Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

State AGs Won't Stand Down In Face Of Federal Breach Law

By **Allison Grande**

Law360, New York (January 14, 2015, 9:32 PM ET) -- The White House's proposal this week to create a national data breach reporting standard would likely strip states of the ability to set their own rules, but attorneys general could keep the pressure on companies using the proposal's enforcement provisions or state laws that aren't preempted by the measure.

On Tuesday night, the White House released the complete text of the Personal Data Notification and Protection Act, a legislative proposal that President Barack Obama had previewed in a speech at the Federal Trade Commission a day earlier. Under the proposed measure, companies would be required to notify affected individuals within 30 days of discovering the incident.

In setting a federal standard, the legislation would preempt any provision of state law "relating to notification by a business entity engaged in interstate commerce of a security breach of computerized data," effectively canceling out the current patchwork of 47 state notification laws and leaving states like California unable to wield more stringent and detailed disclosure obligations.

"States realize that this is a national problem and are generally in favor of something more formal in terms of a federal law, but on the other hand, state attorneys general hate preemption, so there's likely to be a fight over that," Reed Smith LLP partner Divonne Smoyer said.

In the wake of high-profile breaches at companies such as Target Corp. and Neiman Marcus Group Ltd. LLC, states including California and Florida have strengthened their data breach laws to tighten reporting timelines and expand the universe of covered personal information.

But if the federal notification measure proposed by the Obama administration were to make it through Congress, states would no longer have the power to make rules more stringent than the federal baseline.

"I think consumers will lose if federal legislation is passed in the area of breach notification because right now most companies are complying with the most stringent standards in an effort to ensure compliance everywhere," Shook Hardy & Bacon LLP data security and data privacy practice co-chair Al Saikali said. "Chances are, particularly given the new pro-business makeup of Congress, the federal legislation will be less stringent than the most stringent state laws."

Opposition to the proposal is likely to come from not only the attorneys general of big states such as

California and Illinois — the latter of whom pushed lawmakers during a House hearing in February to allow states to continue to set the bar for breach notification — but also members of the president's own party, attorneys say.

"If the legislation were to supersede applicable state statutes, then the consumer affairs objectives that are well-entrenched in states like New York and Massachusetts would no longer be met, and that's not likely going to carry very well with Democrats," Drinker Biddle & Reath LLP partner Kenneth Dort said.

Some of the protections that could be lost if the federal law is allowed to trump state regulations are requirements surrounding breaches involving paper documents and health-related data that does not fall under the purview of the Health Insurance Portability and Accountability Act, attorneys noted.

"Whenever a change is made, it's important to remember that it's not always in a vacuum," Dorsey & Whitney LLP partner Melissa Krasnow said. "You have to consider the whole system of laws and relationships."

One of the most "glaring holes" in the proposed federal legislation is that it does not mention health data. Thus, business entities and associates not otherwise subject to the Health Information Technology for Economic and Clinical Health Act, which governs HIPAA-covered providers, may not be required to notify of certain breaches of health information, according to Mintz Levin Cohn Ferris Glovsky & Popeo PC privacy and security practice chair Cynthia Larose.

"Some states, such as California, have health information tied to identifiers included in their notification laws, but if enacted, this federal law would take over for all entities," Larose said. "So if there's an entity not otherwise covered by HIPAA that has its health information go missing or is accessed without authorization, they may not have to give notice."

However, while states are likely to be hamstrung by the limitations of preemption, attorneys were quick to note that being unable to go beyond the federal baseline does not necessarily mean that companies wouldn't be hearing from state enforcers if they slip up.

In recent years, state attorneys general have used their authority under state notification laws and other consumer protection statutes to launch investigations into data breaches at companies ranging from Target to JPMorgan Chase & Co., and to bring enforcement action against breached entities for their notification and security failures.

Last week, a coalition of nine attorneys general announced a settlement with online retailer Zappos Inc. aimed at addressing cybersecurity concerns from a 2012 hacking attack, and TD Bank NA in December agreed to settle allegations that it waited too long before notifying the Massachusetts attorney general of an intrusion. The California attorney general also grabbed headlines in January 2014 when she sued Kaiser Foundation Health Inc. for allegedly taking too long to notify consumers about a breach.

"I would anticipate that the states will keep doing what they've been doing," said Art Ehuan, a managing director with professional services firm Alvarez & Marsal.

And the administration's proposal allows for enforcement by attorneys general. Under the proposed legislation, attorneys general would be allowed to bring civil actions on behalf of their states' residents to force compliance with the federal standard, enjoin the allegedly unlawful conduct and recoup civil

penalties of up to $1,000 per day per affected individual, up to $1 million per violation.

"Because they would have enforcement authority under the law, to the extent they're not preempted, they could do things the way they have done them before," Smoyer said, noting that several state regulators have similarly seized on the enforcement mechanisms contained in federal consumer protection laws such as HIPAA and the Dodd-Frank Act.

Depending on how broadly the preemption provision is drawn, state regulators should also still be able to provide a check on companies' privacy practices using other state laws that will remain in their arsenal, including those that set specific data security standards and "mini FTC Acts" that prohibit unfair and deceptive trade practices, attorneys noted.

"This legislation doesn't say that states can't pursue claims for unfair or deceptive business practices under state law if they don't like what companies are doing," Smoyer said. "The proposed federal law is about notification and not about how companies protect and use data, which varies widely from state to state."

Attorneys also stressed that there were no guarantees that the administration's proposal would be enacted, given that similar measures in the past have failed to gain traction.

If history repeats itself, attorneys predicted that not only would states not have to worry about giving up any of their power, they might actually be in a better position to strengthen and expand the authority they already have to ensure that breaches are being reported in a timely manner.

"Apart from driving federal action, the continued focus on data breach notification might cause states to take up the issue directly and pass legislation if federal lawmakers don't move," Morrison & Foerster LLP partner Andrew Serwin said.

--Editing by Katherine Rautenberg and Brian Baresch.
