WOMBLE BOND DICKINSON

Client Alert

April 26, 2019

Bill Introduced to Expand NC's Data Protection Laws, Creating New Cybersecurity Obligations and Liability Risk for NC Businesses

NC Attorney General Josh Stein announced during a press conference in January that efforts were underway to expand NC's data protection laws and enforcement in response to the growing number of corporate data breaches affecting NC residents. As promised, on April 16, 2019, Representative Jason Saine and other lawmakers introduced House Bill 904 (HB 904) to amend the North Carolina Identity Theft Protection Act, N.C. Gen. Stat. §§ 75-61 et seq. If adopted, their proposed amendments would substantially increase the data security and breach notification obligations for NC businesses holding any personal information and for other businesses holding the personal information of NC residents.

New affirmative data security obligations

Outside of the healthcare and financial services sectors, many businesses in NC have never had to comply with affirmative legal obligations related to cybersecurity. However, consistent with a growing trend nationwide, HB 904 would fill that gap by creating an affirmative obligation for businesses to have reasonable data security. Specifically, HB 904 would require that businesses "[i]mplement and maintain reasonable security procedures and practices, appropriate to the nature of the personal information and the size, complexity, and capabilities of the business, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." If adopted, this could become a significant new area of compliance and liability risk for any company doing business in NC or holding the personal information of NC residents.

Expanded definition of "security breach" triggering the law

Under the current law, the breach notification framework is triggered by an incident involving "unauthorized access to and acquisition" of personal information. Thus, both unauthorized access and acquisition must occur before there is a data breach under the statute. HB 904 would amend that language to read: "unauthorized access to or acquisition" of personal information. This would dramatically increase what would constitute a data breach triggering the notification analysis under the statute. For example, this broader definition might reach any incident of mere unauthorized access to a company's computer network storing personal information.

Record-keeping obligation even for harmless security breaches

In such situations of unauthorized access to or acquisition of personal information, the company would become obliged to conduct an investigation to determine whether the cybersecurity incident may result in illegal use of personal information or create some other material risk of harm to a consumer – thus triggering consumer notification and other obligations. Even if the company found no material risk of harm, another amendment proposed by HB 904 would require the company to document this determination and maintain it for at least three years. This would create yet another due diligence and record-keeping obligation that is designed to enable official scrutiny of the company's data security practices.

Accelerated timeline for data breach notification

Under the current law, breach notification must be made "without unreasonable delay" to affected individuals and the Consumer Protection Division of the NC Attorney General's Office. HB 904 would replace that flexible language with a far more stringent requirement to provide notification "as soon as practicable, but not later than 30 days after discovery of the breach or reason to believe a breach has occurred." Even in those situations where notification can be delayed based on a law enforcement request for confidentiality, HB 904 would require that the notification be provided "within five days" after the law enforcement agency indicates that the notification will no longer impede their criminal investigation or jeopardize national security. With such a rapid timeline for breach notification – triggered by as little as "reason to believe a breach has occurred" – businesses will need to have an effective breach response strategy put in place before they face the next cybersecurity incident.

Broader notification to the Attorney General and requests for evidence

Under the current law, a company must notify the Consumer Protection Division about a data breach in the event that NC residents are notified under the statute. This disclosure must cover "the nature of the breach, the number of consumers affected by the breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice."

Consistent with its imposition of affirmative data security obligations, HB 904 would add a requirement to provide breach notification to the Consumer Protection Division that is independent of notification to NC residents. Thus, a company doing business in NC which experienced a data breach of personal information of non-NC residents would still have an obligation to notify the Consumer Protection Division within 30 days.

In another move signaling more aggressive enforcement, HB 904 also would specifically empower the Consumer Protection Division to request specific types of evidence about the data breach, including a description of the policies in place regarding breaches, steps taken to rectify the breach, a copy of the police report, a summary of the incident report, and a summary of the computer forensics report, if a forensic examination was undertaken. Of course, such evidence might then be used in an enforcement action arising out of the incident.

Requirement to provide credit monitoring services

Added to breach notification, for a security breach involving social security numbers or any security breach by a consumer reporting agency, HB 904 would require the business to provide 24 months of credit monitoring services to the affected individuals. The current law, by contrast, does not require the provision of credit monitoring services. HB 904 would also create a framework whereby an individual could make a single request for a security freeze that would apply to all credit reporting agencies, who must implement that security freeze free of charge.

Amended definition of "personal information"

HB 904 would add two more categories of information to the definition of "personal information" under the statute: (1) health insurance policy numbers, subscriber identification numbers or any other unique identifiers used by a health insurer or payer to identify a person; and (2) any information regarding an individual's medical history or condition, medical treatment or diagnosis, or genetic information, by a health care professional. Notably, the bill also provides that entities covered by HIPAA would be deemed compliant with NC's breach protection requirements if they comply with HIPAA's requirements.

Furthermore, HB 904 would carve out identification names and parent's legal surname prior to marriage from the definition of "personal information." Electronic identification numbers and email addresses would also be excluded unless the breach includes the security code or password allowing access to the individual's financial account or resources or other personal information. Passwords would be excluded as well unless they enable such access.

HB 904's proposed amendments to NC's data breach law are consistent with a larger national trend toward more stringent data security and breach notification requirements. NC businesses and any business holding the personal information of NC residents should be prepared to enhance their data security compliance program accordingly – or begin implementing one if they have not already. In particular, business should identify their personal information or other sensitive data subject to security requirements, and then develop and maintain a written incident response plan to be able to handle data breaches effectively.

A violation of NC's data breach law would still be enforced as a violation of the North Carolina Unfair and Deceptive Trade Practices Act, and it would be subject to a private cause of action if the plaintiff can show that "injury" occurred as a result. Such a lawsuit would expose a business to treble damages and attorney's fees, in addition to compensatory damages.

Allen O'Rourke
Of Counsel

+1 704.350.6357
allen.orourke@wbd-us.com

Taylor Ey
Associate

+1 919.484.2306
taylor.ey@wbd-us.com