Strict Privacy and Data Security Bill Introduced in North Carolina

Insights
5.13.19

Early last year, I posted about tougher, bi-partisan privacy and data security legislation in the works in North Carolina. North Carolina State Representative Jason Saine (R), Senior Appropriations Chair, teamed-up with North Carolina Attorney General Josh Stein (D) and issued a fact sheet outlining what the new legislation would include.

Finally, on April 16, 2019, Representative Saine (R), Senior Appropriations Chairman, House Deputy Majority Leader Brenden Jones (R), and House Deputy Democratic Leader Robert Reives, II (D) introduced that legislation as H.B. 904 (the "Bill"). As predicted, this Bill, if passed, will significantly impact companies with North Carolina employees.

The Bill will implement noteworthy changes to North Carolina's existing Identity Theft Protection Act, N.C. Gen. Stat. § 75-60, *et seq.* The proposed changes will impact the way companies address "personal information" 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 personal information. Although the Bill will propose a myriad of changes, employers with employees in North Carolina should pay close attention three changes, which could prove costly: (1) the imposition of an affirmative duty to implement and maintain data security procedures and practices; (2) a 30-day breach notification window; and (3) the N.C. Attorney General's statutory right to require production of certain information.

Affirmative Duty to Implement and Maintain Security Program

As promised, the Bill contains a provision which will impose an affirmative duty on businesses that own or license personally identifiable information 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 personal information 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 plaintiffs' counsel.

30-Day Breach Notification Window

Another 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 ***30-days*** following discovery or notification of a breach.

30-days is better than the 15-days originally proposed in the 2018 Fact Sheet. Nonetheless, this is still a very tight timeframe. In fact, it would align North Carolina with the most strict notification period in the Country. Companies will have to be on top of their game. Waiting until a breach occurs to determine your plan-of-attack will no longer suffice. Such a short notification window 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.

Information and Documents the Attorney General May Request

The Bill also spells-out specific information and documents the Attorney General's office may request following a breach. Of particular interest, the Bill would allow the Attorney General to obtain a description of the policies in place regarding breaches, steps taken to rectify the breach, a summary of the incident report, and a summary of the computer forensics report, if a forensic examination was undertaken. This means that in the future the Attorney General's office will likely be requiring the production of much more detailed information than in the past.

As such, companies should not wait to implement or revisit their data security and privacy policies, including incident response plans. Moreover, with the Attorney General's ability to request "a summary of the incident report" and a summary of any computer forensics report, teaming up with outside counsel at the beginning of any incident will be imperative to ensure that vital communications and documents are privileged.

Other Important Changes

Changes to Breach and Personal Information Definitions

The Bill will update the definition of security breach to include mere access to personal information. The current law only applies to personal information that is acquired, not accessed 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 30-days of personal information being accessed.

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

Documentation of Risk of Harm Assessments

Like most states, North Carolina's current law requires that there be a "risk of harm" before a breach notification obligation is triggered. In order for a data breach to constitute a reportable "security breach", it must be one where "illegal used of the personal information has occurred or is reasonably likely to occur or ***that creates material risk of harm to the consumer***." Companies determining that a data breach does not meet these elements, and thus does not require notification under law, must document the reasons for reaching that conclusion and maintain such documentation for a least three years. Several other states have similar documentation requirements.

Additional Consumer Protections

In addition to the proposed 30-day notification window, the Bill also contains other consumer protection provisions. For example, companies would be required to offer at least two years of credit monitoring to affected individuals following a breach involving their Social Security numbers.

The Bill also calls for consumers to be able freeze their credit reports for free and more easily. 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?

It does not appear that the Bill will become a law this legislative session, as it has not yet made it out of committee and the crossover deadline (deadline for bills to pass over to the N.C. Senate for consideration) has passed. The Bill, however, will be back, and absent some unlikely national privacy legislation, employers should be prepared for its passage. In the short term, employers should seek counsel to analyze the intricacies of the Bill and provide an evaluation of its potential impact on their organizations.

Employers should also evaluate 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 curve.

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