NORTH CAROLINA ATTORNEY GENERAL PROPOSES STRINGENT DATA BREACH LEGISLATION

Date: 20 February 2019

Health Care and Public Policy and Law Alert

By: Gina L. Bertolini, Kenneth M. Kennedy

On January 17, 2019, North Carolina Attorney General Josh Stein (D) and Representative Jason Saine (R) held a press conference announcing plans to introduce legislation that would strengthen North Carolina's Identity Theft Protection Act. [1] This follows a 2018 press conference, during which Attorney General Stein and Representative Saine announced a similar proposal, although this year's version includes a few revisions that likely will make the proposed bill more palatable to the business sector. According to Representative Saine's office, a bill is expected to be introduced this year. [2] Proponents of the bill believe that, once introduced, it will receive broad support, in particular given the bipartisan approach and a strong public interest in protecting the personal and sensitive data of North Carolinians.

In addition to announcing the proposed identity theft legislation at the January 17 press conference, Attorney General Stein also released the *North Carolina Data Breach Report 2018*, which details the nature and quantity of data breaches reported to the North Carolina Department of Justice in 2018. [3] According to Attorney General Stein, 1.9 million North Carolinians were affected by a data breach in 2018, [4] an increase of over 250% over the past decade, signaling that North Carolina's data protection laws, while strong, "need to be even stronger." [5]

Given the prevalence of large data breaches in 2017 and 2018, such as Equifax and Uber, it is not surprising that states like North Carolina are beginning to strengthen data protection laws in an effort to stem the tide of data theft. [6] Such new protections will impact health care providers, which, as an industry, experienced data breaches in 2018 affecting over 9.9 million records nationally — the second largest amount of breaches in 2018 as an industry. Moreover, breaches by health care providers in 2018 had the highest rate of exposure per breach. [7]

THE 2019 VERSION OF "THE ACT TO STRENGTHEN IDENTITY THEFT PROTECTIONS"

North Carolina's current Identity Theft Protection Act requires businesses to notify affected individuals "without unreasonable delay" in the event of a security breach that compromises an individual's personal information. [8] A "security breach" is defined as an incident of unauthorized "access to and acquisition" of unencrypted and unredacted records containing "personal information." Personal information is defined as an individual's first and last name in combination with certain types of sensitive financial or identifying information. [9]

As proposed, the "Strengthen North Carolina Identity Theft Protection Act" (the "Act") would significantly increase consumer protection after a breach by: (1) requiring quicker consumer notification within a set timeframe, (2) creating additional responsibilities for credit reporting agencies related to credit freezes and credit monitoring, and (3) expanding the scope of protected personal information to include medical information, genetic information, and health insurance account numbers. Additionally, the Act would amend the definition of security breach to include any unauthorized access to personal information regardless of whether it was also acquired, which would include ransomware attacks where personal information is accessed but not acquired. [10]

The Act would shorten the breach notification timeframe to 30 days following discovery of a breach, as compared to the current law, which requires entities to report breaches without "unreasonable delay." This is longer than the breach notification period proposed in 2018, which, at 15 days, would have made North Carolina among the shortest breach notification periods in the nation. [11] Additionally, the Act would clarify that any business that suffers a breach while failing to maintain reasonable security measures has committed a violation of North Carolina's Unfair and Deceptive Trade Practice Act ("UDTPA"). [12] This is less onerous than the 2018 proposal, which would have established a separate and distinct violation of the UDTPA for every individual whose data has been compromised. [13]

The Act also would increase post-breach protection for consumers if the breach occurs at a credit reporting agency, such as Equifax, by requiring the agency to provide four years of free credit monitoring to affected consumers (compared to the current industry practice of one year). If a business experiences a breach including social security numbers, the business would be require to provide two years of free credit monitoring. The 2018 proposal required five years of free credit monitoring for consumer reporting agency breaches and would have provided three free credit reports from each consumer reporting agency for consumers affected by a breach.

Like the 2018 proposal, the 2019 iteration would allow consumers to place and lift a credit freeze on their credit report at any time at no charge, and a company seeking to obtain a person's credit report or credit score will require permission and a disclosure of the reason such access is sought. Additionally, consumers will have the right to request a listing of both credit-related and non-credit-related information maintained about the consumer by the consumer reporting agency, including source and a list of any person or entity to whom such information is disclosed.

Some of the proposed changes as compared to 2018 were the result of consultation with relevant stakeholders, including representatives of the business community. Indeed, Representative Saine noted that, over the last year, he has spent "numerous hours working with citizen advocates — like AARP, the Attorney General's Office, and the North Carolina business community, to ensure that this bill will create strong protections for North Carolina's citizens' data. We are strongly committed to getting this right, and creating a strong framework for protecting our most personal information." [14] By curtailing some of the more onerous requirements of the 2018 proposed bill, the current iteration has a greater likelihood of passage, and would still bring North Carolina's data protection laws in line with many of the most demanding in the nation.

