RHODE ISLAND LAWYERS WEEKLY

New identity theft protection law receiving mixed reviews

Businesses seen as benefitting from high liability standards

By: Pat Murphy August 27, 2015

While lawyers of all stripes see the state's new identity-theft statute as a step forward, some question whether it has the "teeth" necessary to be a truly strong consumer-protection measure.

Enacted by the General Assembly in June, the Identity Theft Protection Act governs the steps businesses and other entities must take to prevent the theft of personal information like Social Security and credit card numbers from their systems.

The law provides for civil penalties of up to $100 per record for "reckless" violations of the statute, and penalties up to $200 per record for "knowing and willful" violations.

Pawtucket consumer protection attorney Christopher M. Lefebvre called the new law a "good start."

However, Lefebvre believes the law doesn't go far enough, in particular because it doesn't hold businesses liable for negligence or expressly provide consumers a private cause of action.

"If the state really wanted to be at the forefront of identity-theft protection, then the statute should provide very strong penalties," Lefebvre said. "This statute does not do that."

But Providence attorney Steven M. Richard rejected any notion that the new identity-theft law is an impotent piece of legislation.

"The law has some very important signals within it that businesses, municipalities and state agencies are expected to be proactive in protecting data and react promptly in event of breach," said Richard, who practices commercial law at Nixon Peabody in Providence.

'Risk-based' security programs

The new identity-theft law replaces a similar one enacted by the General Assembly in 2005 and takes effect June 26, 2016.

A central feature of the act is a requirement that businesses, and any other covered entities that acquire the personal information of Rhode Island residents, implement and maintain a "risk-based information security program." A security program must include "reasonable security procedures and practices appropriate to the size and scope of the organization, the nature of the information and the purpose for which the information was collected."

Providence attorney Roger W. Hood recognized an inherent advantage in the "reasonableness" standard adopted by the state legislature.

“It gives small businesses the flexibility to tailor a plan to their needs, balancing both the security requirements that they may have and their overall business requirements,” said Hood, a business and intellectual property lawyer at Duffy & Sweeney.

New G.L. §11-49.3-4(a)(1) obligates covered entities to provide notice to residents whenever a security breach “poses a significant risk of identity theft.” Like the old statute, notice must be provided in the “most expedient time possible.”

The new law, however, adds that notice shall be made “no later” than 45 days after “confirmation of the breach.”

“The 45-day period is a necessary and reasonable limitation because you have to have some period of time that is prescribed in which you take the appropriate measures to react to any type of breach or improper release of data,” Richard said.

Hood believes the 45-day time limit is the most significant change to the state’s identity-theft law.

“There are very few states that have enacted fixed time limits for when you must notify individuals of a security breach,” he observed.

Linn F. Freedman practices data privacy and security law at Robinson & Cole in Providence. Freedman emphasized that the 45-day notice period isn’t triggered until there’s actual confirmation that there was an unauthorized disclosure.

“That is a very fair and balanced way to decrease the amount of time businesses have to provide notice,” she said.

Freedman added it was important that the new identity theft law retained language from the old statute imposing a notification duty only when a security breach poses a “significant risk” of identity theft.

“It’s a really good thing so you’re not sending out letters [all the time],” said Freedman. “Consumers are getting desensitized. In many states, you have to notify even when there isn’t a significant risk of identity theft.”

The new law also requires businesses and other covered entities to notify the Attorney General and the major credit reporting agencies whenever a data breach involving more than 500 Rhode Island residents occurs. In addition, the act adds medical information, health insurance information and email addresses, when acquired with their passwords or other access codes, to the statutory definition of protected “personal information.”

Liability gap?

Companies and other covered entities are subject to civil penalties as provided in G.L. §11-49.3-5. Under G.L. §11-49.3-5(a), each “reckless” violation is subject to a penalty of not more than $100 per record, and under G.L. §11-49.3-5(b), each “knowing and willful” violation is subject to a penalty of not more than $200 per record.

According to Lefebvre, the statute contains an inherent inconsistency between the duty of care imposed by the statute with respect to the security of personal information and the authorized penalties. Lefebvre maintains that the statute suggests a negligence standard of liability by requiring businesses to implement “reasonable” security procedures, yet the statute does not authorize civil penalties for negligence.

“Typically, when you bring a lawsuit, the standard is simple negligence,” said Lefebvre. “Do you have a duty? Did you breach that duty?”

Lefebvre said he expected that it would be difficult to prove recklessness under the statute and “almost impossible” to show willfulness. According to Lefebvre, by imposing heightened standards of liability, the statute would be less likely to achieve its objective of protecting consumers.

“There’s no doubt whenever a law is passed the standard for a breach is always what motivates businesses to change their practices,” he said.

Corporate and business lawyer Brian J. Lamoureux likes the new law.

“In the short term it’s great news for consumers, and in the longer term it will be very good news for businesses who implement the controls and protect themselves in the event of a data breach,” said Lamoureux, of Pannone, Lopes, Devereaux & West in Providence.

Yet Lamoureux admitted to also being surprised that the statute did not impose liability for negligence.

“It appears the General Assembly has set a standard that might not catch some well-meaning but negligent companies in its grasp,” he said.

Lamoureux suggested that the omission of a negligence standard of liability was the product of a legislative compromise.

“There are a lot of companies out there trying to make payroll every two weeks and I don’t think the General Assembly was really interested in having them all subject to being whacked for negligent failures to comply with the statute,” he said.

Richard said it makes sense not to hold companies liable for simple negligence.

“Penalties in deterrence imply a higher level of culpability,” he said. “My assumption is that the General Assembly recognized that we do have to give companies some latitude as it comes to and relates to their business judgment.”

No private cause of action

Lefebvre was also troubled that the statute does not expressly recognize a private right of action for consumers to recover actual damages in addition to penalties, or provide for the recovery of attorneys’ fees and costs.

“States that are very progressive in protecting privacy will typically have a private right of action so that those attorneys that deal with consumer protection will have an incentive to bring cases against those entities that don’t comply with the law,” said Lefebvre.

Freedman noted that, even though consumers don’t have a remedy under the statute, they still can bring a separate cause of action against a business to recover any actual damages relating to the disclosure of their personal information.

Lamoureux suggested that state courts could ultimately decide that a private right of action was implied under the statute. He added that he was unsure how class actions would ultimately fare under the new law. On the issue of attorneys’ fees, Lamoureux conjectured that the common-fund doctrine could prove to be an avenue for recovery.

Freedman said it was important to note that the new law eliminated the old law’s $25,000 cap on penalties.

“It’s definitely a concern because the civil penalties now are unlimited and you can’t really manage that risk,” said Freedman.

Freedman said another “consumer friendly” change was the law’s clarification that state agencies and municipalities are required to protect personal data just like private companies.

“That is important because a lot of times Rhode Island residents have had to provide their Social Security number, their driver’s license number and all sorts of personal information to state and municipal agencies with no statutory protection,” she said.