THE
NATIONAL LAW REVIEW

Cyber Bulletin: Cyber-Related Legislation and Litigation- July 2017

Friday, July 7, 2017

Federal Legislative and Regulatory Update

OCR Issues Cyberattack Response Checklist for HIPAA Covered Entities

Article By Christopher F. Petillo
Stephen A. Serfass
Drinker Biddle & Reath LLPPublications

Communications, Media & Internet
Election Law / Legislative News
All Federal

The Department of Health and Human Services' Office of Civil Rights (OCR) issued a checklist in June for HIPAA covered entities and business associates to use as a guide following a cyberattack. In doing so, OCR joins a host of other federal agencies that have issued similar guidance, including the Federal Trade Commission, which issued more robust guidance in September of last year. (OCR has also issued monthly newsletters on cyber issues generally since February 2016.) The OCR guidance contained the following four considerations, most of which relate to key regulations implementing HIPAA.

(1) Execute response and mitigation procedures and contingency plans

Among the first steps OCR wants businesses to take immediately upon learning of a cyberattack is to disrupt any further disclosure of protected health information (PHI) that may have occurred as a result of the incident. Implicit in the first checklist item is a reminder for covered entities to ensure they have established and implemented contingency plans for emergencies, as required by HIPAA's Security Rule, including data backup plans, disaster recovery plans, and emergency mode operation plans. *See* 45 C.F.R. § 164.308(a)(7). Of course, covered entities and their business associates should also ensure that they conduct periodic risk analyses[1] and implement preventative measures to help protect the integrity of key business data and PHI. *See generally* 45 CFR Part 160 and Part 164, Subparts A and C (HIPAA's Security Rule).

(2) Report the event to law enforcement agencies

The checklist also encourages victims of cyberattacks to involve local, state and federal authorities, as necessary. The Privacy Rule specifically permits covered entities to make such reports. *See generally* 45 C.F.R. § 164.512. At the same time, OCR reminds us that the ability to disclose PHI to law enforcement is not unlimited. Companies should therefore ensure that any disclosure is appropriately circumscribed, *i.e.*, consistent with the specific exception to the HIPAA Privacy Rule that the company is relying on to make the disclosure.

(3) Report all cyber threat indicators to federal and information-sharing and analysis organizations (ISAOs)

The third guideline strongly encourages covered entities to share cyber threat indicators with governmental entities that collect and analyze information related to cyberattacks to better understand and prevent such attacks. OCR cautions that disclosures to ISAOs should not include PHI unless the disclosure falls within an exception to the HIPAA Privacy Rule. As companies heed this advice, it is important to consider the provisions of the Cybersecurity Information Sharing Act of 2015, which OCR cites in the checklist and which outlines certain steps that must be taken before sharing cyber threat indicators with an ISAO—*e.g.*, scrubbing PHI before sharing.

(4) Report the Breach to OCR and affected individuals ASAP

Finally, OCR reminds covered entities of their obligation to notify OCR and affected individuals following a breach

of unsecured PHI—assuming the covered entity has determined that the cyber incident resulted in a "breach" as defined under HIPAA. If, when and to whom such notifications must be made are outlined in the HIPAA Breach Notification Rule. *See* 45 C.F.R. § 164.402-414.

Certainly, the informal guidance issued by OCR is helpful information. Its issuance also serves as a gentle reminder from OCR to covered entities and business associates to review their breach response plans and ensure that their policies and procedures follow the letter and spirit of the regulations implementing HIPAA. And, even if the regulations do not necessarily require the steps outlined above (*e.g.*, sharing of cyber threat indicators with ISAOs), the HIPAA Enforcement Rule contains both aggravating and mitigating factors OCR may consider in devising punishments for non-compliance with HIPAA. That is, implementing such informal guidance into company policies and procedures will help demonstrate a culture of compliance and place the company in a better position if it finds itself defending the actions it took in the wake of a cyberattack.

President Signs Cybersecurity Executive Order

President Donald Trump signed an executive order on May 11, 2017, calling for the strengthening of the cybersecurity of federal networks and the critical infrastructure of the executive branch. The administration cited the vulnerability of the federal government's aging legacy systems and the rise of global political cybersecurity threats, most notably from Russia and China, as the purpose of the order. The order seeks to hold heads of executive departments and agencies accountable for managing their respective departments' cybersecurity risks "commensurate with the risk and magnitude of the harm" resulting from any unauthorized access, use, or disclosure, among other misappropriations of critical information. The order also requires agencies to follow the NIST standards (The Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of Standards and Technology) in devising their risk management programs. In short, this executive action demonstrates that the Trump administration will continue the federal government's commitment to address the increasing cybersecurity risks that significantly affect the global political landscape.

