

Business Insurance

NEWS

Data security law sparks concerns; Massachusetts rule may boost exposure for companies

JUDY GREENWALD

1,001 words

5 April 2010

Business Insurance

BZIN

0003

Volume 44; Number 14

English

(c) 2010 Crain Communications, Inc. All rights reserved.

Data security regulations in Massachusetts, which many describe as the most stringent such rules to date, are proving to be a challenge for businesses, observers say.

The regulations, which apply to any company that has personal information on a Massachusetts resident regardless of whether the business is based in the state, could lead to increased litigation against firms, legal experts say.

The rules that Massachusetts implemented last month based on a 2007 law are likely to influence other states in developing their own regulations, experts say.

Unlike most previous data security rules, Massachusetts' regulations require businesses to proactively implement security measures to protect personal information before a data breach occurs.

The 2007 law, however, is ambiguous about fines for violating the data protection requirements. It also is unclear how vigorously the state attorney general will enforce the provisions. The law was delayed and revised several times in response to complaints by businesses about its feasibility and expense.

Massachusetts passed the law in response to data breaches by retailers, including Framingham, Mass.-based TJX Cos. Inc., which revealed in 2007 that hackers had obtained millions of its customers' credit and debit card and driver's license information.

The rules implemented last month—based in part on the size, scope and type of business—cover the storage and transmission of information. They require firms to develop a written policy and maintain proper information security practices to personal data in their activities and those of their third-party providers (see box, page 22).

They apply to all businesses that maintain personal information about a Massachusetts resident, whether customer or employee, including their name and Social Security number, driver's license, credit cards or similar personal and financial information.

Helen A. Christakos, an associate with law firm Greenberg Traurig L.L.P. in East Palo Alto, Calif., said Massachusetts' approach differs from other states.

"Other state laws are retroactive, in that after there's a security break, then you're required to take certain steps, potentially, to comply with the law," Ms. Christakos said. "This is forward-reaching. It applies even before you have a data security breach" if a business collects personal information.

Firms' readiness for the new rules has differed. Some companies "are just now really focusing on having their compliance efforts in place," said Mark Paulding, an attorney with Hogan & Hartson L.L.P. in Washington. Others have been more proactive, he said.

Matthew D. Hanaghan, a staff attorney with Nutter McClennen & Fish L.L.P. in Boston, said one of the more difficult tasks companies have faced has been "identifying what information they store, where it is and how it's stored, and conducting a risk assessment to determine how vulnerable that information is, and how they can go about protecting it by applying at least the minimum security that's required by the regulations' standards."

Another challenge has been the rules' required encryption of personal data, attorneys say.

"In some cases, it may be easier for some companies to not distinguish between Massachusetts' personal information and others' and encrypt everything," said Barry A. Guryan, a member of law firm Epstein Becker & Green P.C. in Boston. "On the other hand, that may be so onerous to other companies that it is not a practical solution."

The statute provides for a fine of \$5,000 per violation, but it is unclear whether that applies to a single data breach or whether it applies to every person affected by a data breach, observers say.

A spokesman for the Massachusetts Division of Insurance, which is part of the Office of Consumer Affairs and Business Regulation, did not respond to a query as to whether these fines can be insured under Massachusetts law.

As for enforcement, "I don't know what resources they have to be able to do this or how aggressive they're going to be," said David Navetta, a partner with the Information Law Group in Denver. "It's not a given that Massachusetts will be able to enforce this statute against out-of-state companies."

There is no private right of action under the law, which means plaintiffs cannot bring suit under the law itself, said Bruce H. Nielsen, a partner with law firm K&L Gates L.L.P. in Washington. But companies found in violation could be sued, for example, for invasion of privacy, he said.

Some observers expect litigation will result from the rules.

"I think it's an invitation to a greater amount of lawsuits against organizations," with the regulations setting a "pretty high bar for companies to establish that they put reasonable security measures in place," said Tracey Vispoli, global cyber security manager for Warren, N.J.-based Chubb Corp.

The regulations set expectations "for what a company should be doing," said **Toby Merrill**, Philadelphia-based vp at ACE Professional Risk, a unit of ACE USA. "If a company has an incident and it's clear that they were not living up to that standard, I think the argument is made easier for the plaintiffs bar to go after" that firm, he said.

Past data breach cases generally have not been successful, but they still incur defense costs, with some proceeding as far as the summary judgment stage, said Philip C. Gordon, a shareholder with law firm Littler Mendelson P.C. in Denver.

Amy Crafts, an associate with law firm Proskauer Rose L.L.P. in Boston, said the Massachusetts rules, which are the "most stringent" of any states', could influence other states.

It provides "a blueprint for regulation in this area," said Elizabeth A. Ritvo, a partner with law firm Brown Rudnick L.L.P. in Boston.

"I think that other states will carefully look to see how this goes in determining how they will want to make changes to their notification laws," said Mark Camilo, vp, professional liability with Chartis Inc. in New York.

Document BZIN000020100409e64500006