New data privacy laws broaden protections for NY residents and impose major obligations on organizations

Dominic A. Paluzzi | Thursday, September 12, 2019

On July 25, 2019, Gov. Andrew Cuomo signed the "Stop Hacks and Improve Electronic Data Security Act" (SHIELD Act) and the Identity Theft Protection and Mitigation Services Act into law. Together, these laws broaden protections for New York residents while imposing significant obligations on businesses and organizations. Below is an overview of the requirements for these recently enacted laws and information to make sure your organization is prepared to comply.

The SHIELD Act

Effective March 21, 2020, the SHIELD Act broadens the existing New York data breach law and incorporates additional requirements for businesses holding the personal information of at least one New York resident. The SHIELD Act revises the state data breach law in the following significant ways:

- **Expands the definition of "breaches" requiring notification to include incidents in which personal information was only accessed.** A "breach of the security of the system" requiring notification under New York law previously required the acquisition of private information. With the passage of the SHIELD Act, the term is expanded to include incidents where such private information is only "accessed," a lower standard for notification. This will require notification even when private information is merely accessed, even if it is not acquired.

- **Expands the definition of "private information" to include biometric information, user name or email address with a password, and an account, credit or debit card number without a security code.** Previously New York only considered a Social Security number, driver's license number or non-

driver identification, and account number, credit or debit card number in connection with a security code access code or password to be data elements amounting to "personal information." The SHIELD Act broadens that definition, including the following data elements as "personal information" requiring notification when breached:

- Biometric information.
- User name and e-mail address in connection with a password or security question answer that would permit access.
- An account, credit or debit card number without a security code, if the account number alone is sufficient to allow access to the account.

This brings the New York law into congruence with some of the more modern data breach statutes in the country.

- **Creates a risk of harm analysis for inadvertent disclosure.** The SHIELD Act does not require notice if the exposure of private information was an inadvertent disclosure and there is a reasonable determination that the disclosure will not likely result in misuse or financial or emotional harm. Considering the significant number of breaches that are inadvertent disclosures, this could lighten the requirements of many businesses. However, the SHIELD Act does not get rid of all obligations for such breaches. Instead, it requires the determination to be documented and maintained for at least five years and, if more than 500 residents of New York are affected, the written determination must be provided to the New York Attorney General within 10 days.

- **Requires notification to statute regulators if notification is made pursuant to other laws.** The SHIELD Act exempts businesses making notification pursuant to the Gramm-Leach-Bliley Act, or the Health Insurance Portability and Accountability Act, or any other federal or New York state data security rules and regulations from notifying residents pursuant to New York law. Although this is in line with many other data breach statutes, the SHIELD Act requires notification to the state attorney general, the department of state and the division of state police when notification is made to New York residents pursuant to these laws. Further, the SHIELD Act also requires notification to the New York attorney general within five days of a business notifying the Secretary of Health and Human Services of a breach pursuant to the Health Insurance Portability and Accountability Act.

- **Adds additional disclosure requirements to notifications.** Requires notifications given under the statute to include additional information, including the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information. This will require notifying entities to ensure that they include contact information for the relevant New York agencies on its notification letter.

- **Requires persons or businesses to maintain certain data security protections.** The SHIELD Act requires businesses that owns or licenses computerized data including the privacy information of a resident of New York to develop, implement, and maintain reasonable safeguards. The SHIELD Act lays out specific requirements that are considered "reasonable," the totality of which deems a business to be in compliance. These requirements include, among other things a data security program with

reasonable technical and physical safeguards. The failure to establish these safeguards could expose the business to potential administrative actions.

The Identity Theft Protection and Mitigation Services Act

Effective Sept. 23, 2019, the Identity Theft Protection and Mitigation Services Act requires the following:

- **A credit reporting agency that has suffered a breach that includes any Social Security number must offer at least five years of credit monitoring.** Under the recently enacted law, any credit reporting agency that suffers a breach, as defined under New York state law, that includes a Social Security number must provide at least five years of credit monitoring services to the consumer, at no cost.

- **A credit reporting agency that has suffered a breach must provide information about how a consumer can request a freeze.** In addition, the credit reporting agency must also provide all information required for consumers to enroll in credit monitoring services and how they can request a security freeze at no cost.

Based on these recent changes and the increased interest in data privacy and cybersecurity, we recommend that you ensure that your organization has any and all required policies and procedures in place. McDonald Hopkins' team of experienced data privacy and cybersecurity attorneys can assist your organization with compliance with the SHIELD and Identity Theft Protection and Mitigation Services Acts.

Dominic A. Paluzzi