet or in an employee’s briefcase.

• Is there a harm threshold in Massachusetts before notice must be given?

Yes, the “substantial risk of identity theft or fraud” is a key component of the definition of breach of security in Chapter 93H. This is a higher standard than most states. If a company can make a good faith determination, based on supportable facts, that no such substantial risk exists, presumably no notice need be given.

In practice, this may be a judgment call. In some instances, companies will decide to give notice, either because the circumstances are not clear and/or notices must be given in other states regardless.

• When must notice be given?

Chapter 93H does not provide a specific timeframe in which notice of a breach must be given, although other states provide a 45-day limit. The statute provides only that a covered entity must provide notice “as soon as practicable, and without unreasonable delay” after that entity knows or has reason to know that its notice obligations have been triggered by a security breach or unauthorized acquisition. This “as soon as practicable” standard applies both to the data owner and data storer.

There is no explicit delay for a company’s internal investigation, but this is implied in the evaluation of a substantial risk of identity theft, e.g., to make that assessment requires facts that usually require an internal investigation. There is a delay exception if law enforcement determines that the breach notice may impede a criminal investigation and has notified the attorney general of such determination.

• Who must give the notice and to whom?

The data storer (such as, in the employment context, a third-party benefits administrator), is required to provide notice to the data owner (in this case, the employer). The data owner must provide notice to the attorney general, the director of CABR and each affected Massachusetts resident.

The director of CABR will forward the names of any relevant consumer reporting agency or state agency, as deemed appropriate, and the data owner must then provide notice to such consumer reporting agencies and/or state agencies.

• What form must the notice be in?

Written notice is required, which may be in the form of e-mail notice if the entity complies with the federal Electronic Signatures in Global and National Commerce (E-SIGN) Act.

If the cost of providing written notice will exceed \$250,000, or the number of Massachusetts residents to notify exceeds 500,000, the entity may provide notice by e-mail, without having to meet the requirements of the federal E-SIGN Act (if it has the e-mail addresses of the affected residents), posting on the home page of the entity’s website and publication in or broadcast through media that reaches all of Massachusetts.

• What must the notice contain?

The content of the notice depends on the intended recipient. For the data storer, notice to the data owner must include the approximate date and nature of the breach of security or unauthorized acquisition or use and any steps the entity has taken or plans to take regarding the incident.

The data owner’s notice to the attorney general, the director of CABR and any applicable consumer reporting agencies or state agencies must include the nature of the breach, the number of Massachusetts residents affected, and any steps the data owner has taken or plans to take relating to the incident.

The data owner’s notice to individual Massachusetts residents must include information concerning the individual’s right to obtain a police report and how to request a security freeze on one’s consumer report and related fees.

However, as noted, Chapter 93H prohibits the notice to individuals from containing information concerning the nature of the breach, unauthorized acquisition or use, or the number of residents affected. This absence of information was intended to avoid exploitation by others of security breach details; it may also create unnecessary anxiety in some individual notice recipients, which seems to be at odds with the underlying purpose of Chapter 93H.

Finally, the issue of police reports will impose new obligations on local police departments, which hopefully the new regulations will address.

MLW