Bond

INFORMATION MEMO
CYBERSECURITY AND DATA PRIVACY

AUGUST 6, 2019

New York Significantly Expands Breach Notification Law

Since 2005, New York State has required businesses operating in the State to report the breach of customers' and employees' private information to individuals affected by the breach and to state authorities.[1] On July 25, 2019, Governor Cuomo signed the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) into law. The SHIELD Act extends the information covered and the reach of New York's breach notification act beyond entities that conduct business in the State to all persons and businesses that possess computerized information about New York State residents. Changes go into effect on October 23, 2019.

The SHIELD Act also made significant changes to the cybersecurity landscape both within and outside of the State by setting minimum cybersecurity requirements for businesses and persons in possession of private information about New York State residents. This memorandum focuses on the changes in the breach notification requirements. A companion memorandum discusses the new cybersecurity practices mandated by the State.

Expanded Scope for the Breach Notification Law

Prior to the SHIELD Act, New York's Breach Notification Law, codified at General Business Law § 899-aa and State Technology Law § 208 (the Breach Notification Law), applied only to businesses and persons that conducted business in New York and "State Entities,"[2] respectively. The SHIELD Act expands coverage by eliminating the requirement that all entities, both for profit and not-for-profit (Business or Businesses) or a person "conduct business in New York," subjecting any out-of-state entities that own or license personal information about New York State residents to the SHIELD Act's mandates.

As with the security requirements, the SHIELD Act recognizes the existence of other regulatory schemes and their overlapping applicability. Thus, it relieves entities that provide notice in accordance with other laws or regulations from the reporting obligations under the Breach Notification Law. For example, entities that report a breach to individuals and the specified regulatory authorities under New York's Department of Financial Services regulations (DFS Cybersecurity Rule) or Health Insurance Portability and Accountability Act (HIPAA) are no longer required to separately comply with the notification requirements of Breach Notification Law.[3]

Expanded Definition of Private Information

Under the prior provisions of the Breach Notification Law, private information was defined as computerized copies of social security numbers, drivers' license numbers, account numbers and credit card numbers (Private Information). The duty to notify individuals about the release of credit card and account numbers was triggered only if the numbers were released in combination with passwords, security codes or other access codes that would permit their actual use.

The SHIELD Act expands the definition of private information to include account numbers, credit card numbers and debit card numbers that could be used without any additional identifying information, security code or password, as well as biometric data (finger prints, voice prints, retina or iris images, or other unique data used to ascertain or authenticate a person's identity). Notably,

1 State authorities to be notified are the Attorney General, Department of State and State Police.

2 State entities include state boards, bureaus, divisions, committees, commissions, councils, departments, public authorities, public benefit corporations, offices or other governmental entities performing governmental or proprietary functions for the state of New York, but do not include the judiciary or cities, counties, municipalities, villages, towns and other local agencies.

3 If breach notifications are made pursuant to an industry specific regulation, the party making the notification must still notify the New York Attorney General, Department of State and State Police. A breach notification to the Secretary of Health and Human Services under HIPAA must be followed up within five days with notification to the New York Attorney General.

user names or e-mail addresses in combination with a password or security question and an answer that would allow access to a person's online account now also fall under the ambit of Personal Information under the Act.

Breach Definition Expanded

Until amended by the SHIELD Act, the Breach Notification Law provided that a breach was the "unauthorized acquisition or acquisition without valid authorization" of Private Information, which implied that the unauthorized person had to download a copy of the information or otherwise take possession of it. As amended by the SHIELD Act, notice to individuals affected and state authorities is required in the event of unauthorized access, even if the Private Information is not acquired or exfiltrated from the computer system.

The SHIELD Act also updated the guidance that Businesses and individuals should use to determine when Private Information was acquired. A Business or a person must have a "reasonable belief," which belief might be informed by considering whether the Private Information was on a lost or stolen device, whether there was evidence that the information was downloaded or copied, and whether affected persons whose information was believed to have been acquired reported identity theft. Now that Businesses must report unauthorized access, not just acquisition, they must consider indications that "information was viewed, communicated with, used or altered" by an unauthorized person. Inherent in this requirement is the capacity of Businesses to track access and conduct a forensic investigation in the aftermath of a breach to determine which information in their computer systems was accessed, by whom and with what credentials.

Clarification on Reporting Requirements

While the SHIELD Act expanded the Breach Notification Law to require reporting of unauthorized access, it does not require notice if access to Private Information was inadvertent, and the Business or person determines that exposure is not likely to result in misuse of such information or cause financial harm to affected individuals. When Businesses and persons make these determinations, they must now document them and maintain that documentation for five years. Determinations made with respect to the inadvertent exposure of Private Information of 500 or more affected individuals must be reported to the Attorney General within ten days after the determination.

Lawsuit by Attorney General

The SHIELD Act expands the time for the Attorney General to commence litigation related to a breach from two years after learning of the breach (usually the date of notification) to three years, but in no event more than six years after the breach occurred, unless the Business took steps to hide the breach. While there is no private right of action under the Breach Notification Law, the Attorney General can seek damages based on "actual costs or losses incurred by a person entitled to notice pursuant to this article, if notification was not provided to such person pursuant to this article, including consequential financial losses." If and when the Attorney General's office considers bringing litigation, it will undoubtedly take into account a Business's compliance with the additional cybersecurity requirements of the SHIELD Act, codified at N.Y. Gen. Bus. Law § 899-bb, which go into effect on March 21, 2020.

If you have any questions about the SHIELD Act, contact Tracy E. Miller, Co-Chair of the Cybersecurity and Data Privacy Practice, Curtis A. Johnson, a member of the Practice Group, or the attorney in the Firm with whom you are regularly in contact.

BOND SCHOENECK & KING ATTORNEYS