Tougher Privacy and Data Security Protections Coming to North Carolina

Insights
1.25.18

A bi-partisan privacy and data security bill, which will significantly impact companies with North Carolina employees, is in the works. North Carolina State Representative Jason Saine (R), Appropriations Chairman of Information Technology, has joined with North Carolina Attorney General Josh Stein (D) to strengthen protections against identity theft in North Carolina. The unique pair are co-authoring a bill titled, "The Act to Strengthen Identity Theft Protections" (the "Bill"). Through the Bill, the authors desire to provide stronger protections, while at the same time avoid hampering innovation in the private sector.

Although a draft is currently unavailable, Rep. Saine and Attorney General Stein announced details of the Bill on January 8, 2018. They plan to seek its introduction in both chambers of the North Carolina General Assembly in May.

The Bill will implement noteworthy changes to North Carolina's existing Identity Theft Protection Act, N.C. Gen. Stat. § 75-60, *et seq.* If passed, the changes will impact the way companies address personally identifiable information ("PII") they maintain on their customers and employees. The Bill will propose changes aimed at curbing data breaches, increasing consumer protection post-breach, and providing for greater consumer control over PII. Although the Bill will propose a myriad of changes, employers with employees in North Carolina should pay close attention to two changes, which could prove costly: (1) the imposition of an affirmative duty to implement and maintain data security procedures and practices; and (2) a 15-day breach notification window.

Affirmative Duty to Implement and Maintain Security Program

According to its authors, the Bill contains a provision which will impose an affirmative duty on businesses that own or license PII to implement and maintain ***reasonable security procedures and practices*** to protect the information from a security breach. If this provision becomes law, all companies that maintain PII on North Carolina customers or employees will have to evaluate their data security and privacy programs to ensure they meet the proposed "reasonableness" standard. Many other companies that have not given serious thought to such programs will have to create, implement, and begin to maintain them. Failure to abide by this new duty could prove costly.

Under the proposed law, companies who suffer a breach and have failed to maintain reasonable security practices will have committed a *per se* violation of the North Carolina Unfair and Deceptive

Trade Practices Act, N.C. Gen. Stat. § 75-1.1, *et seq.* Moreover, each person affected by the breach would represent a separate and distinct violation of the law. This would prove harsh as the Unfair and Deceptive Trade Practices Act provides for treble damages and attorneys' fees, even when actual damages are nominal. As you can imagine, this would make breach cases much more attractive to plaintiff's counsel.

15-Day Breach Notification Window

The other significant change being sought is the time within which entities must notify affected individuals and the North Carolina Attorney General's office in the event of a data breach. The current Identify Theft Protection Act generally requires companies to notify affected individuals and the Attorney General without "unreasonable delay." The new law would substantially alter this to require that companies provide those notifications within ***15-days*** following discovery or notification of a breach.

15-days is a very tight timeframe. It will require companies to be vigilant in developing and implementing effective privacy and data security programs, which allow for rapid internal discovery and internal and external reporting of data breaches. In order to meet this new notification deadline, companies will have to stay on top of potential breaches and have a plan in place before one occurs. Gone will be the days of waiting until a breach has occurred to determine your plan-of-attack.

Other Important Changes

Changes to Breach and PPI Definitions

The proposed Bill will update the definition of security breach to include Ransomware attacks. The current definition does not cover such events. It only applies to PII that is acquired, not assessed like data in a Ransomware attack. Thus, if adopted, the new law would require companies to notify both affected individuals and the North Carolina Attorney General within 15-days of a Ransomware attack.

The Bill would also broaden the definition of PII to include medical information and insurance account numbers. As such, the type of data companies must protect would increase.

Additional Consumer Protections

In addition to the proposed 15-day notification window, the Bill is slated to contain other consumer protection provisions. For example, the outline of the Bill calls for consumers to be able to more easily freeze their credit reports for free. Consumer reporting agencies, like Equifax, would be required to create a "simple, one-stop shop for freezing and unfreezing a consumer's credit reports across all major consumer reporting agencies without any additional action by the consumer."

Individuals would also have greater access to free credit reports following a breach. If a security breach occurs at a consumer reporting agency, that agency will have to provide five years of free credit monitoring to affected individuals.

Finally, the changes would provide individuals with greater access to and control over their personal data. A company that wanted to use someone's credit report or score would need that person's permission and would have to disclose the reason for seeking access to the information. A consumer would also be entitled to request from a consumer reporting agency a listing of the information maintained on him or her, both credit related and noncredit related, its source, and a list of any person or entity to which it was disclosed.

What Should Employers Do?

As mentioned above, Rep. Saine and Attorney General Stein intend to introduce the Bill this May. Once introduced, employers should seek counsel to analyze the intricacies of the Bill and provide an evaluation of its potential impact on their organizations. Given the bi-partisan support touted, some version of the Bill will likely become law. Affected employers should thus closely monitor the Bill though the North Carolina General Assembly.

Employers, however, should not wait to begin evaluating their internal privacy and data security programs. If your company has a privacy and data security program, audit it now. If it does not, develop one immediately, as you are already behind the eight ball.

If you would like more information on developing and implementing privacy and data security programs, please contact us. In the unfortunate even you need it, we also have extensive experience in guiding organizations through data breaches and representing clients in data breach litigation.