Notably, President Trump's executive order has been accompanied by a similar impetus to improve national cyber resiliency from Congress over the last year. Already, more bills have been introduced in Congress concerning cybersecurity issues than in years past, many of which affect the private sector. For example, Senate Bill No. 536, titled "Cybersecurity Disclosure Act of 2017," was introduced by Rhode Island Democrat Jack Reed to promote transparency in the oversight of cybersecurity risks at publicly traded companies. Senator Reed introduced the bill on March 7, 2017. The bill would require publicly traded companies to disclose whether any member of the governing body (such as the board of directors or general partner) has expertise or experience in cybersecurity. If the company does not have any cybersecurity experts on its board or managing committee, the proposed legislation would require the company to explain why such expertise is not required based on other steps taken by the company. We will continue to monitor the progress of these legislative and administrative developments.

State Legislative Update

NYDFS Cybersecurity Regulation May Serve as Polestar for National Association of Insurance Commissioner's (NAIC) Insurance Data Security Model Law

Early this year, the New York Department of Financial Services (NYDFS) implemented new cybersecurity requirements for entities that require a license or similar authorization under the New York Banking Law, the Insurance Law, or the Financial Services Law. The first-of-its-kind regulation sets forth specific standards covered entities (as defined in the regulation, not as used in HIPAA) must follow in administering a cybersecurity program, and includes guidelines ranging from the scope of the risk analysis entities must conduct to the timing for reporting a cybersecurity incident to the NYDFS (72 hours). Although the regulation requires companies to specifically consider adoption of certain security protocols (encryption key among them), the regulation itself reflects a risk-based approach and provides companies some flexibility to comply with its mandates.

Although most New York-governed entities are likely aware of the regulation, businesses that do not have New York operations should know that there is a strong push among state regulators and intergovernmental entities like the NAIC to use the New York cybersecurity regulation as the model for other similar regulatory enactments. Included among such regulations is the NAIC Insurance Data Security Model Law, which has been under development and consideration by the NAIC Cybersecurity Working Group for more than 18 months. During the Working Group's meeting on April 9, 2017, at the NAIC National Spring Meeting in Denver, Superintendent Maria Vullo of New York presented on the NYDFS regulation. After hearing the presentation, the Working Group acknowledged the shortcomings of the then-current draft of the Model Law and proposed using New York's risk-based approach as a basis to redirect their Model Law drafting efforts.

The latest version of the Model Law, released on April 26, 2017, reflects these intentions. The revisions are

particularly noticeable in Sections 3.H-J, Section 4.F, and Section 6.A of the model law. For example, the updated terms and definitions in Section 3 ("multi-factor authentication," "nonpublic information," "publicly available information," "information systems" and "cybersecurity event") all borrow specific language from the NYDFS regulation.

Companies outside of New York should begin considering what it would take to comply with the NYDFS cybersecurity regulation, as all indications show that regulation could become the prevailing standard in many states in the months and years ahead.

New Mexico Enacts Data Breach Notification Act

New Mexico is the latest state to join the ranks of states (now up to 48) that have enacted a data breach notification law. HB 15 was signed into law on April 6, 2017, codifying New Mexico's Data Breach Notification Act (the "Act"). The Act became effective on June 16, 2017.

The Act requires notice of a breach to affected New Mexico residents no later than 45 days after discovery of the breach. If the breach affects more than 1,000 New Mexico residents, the New Mexico Attorney General and certain consumer reporting agencies must be notified as well. Notification need not be made, however, if the company determines that the breach does not give rise to a significant risk of identity theft or fraud. Notification may also be delayed if requested by law enforcement, if the scope of the breach is still being determined, or to restore the integrity and confidentiality of the data system affected. Importantly, third-party service providers are required to inform the owner or licensor of a data breach within 45 days of the discovery of the breach.

The following provisions are also of note:

- Entities subject to the Graham-Leach-Bliley Act or HIPAA are exempt;
- The definition of "personal identifying information" includes biometric information (*e.g.*, fingerprints, retina/iris), which follows a trend of states that have enacted laws targeting risks created by the continued use of biometrics (the one receiving the most attention is probably Illinois' Biometric Information Privacy Act);
- PII must be erased, shredded, or made unreadable if it is no longer "reasonably needed"; and
- The law also requires implementations of reasonable security procedures, and contracts with third-party providers must require the third parties to similarly implement such procedures.
  With this development, Alabama and South Dakota are the only states left that have not enacted security breach notification statutes.

Cyber Litigation Update

District Court Grants Motion to Dismiss Class Action with Prejudice in *In re Barnes and Noble Pin Pad Litigation*, Case No. 12-08617 (N. D. Ill.)

On June 13, 2017, Judge Andrea Wood of the U.S. District Court for the Northern District of Illinois granted Barnes & Noble's motion to dismiss the second amended complaint filed by a putative class of Barnes & Noble customers who claimed that their personal identifying information (PII) had been stolen. The decision represents the third time the court has dismissed the case. This time, however, the court dismissed the case with prejudice, ending the litigation (absent an appeal to the 7th Circuit).

The case arose in September 2012 when a group of hackers installed "skimmers"[2] on PIN pad terminals at 63 Barnes & Noble locations. Six weeks after discovering the skimmer scheme, Barnes & Noble informed all potentially affected customers of the breach (notably, Barnes & Noble delayed notification by several weeks at the request of law enforcement). Plaintiffs, customers of affected Barnes & Noble stores during the time of the breach, filed a putative class action on March 25, 2013.