WHAT THIS COULD MEAN FOR HEALTH CARE PROVIDERS

The new law, if passed as proposed, would significantly strengthen North Carolina's current data privacy laws, making it one of the more stringent in the nation. In particular:

- By including ransomware attacks within the definition of a breach, North Carolina's approach would be consistent with the Office for Civil Rights' interpretation of the Health Insurance Portability and Accountability Act ("HIPAA")-related ransomware attacks [15] but would be one of the first states in the nation to include ransomware within its definition of breach for notification purposes.
- The 30-day notification period could pose practical challenges for businesses required to provide notice and would be one of the shortest notification periods nationally.
- Similar to HIPAA, which offers no private right of action to affected individuals, current North Carolina data privacy laws offer limited recourse for affected consumers. Under the proposed Act, health care providers experiencing a data breach would be liable under North Carolina's UDTPA if their security measures are not reasonable or if the they fail to provide timely notice. [16] This could create substantial risk for providers, as large data breaches with respect to health data are not uncommon, and merely aligning policies and procedures with HIPAA may not be adequate to stem liability, depending on how the "reasonableness" requirement is interpreted.

If passed, providers conducting business in North Carolina will have increased incentives to ensure that their cybersecurity and data management policies are consistent with evolving privacy and security standards and adhered to by their workforce members, especially if the definition of personal information is expanded to include medical and genetic information, as proposed.

The K&L Gates' health care and food, drugs, medical devices and cosmetics (FDA) practice regularly advises clients in the area of health care data privacy, security, and operational matters and stands ready to assist in assessing the impact of this proposed legislation on their current and future operations.

NOTES:

[1] Press Release, N.C. Dep't of Just., Attorney General Josh Stein and Rep. Jason Saine Announce Legislation to Strengthen Protections Against Identity Theft, News Release (Jan. 17, 2019), https://ncdoj.gov/News-and-Alerts/News-Releases-and-Advisories/Attorney-General-Josh-Stein-and-Rep-Jason-Sain-(1).aspx (hereinafter, "Press Release"). For North Carolina's existing data protection laws, see "Identity Theft Protection Act," N.C.G.S. § 75-60 *et seq.*

[2] Although some news outlets reported inaccurately that a bill called "The Act to Strengthen Identity Theft Protections" was proposed before the North Carolina General Assembly in 2018, there are no records of such bill, and a spokesperson from Representative Saine's office, contacted February 4, 2019, confirmed that it was not introduced in 2018. According to this same spokesperson, the 2019 version currently is being drafted and will be introduced as a bill this year.

[3] N.C. DEP'T OF JUST., NORTH CAROLINA DATA BREACH REPORT 2018, https://ncdoj.gov/Files/News/2018-Data-Breach-Report.aspx.

[4] While the number of North Carolinians affected by a data breach was down 63% in 2018 as compared to 2017, an estimated five million North Carolinians were impacted in 2017 by a single breach — the Equifax breach, which was "one of the most significant security breaches in the American history." Press Release, *supra* note 1.

[5] *Id.*

[6] *See, e.g.,* N.C. DEP'T OF JUST., NORTH CAROLINA SECURITY BREACH REPORT 2017, https://ncdoj.gov/CMSPages/GetFile.aspx?nodeguid=2ba9efc3-bee8-4fce-9df7-cd4635a6621c&lang=en-US; Attorney General Josh Stein, Rep. Jason Saine, and AARP North Carolina on proposed measures to increase identity theft protection in North Carolina (Jan. 8, 2018), https://www.facebook.com/NCDOJ/videos/vb.157759274279900/1537201246335689/?type=2&theater.
[7] IDENTITY THEFT RESOURCE CTR, 2018 END OF YEAR DATA BREACH REPORT (Jan. 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINALWEB-V2-2.pdf.
[8] N.C. GEN. STAT. § 75-65.
[9] N.C. GEN. STAT. §§ 75-61 (10), (14), 14-113(b).
[10] Fact Sheet, N.C. Dep't of Just., Strengthen North Carolina Identity Theft Protection Act, https://ncdoj.gov/Files/News/ID-Theft-Act-Fact-Sheet_updated_1-15_final.aspx (hereinafter, "Theft Protection Act Fact Sheet").
[11] Fact Sheet, N.C. Dep't of Just., Act to Strengthen Identity Theft Protections, https://ncdoj.gov/CMSPages/GetFile.aspx?nodeguid=89988b8d-2bbe-4854-bc7f-a77cfc4b38b2&lang=en-US.
[12] N.C.G.S. § 75-1.1 *et seq.*
[13] *Id.* ("A business that suffers a breach and failed to maintain reasonable security procedures will have committed a violation of the Unfair and Deceptive Trade Practices Act and each person affected by the breach represents a separate and distinct violation of the law.")
[14] Press Release, *supra* note 1.
[15] Fact Sheet, U.S. Dep't of Health & Hum. Servs., Fact Sheet: Ransomware and HIPAA, https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.
[16] Theft Protection Act Fact Sheet, *supra* note 10.

KEY CONTACTS

GINA L. BERTOLINI
PARTNER
RESEARCH TRIANGLE PARK
+1.919.466.1108
GINA.BERTOLINI@KLGATES.COM

KENNETH M. KENNEDY
ASSOCIATE
RESEARCH TRIANGLE PARK
+1.919.314.5630
KENNETH.KENNEDY@KLGATES.COM

