Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

NY Data Security Law Boosts Liability As Cyberattacks Surge

By **Allison Grande**

Law360 (April 16, 2020, 9:18 PM EDT) -- A New York law that requires companies to fortify their data security programs went live quietly last month, significantly expanding businesses' liability risks and forcing them to take a hard look at how they're protecting personal data at a time when hackers are seizing on the coronavirus pandemic to launch a fresh wave of attacks.

While most companies have grown accustomed to government mandates to beef up their security protections in the face of mounting cyber threats, New York's move to require businesses to include certain specific elements in their data security programs takes to the next level the work that companies must put into protecting state residents' data.

"This law really forces companies to take cybersecurity much more seriously and take a much deeper dive to look at what security measures they have in place and whether they'd be susceptible to fines because they don't have what the law says are reasonable security measures," said Matthew Dunn, an associate managing director in the cyber risk practice at Kroll Inc., a division of Duff & Phelps Corp.

The Stop Hacks and Improve Electronic Data Security Act, or Shield Act, empowers New York's attorney general to bring claims and seek restitution against businesses that fail to comply with the law's enhanced data security and breach notification requirements and to recover uncapped civil penalties of up to $5,000 per violation for data security missteps.

The law took effect in two phases. The portion that broadens the state's existing breach notification requirement came into force in October, while the requirement for companies to adopt reasonable safeguards to protect New Yorkers' data kicked in on March 21. With both provisions now live, attorneys expect New York Attorney General Letitia James to quickly begin exercising her new enforcement powers.

"In general, apart from this statute, the New York attorney general has been very proactive on cybersecurity enforcement issues, and it wouldn't be surprising to see that follow through into this area as well," said Mark Krotoski, co-head of Morgan Lewis & Bockius LLP's privacy and cybersecurity practice.

The attorney general is most likely to act in instances where "a business has had a data breach or has suffered a cybersecurity vulnerability that has become public," said Kristen Mathews, a partner in Morrison & Foerster LLP's global privacy and data security group.

But enforcement won't be limited to these circumstances, attorneys said.

Under the old version of the state's breach notification law, which the Shield Act amended, businesses' exposure was contained to liability for failing to timely report an incident to the attorney general. But the new statute allows the attorney general to widen her enforcement net by going after not only deficient breach notices, but also subpar data security standards.

"I would expect the Shield Act would allow the attorney general to do more than say, 'You were late in notifying,'" said Theodore P. Augustinos, a Locke Lord LLP partner and member of the firm's privacy and cybersecurity group. "Now the attorney general can say that a company didn't meet some reasonable standard of security."

This shift gives the attorney general an opening to look closely at the steps that companies are actually implementing to secure consumers' data and to measure that against the statute's uniquely specific security requirements, which include conducting regular employee training and ensuring service providers are implementing similarly robust security safeguards, according to Augustinos.

"I would expect we'll see more interest, more follow-up questions and potentially more enforcement actions from the attorney general moving forward," he said.

While the Shield Act doesn't allow consumers to sue for alleged violations, attorneys are anticipating that the plaintiffs bar will be looking at the specific security requirements contained in the law to bolster claims that a company had failed to meet their legally mandated obligations to institute reasonable security protections.

"The law does inform what reasonable security is, and we've seen in the past that kind of use by plaintiffs of a legal standard that doesn't have a private right of action attached, so I'd expect that we'll see it here as well," Augustinos said.

This scrutiny from the attorney general and class action bar is expected to be particularly intense during the coronavirus crisis.

Attorneys have said that they are responding to a spike in data security incidents as cyber criminals attempt to take advantage of distracted, newly remote workers and stretched-thin IT staffs, and several government agencies have recently issued warnings about the heightened risk of threats such as ransomware and phishing attacks.

This landscape is likely to lead to not only more breach reports but also more questions about how companies are protecting their networks from such intrusions and whether those protections comply with the Shield Act.