The plaintiffs initially asserted five claims: (1) breach of contract; (2) violation of the Illinois Consumer Fraud and Deceptive Business Practices Act , 815 ILCS § 505/1 et seq.; (3) invasion of privacy; (4) violation of the California Security Breach Notification Act, Cal. Civ. Code § 1798.80 et seq.; and (5) violation of California's Unfair Competition Act, Cal. Bus. & Prof. Code § 17200 et seq. These claims were generally predicated on Barnes & Noble's untimely provision of notice of the breach. The plaintiffs sought damages for, *inter alia*, the lost value of their PII, expenses incurred in mitigating the increased risk of identity theft, anxiety, and emotional distress.

The court dismissed the first complaint for lack of standing on September 3, 2013. Plaintiffs filed an amended complaint on September 24, 2013. On October 3, 2016, although the court found that plaintiffs had cured the

standing deficiency,[3] it dismissed the amended complaint because the plaintiffs failed to state a claim by not pleading economic or out-of-pocket damages. The court recognized that one of the class representatives alleged that he purchased credit monitoring as a result of the breach, the court found causation between the purchase of credit monitoring and notice of the breach lacking, as that plaintiff alleged she purchased credit monitoring in the past and admitted that her renewal of the credit monitoring service was only partially motivated by Barnes & Noble's (allegedly untimely) notice of the breach.

In response, the plaintiffs filed a second amended complaint (SAC) on October 31, 2016. The SAC omitted the invasion of privacy claim and included the following damages theories: (1) unstated harm flowing from an inability to access a bank account because it was put on hold; (2) unstated harm flowing from the inability to use affected credit cards until a new one was delivered; (3) time spent with police officers and bank employees to discuss the breach; (4) the cost of cell phone minutes used to communicate with the banks issuing the cards; (5) lost value of PII; and (6) notification of the breach was the "decisive factor" in renewing credit monitoring services.

Notwithstanding these amendments, the court dismissed the SAC because the plaintiffs still failed to allege damages sufficient to state any of their claims. Specifically, the court found that each of the claims required "out-of-pocket" or economic damages sufficient to state each claim, a standard that most of the damages allegations in the SAC failed to meet. For example, the value of PII, the inconvenience in resolving issues with their banks, and emotional distress all lacked any pecuniary impact. The court also relied upon plaintiffs' inability to plead any monetary harm suffered by the plaintiffs who alleged an inability to use bank accounts and credits cards for a finite period of time. Although the court noted one plaintiff alleged costs associated with accumulated cell phone minutes were economic-like damages, these costs were *de minimis* and too attenuated from the claims—which were based on delayed notification of the breach—to meet the pleading standards. Finally, the court was not persuaded by one plaintiff amending her reason for renewing credit monitoring service reason from the security breach "only [playing] a part" in the decision to the security breach being the "decisive factor" for the renewal. Moreover, the court noted that even if the security breach was the reason for renewing the credit monitoring services, it would not be a redressable injury under the claims brought in the lawsuit. Consequently, the court dismissed the case with prejudice based on the plaintiffs' inability to plead injuries sufficient to state a claim.

The company's success on a motion to dismiss in a data breach class action is significant in its own right, but also demonstrates that the threshold for alleging damages for purposes of stating a claim can often be higher than the threshold needed to allege damages sufficient to confer standing—a typical battleground between plaintiffs and defendants in data breach class actions, especially following the Supreme Court's decisions in *Clapper* and *Spokeo*. (Earlier editions of the Drinker Biddle Cyber Bulletin addressed some of the significant decisions on standing.) *Barnes & Noble* should prove useful in illustrating this point and is a must-cite decision in cases where the damages allegedly incurred by data breach victims are *de minimis*; where plaintiffs rely on reimbursable credit card charges or credit monitoring services; and/or where there are no allegations showing that affected individuals have suffered actual identify theft or fraud.

1The HIPAA Security Rule does not outline how often a risk analysis must be conducted. Rather, the HIPAA Security Rule requires companies to conduct an analysis "as needed." See 45 C.F.R. §§ 164.306(e) and 164.316(b)(2)(iii). Each covered entity's needs are different, but conducting a risk analysis annually and contemporaneous with any material change to company networks, electronic systems, or procedure is a good baseline.

2A skimmer is a general term describing any device or software used to siphon PII from a variety of sources, including creating a duplicate ATM card reader that can copy credit card information when it is inserted into the reader; or creating fake credit cards that, when inserted into a credit card machine, install malware into the machine permitting hackers access into the payment system. In the case of Barnes & Noble, the hackers installed bugs in the point-of-sale credit card machines, which permitted access to the PII of Barnes & Noble customers.

3The court relied on the facts that the hackers used the skimmers to specifically obtain PII of Barnes & Noble customers; the plaintiffs were among the potentially affected individuals because they used credit cards at the stores affected during the time period in which the hack was executed; the hackers made unauthorized charges on the stolen cards (even though such charges were reimbursable); and the plaintiffs had taken steps to protect their identity after learning of the breach. These allegations were deemed to be sufficient to satisfy the "injury in fact" requirement of the standing analysis.