Wyrick Robbins Yates & Ponton LLP
4101 Lake Boone Trail, Suite 300
Raleigh, NC 27607
919.781.4000
www.wyrick.com

2018 Actions Show North Carolina Attorney General Emerging as Leading Privacy Enforcer

January 8, 2019

Unlike attorneys general in Massachusetts, New Jersey, and California, North Carolina's Attorney General has not historically been an active privacy and data security regulator. But if his 2018 activity is any indication, North Carolina Attorney General Josh Stein should be top of mind when privacy practitioners name the most active privacy enforcers in the U.S.

The activity described below demonstrates that the North Carolina Attorney General's office (1) has a consistent concern that data breach notifications are not made quickly enough, (2) is maximizing enforcement and investigation efforts by joining multistate actions and pursuing independent initiatives simultaneously, and (3) is consistently undertaking legislative and policy advocacy that demonstrates a strong and comprehensive interest in privacy issues.

Data Breach Notification Timing

In an interview, Attorney General Stein stated that he is "alarmed when companies hold back information about breaches from their customers" and that "people need to know as soon as possible that their data may be compromised."

Attorney General Stein acted on that concern both in his legislative and enforcement efforts. At the beginning of the year, he and Representative Jason Saine published a bipartisan fact sheet proposing new data legislation called The Act to Strengthen Identity Theft Protections. One proposal would eliminate the current provision requiring notification "without unreasonable delay" in favor of a 15-day deadline for consumer notification. If passed, this deadline would be half the 30-day deadlines of Florida and Colorado that are currently the shortest in the nation for industry-agnostic breach laws.

Even without a stricter notification deadline enacted, Attorney General Stein successfully recovered from Uber for delaying notification of a data breach to its drivers for over one year. On September 26, the Attorney General's office

Related Attorneys

Sean W. Fernandes
sfernandes@wyrick.com

Elizabeth H. Johnson
ejohnson@wyrick.com

announced the state would collect $3.6 million from a nationwide settlement of claims stemming from the notification delay.

Maximizing Available Enforcement and Investigation Tools

The Attorney General's office also maximized privacy enforcement efforts through both multistate and unilateral action. North Carolina joined in a multistate HIPAA lawsuit that is the first use of states' HIPAA enforcement authority in federal court since the HITECH Act extended that authority in 2009. The states claim that hackers obtained the social security numbers and health diagnoses for 3.9 million patients due to health care vendors' failure to implement basic security measures. They also assert claims based on the vendor's misleading representations, such as statements in the vendors' privacy policies claiming they would encrypt the breached data.

Attorney General Stein also joined other attorneys general in signing a National Association of Attorneys General letter to Facebook about the Cambridge Analytica scandal. The letter stressed potential consumer deception as a regulatory concern. The signatories noted Facebook's position that the data disclosure to third parties "was not the result of a technical data breach," but were still critical because "Facebook allowed third parties to obtain personal data of users who never authorized it, and relied on terms of service and settings that were confusing and perhaps misleading to its users."

The Attorney General's office also pursued investigations of Facebook and Google over security incidents to which North Carolina's data breach notification law did not apply, suggesting future investigation and enforcement actions may rely more on consumer protection theories than privacy and data security statutes. The Attorney General's office demanded an accounting of incident impacts in the letter discussed above, a later letter to Facebook about a breach of 50 million accounts, and a letter to Google about the exposure of Google+ accounts. None of those incidents triggered the North Carolina breach notification law because the impacted contact and profile information did not include the more sensitive data elements covered by the North Carolina law. Nevertheless, the Attorney General's office demanded an accounting of how many North Carolina consumers the incidents impacted, a description of the incident, and the companies' efforts to prevent a similar incident from occurring in the future.

Privacy and Data Security Policy and Legislative Advocacy

Attorney General Stein also engaged in extensive policy and legislative advocacy throughout 2018. As mentioned above, Stein joined Representative Jason Saine in publishing a fact sheet proposing new privacy and data security legislation. In addition to the 15-day notification deadline, other proposed changes would expand the scope of North Carolina's data breach law, make existing response requirements stricter, and create new enforcement risks:

- Expanding the definition of "Security Breach" to cover incidents where

information is only “accessed,” not “accessed and acquired.” This modification is intended to cover ransomware incidents, and, depending on its final drafting, could also cover system glitches or other errors that allow access with no impact to consumer protection.
- Adding medical information and insurance account numbers to the already expansive list of covered personal information.
- Requiring businesses to implement and maintain reasonable security measures for personal information and make a violation of this requirement a per se unfair and deceptive trade practice punishable with treble damages for each affected individual.

As a policy matter, the Attorney General’s office demonstrated its focus on data breach impacts to North Carolina by issuing, for the first time, a report on the prior year’s data breaches. The data were compiled leveraging the online reporting portal the North Carolina Department of Justice requires organizations to use to report breaches. That report shows that 1,022 data breaches that may have impacted over 5.3 million North Carolinians occurred in 2017 and that 53% were caused by “[h]acking/unauthorized access.” The report concluded that “protecting consumers’ sensitive, personal information must be a top priority for all organizations.”

Attorney General Stein also engaged in federal legislative and regulatory advocacy on privacy issues beyond data breaches. He signed onto two letters from attorneys general to Congress. The first letter supported the passage of the CLOUD Act, which ensured law enforcement could obtain warrants for data stored on foreign servers. The second letter advocated for the preservation of existing state law privacy protections under any federal privacy or data breach legislation.

The Attorney General also took a leadership role in a bipartisan group of state attorneys general addressing robocall regulation. He also sent a comment to the Federal Communications Commission calling for a rule that would allow telecommunications providers to block illegal robocalls.

Conclusion

The North Carolina Attorney General’s office had a very active privacy and data security year in 2018. There is little reason to expect that North Carolina’s Attorney General will slow or abandon this level activity. Organizations processing personal information regarding North Carolina residents would be well-advised to put the state more fully on their radar for continuing developments. In particular, if Attorney General Stein reasserts his interest in a news-making change to North Carolina’s breach notice law, businesses nationwide will need to shift their compliance programs to meet a new high bar.

Timeline of 2018 North Carolina Attorney Actions and Advocacy

- **January 2018: Report on 2017 Data Breaches**

- January 8, 2018: New Data Breach Legislation Proposals
- February 21, 2018: Letter on Passage of CLOUD Act
- March 19, 2018: Bipartisan State Attorneys General Letter on Preserving State Data Breach Authority
- March 26, 2018: National Association of Attorneys General Letter to Facebook
- September 26, 2018: Uber Settlement Over Delayed Notification of Data Breach
- October 9, 2018: Comment to FCC About Robocalls and Spoofing
- October 9, 2018: Second Letter to Facebook
- October 11, 2018: Letter to Google
- December 5, 2018: First Multistate Attorneys General HIPAA Lawsuit
- December 5, 2018: Leadership of Bipartisan Group of Attorneys General on Robocalls