"The threats have not abated because of the pandemic and the interest of enforcement agencies won't abate because of the pandemic, so companies really need to forge ahead," Augustinos said.

Experts acknowledged that some companies may be struggling right now to find the proper resources to devote to their cybersecurity efforts. Kroll's Dunn noted that requirements like holding regular employee training are likely to be significantly affected by the mass migration to remote working and IT departments' focus on dealing with issues arising from that change.

"When we're talking about reasonable security measures, that's going to be a balancing act for IT departments that are trying to ensure that people have access to the network if they're working from home and that they're keeping the company up and running," Dunn said.

But at the same time, the technical, physical and administrative data security safeguards contained in the Shield Act, while more specific than other laws, aren't necessarily groundbreaking, attorneys noted. And companies have been aware of their obligations to impose these measures since July, when the bill was enacted, meaning the attorney general is likely going to expect companies to have a solid data security framework in place even if they can't execute all the elements at the moment.

"I'm not sure anyone is expecting the pandemic to be a good excuse for taking their foot off the gas on cybersecurity or for getting to it later," Augustinos said.

Overall, the Shield Act doesn't mark a dramatic departure from the existing 50-state breach notification laws or roughly two dozen state data security laws, in that it only adds new standards and doesn't conflict in any material way with these laws.

What is notably different about the law, however, is that it gives more context to what's considered "reasonable" security and lays out some specific elements that should be included in a corporate data security plan. These include mandates that companies designate an employee to oversee cybersecurity operations, provide employees with regular training on these issues, and select service providers that are capable of maintaining appropriate security safeguards.

The law also includes the novel requirement for businesses to dispose of sensitive personal information within a reasonable amount of time after it is no longer needed for business purposes, a task that "may present a challenge for businesses that retain records in filing cabinets, archival tapes and in unstructured digital formats," said Mathews, the Morrison & Foerster partner.

These clear obligations have inspired even companies that already have these protections in place to revisit what data they hold and how they're protecting it, and to make sure policies and procedures that may have been in place for years are written down and properly documented.

"This has been the time for a lot of companies to sit up and say, 'Here's another set of requirements, let's see if we meet these,'" Augustinos said.

Companies that experience breaches, whether they stem from the pandemic or not, will also need to be careful about how they go about deciding whether to disclose these incidents to the public, according to attorneys.

Under the Shield Act's breach notification provision, which subjects companies to the potential for fines of $20 per instance of failed notification with a $250,000 cap, incidents that trigger a breach notification include not only instances where data has been acquired but also where it has been viewed without authorization and there's a likelihood of consumer harm.

That expansion is likely to change the way that companies assess incidents and lead to additional notifications, attorneys said.

"Companies will need to think hard about what information's been accessed and how likely it is that the incident exposed the information or individuals to harm," Augustinos said.

This type of heightened liability for botched breach reports and inadequate data security isn't limited to New York and may soon be expanding to other states, attorneys said.

While the pandemic has put most lawmaking activities not related to the crisis on hold, states have been aggressively responding to a lack of federal data security legislation by enacting their own laws to address the issue.

Some states, like New York, Massachusetts and California, have taken the approach of requiring companies to implement reasonable security protections, such as running data-mapping exercises to figure out what information they hold and where it's stored. Ohio, on the other hand, has taken a more hands-off approach by rewarding companies that follow certain established data security guidelines rather than punishing them in the wake of lapses.

"At the end of the day, states want to incentivize companies to ensure they're implementing cybersecurity safeguards in a reasonable manner," Krotoski said. "There are many ways to do that, so states have a lot of different options to choose from."

What impact the Shield Act will have on the debate over whether to mandate or encourage strong cybersecurity safeguards remains to be seen, but attorneys said the regime set up by New York lawmakers will at least be a major part of the discussions in other states moving forward.

"I'm not sure that the New York law will be a clear model, but it will certainly be an inspiration for other states to do something along these lines in the future," Augustinos said.

--Editing by Aaron Pelc.
