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

Conn., NY Pave Way For Privacy Crackdown Among AGs

By **Allison Grande**

Law360, New York (November 14, 2011, 2:58 PM ET) -- Attorneys general in Connecticut, Massachusetts and New York are leading the crackdown on privacy enforcement as the states' regulatory reach expands and officials scramble to capitalize on this hot-button issue, attorneys say.

"Whether you're a Republican, Democrat or independent, you like the idea of knowing that the state is taking steps to protect your medical records or financial records or other personal information," Littler Mendelson PC's privacy and data protection practice group chair Philip Gordon told Law360.

The most active attorneys general in privacy enforcement have all sought higher office, with former Connecticut Attorney General Richard Blumenthal winning a seat in the U.S. Senate, ex-New York Attorney General Andrew Cuomo running a successful campaign for state governor, and current Massachusetts Attorney General Martha Coakley losing a senatorial bid.

And attorneys general who bring successful enforcement actions in high-profile privacy and data breach cases are seeing a major boost to their political profile, according to Gordon.

"Privacy and information security enforcement actions are a good way to get media attention to show that the attorney general's office is doing something to make a difference in the state," Gordon said.

In September, current Connecticut Attorney General George Jepsen stepped up enforcement in his state with the creation of a task force to investigate Internet privacy and data breaches and to educate the public about those issues.

"There's definitely been a trend toward an increase in the number of state attorneys general enforcement actions, and Connecticut has been one of the more active states, so the fact that it is formalizing a task force to better educate consumers and enforce privacy statutes is not surprising," Dorsey & Whitney LLP partner Melissa Krasnow said.

Jepsen's action builds on the precedent set by Blumenthal, who in May 2010 became the first state attorney general to exercise the expanded authority under the February 2009 Health Information Technology & Economic Clincial Health Act that allows state attorneys general to bring actions against companies for violations of the Health Insurance Portability and Accountability Act.

In that case, Blumenthal secured a first-of-its-kind settlement in July 2010, which required Health Net Inc. and its affiliates to pay $250,000 for failing to secure the private patient medical records and financial information on nearly half a million Connecticut enrollees.

While Blumenthal and Vermont Attorney General William Sorrell — who settled with Health Net for $55,000 in January over the same alleged violation — have been the only attorneys general to date to use this expanded authority, Krasnow predicted that more attorneys general may soon follow suit.

“HITECH is fairly recent in terms of enactment, and now the practical implementation of enforcement will follow, especially as increasing attention is being paid to privacy and data breaches,” Krasnow said.

And given the weight that consumers are placing on the protection of their health care information, attorneys general will find that these actions further help them gain exposure, Gordon added.

“The attorney general can use these actions to show that he is fulfilling his or her mandates to enforce state law and to protect consumers, and if he is seeking higher office, that's an additional plus,” Gordon said.

After losing her U.S. Senate race in 2010, Coakley went back to being active in the privacy enforcement arena in her state, reaching two well-publicized settlements in privacy actions brought under Massachusetts data breach law in 2011.

In August, Coakley announced a $7,500 settlement with Belmont Savings Bank following a May 2011 data breach involving the names, Social Security numbers and account numbers of more than 13,000 state residents.

This resolution came five months after Briar Group LLC, which owns and operates several popular bars and restaurants in the Boston area, agreed to pay the state $110,000 to resolve allegations that it failed to take reasonable steps to protect patrons' personal information, which put the payment card information of tens of thousands of consumers at risk during an April 2009 data breach.

Meanwhile, before being elected governor, Cuomo brought a high-profile action under the state's consumer protection regulation derived from Section 5 of the Federal Trade Commission Act, securing a $100,000 settlement against software company Echometrix for allegedly offering to sell children's private online conversations to marketers.

While Connecticut, Massachusetts and New York have taken the lead in these actions, evolving state data breach notification laws have allowed other state attorneys general to increase their involvement in this area as well.

“Any state with data breach authority can bring these actions; it's just a matter of how aggressive they want to be and how much they want to focus on that issue over other issues,” Foley & Lardner LLP's privacy, security and information management practice founding chair Andy Serwin said.

In July, Indiana attorney general Greg Zoeller reached a $100,000 settlement with health insurer WellPoint Inc. for failing to timely notify his office of a data breach as required by the state's new breach notification law passed in 2009.

California, the first state to pass a breach notification law, recently enacted an amendment to its statute, requiring companies to notify the attorney general of a breach that impacts more than 500 residents beginning in 2012.

But while some states have reaped the benefits of an increase in statutory power, others have lagged behind, with four states not having any data breach notification laws and other states' laws lacking a requirement to notify the attorney general of a data breach.

“Different statutes provide for different attorney general enforcement, so a state that has no affirmative legal requirement to notify the attorney general or other state regulator or a resident will be less likely to bring enforcement actions,” Krasnow said, adding that these discrepancies are unlikely to be fixed unless uniform federal data breach legislation passes in Congress.

Another factor preventing more states from bringing these actions is a lack of resources, according to Serwin.

“There's certain policy decisions to be made that affect how active a state attorney general wants to be in a certain area,” Serwin said. “Attorneys general only have so much time, so it becomes a resource allocation issue if you have a large-scale business fraud that sends a bigger message to bring an enforcement action for than a privacy case would.”

But despite these limitations, attorneys agree that as information becomes ever more valuable to consumers and hackers find new ways to attack this commodity, attorneys general will find more ways to protect their residents through enforcement actions.

“There's an increasing focus on the issue and the role of information in our society, and it's only going to get more important,” Serwin said. “And the more important it gets, the more law enforcement resources we're going to see focused on it.”

--Editing by Eydie Cubarrubia.