SULLIVAN & CROMWELL LLP

July 26, 2019

New York Enacts the Stop Hacks and Improve Electronic Data Security Act

New York Amends Data Breach Notification Statute and Requires Businesses to Comply with Reasonable Security Requirements

SUMMARY

On June 17, 2019, the New York State Legislature passed the Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act"),[1] which was signed by Governor Cuomo's office on July 25, 2019. The SHIELD Act amends the New York statute covering notification requirements for unauthorized acquisitions of private information and adds new requirements for businesses and persons that own or license private information of a New York resident to comply with reasonable data security protections. The SHIELD Act will generally take effect within 90 days, with the new requirements for data security protections becoming effective within 240 days.

As detailed below, the SHIELD Act amends New York's notification statute most notably by:

- Broadening the jurisdictional reach to cover any person or business that owns or licenses computerized data including private information of a New York resident, whereas previously the notification statute applied only to a person or business conducting business in New York state;
- Expanding the definition of private information;
- Expanding its scope to apply to unauthorized "access" to personal information and not just "acquisition";
- Excusing notice to affected New York residents if the person or business that is the target of the security breach "reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials";
- Providing that an additional notice to New York residents is not required if notice is made to affected persons pursuant to the breach notification requirements set forth in certain regulatory regimes;

- Enhancing the civil penalties for knowing and reckless violations to the greater of $5,000 or up to $20 per instance of failed notification, provided that the latter does not exceed $250,000; and
- Extending the statute of limitations to three years after either the date on which the state attorney general becomes aware of the violation, or the date of notice to the state attorney general, whichever is earlier, with an outer limit of six years after the discovery of the breach unless the person or business took steps to hide it.

As described in more detail below, the SHIELD Act also adds new data security requirements for persons or businesses that own or license computerized data of New York residents. Entities already regulated under certain federal and New York state compliance schemes are deemed in compliance with the statute. Separately, a person or business will be deemed compliant with the SHIELD Act's data security requirements upon implementing a data security program with certain reasonable administrative, technical and physical safeguards as set forth below.

KEY PROVISIONS OF THE SHIELD ACT

Applicability

The SHIELD Act extends the applicability of the notification requirements and new data security requirements beyond persons or businesses "conduct[ing] business in New York state" to persons or businesses that own or license computerized data of New York residents.[2] Previously, the notification requirements applied only to persons or businesses conducting business in New York state.

Amendments to Notice Requirements

- ***Definition of Private Information*****.** The SHIELD Act broadens the definition of "private information" to incorporate, in combination with a name, number, personal mark, or other identifier used to identify a natural person, (1) an "account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password"; or (2) biometric information (*e.g.*, fingerprints). Additionally, the SHIELD Act adds to the definition of private information "a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account" (even without a corresponding name or other identifying personal information).[3]
- ***Definition of Breach*****.** In addition to broadening the scope of private information, the SHIELD Act also lowers the standard for "breach of the security of the system" from an "acquisition" standard to an "access or acquisition" standard. In determining whether personal information has been "accessed, or is reasonably believed to have been accessed," a business may consider certain factors, including "indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person."[4]
- ***Disclosure to Residents*****.** The SHIELD Act establishes two new exceptions to the existing requirements to "disclose any breach of the security of the system" to any affected New York resident in the "most expedient time possible and without unreasonable delay[.]"[5]
  - *First*, the SHIELD Act provides that notice to New York residents is not required if the disclosure was inadvertent and "the person or business reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials."[6] However, if the incident affects over 500 New York residents, the written determination must

be shared with the state attorney general within ten days of such determination.[7] Notably, the SHIELD Act does not define the term "emotional harm."

- *Second*, the SHIELD Act provides that an additional notice pursuant to New York's data breach notification statute is not required if notice is made pursuant to certain other breach notification requirements, including (1) the regulations promulgated pursuant to Title V of the Gramm-Leach-Bliley Act[8], (2) the regulations implementing the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[9] and the Health Information Technology for Economic and Clinical Health (HITECH) Act[10]; (3) the New York State Department of Financial Services (NYDFS) cybersecurity regulations[11]; or (4) "other data security rules and regulations of, and the statutes administered by, . . . the federal or New York state government."[12] However, notice must still be provided to the state attorney general, the department of state and the division of state police[13] and, if over 5,000 New York residents are notified, to consumer reporting agencies.[14]

- ***Notice Methods*.** The SHIELD Act also fine-tunes the requirements for "substitute notice" (*i.e.*, notice other than written notice, electronic notice or telephonic notice),[15] which consists of all of the following: (1) e-mail notice; (2) posting to the businesses' website, if one is maintained; and (3) notification by "major statewide media."[16] Pursuant to the SHIELD Act, if the information breached consists of an e-mail address with the password or security question and answer, the person or business must provide the e-mail notice to the consumer online while the consumer is connected to the online account from an IP address or online location that the consumer "customarily uses to access the online account."[17]

- ***State Attorney General, Department of State and the Division of State Police*.** For notification to the state attorney general, the department of state and the division of state police (which must occur if notice is to be provided to any New York residents), the SHIELD Act adds that the person or business must provide a copy of the notice template sent to affected persons.[18] Additionally, if any person or business is required to provide notice to the Secretary of Health and Human Services pursuant to HIPAA or the HITECH Act, such person or business must also provide such notification to the state attorney general within five business days of such notification.[19]

- ***Penalties*.** The SHIELD Act includes enhanced penalties for knowing and reckless violations, in which the court may impose a civil penalty of the greater of $5,000 or up to $20 per instance of failed notification, provided that the latter will not exceed $250,000.[20]

- ***Statute of Limitations.*** The SHIELD Act also extends the statute of limitations from two years to three years after either the date on which the state attorney general becomes aware of the violation, or the date of notice to the state attorney general, whichever is earlier.[21] However, the action must be brought within six years after the discovery of the breach unless the person or business took steps to hide it.[22]

New Data Security Protections

In addition to the foregoing, the SHIELD Act also adds a new statutory section relating to data security protections.[23] Specifically, a person or business that owns or licenses computerized data including a New York resident's private information must "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data."[24]

- ***Compliant Regulated Entities*.** A person or business is deemed in compliance with the reasonable security requirement if otherwise "subject to, and in compliance with" the federal or New York state regimes discussed above.[25]

- ***Data Security Program*.** Otherwise, a person or business is deemed compliant with the SHIELD Act's requirements upon implementing a data security program with certain administrative, technical and physical safeguards.[26]
  - Reasonable administrative safeguards include: (1) designating employee(s) to coordinate the program; (2) identifying foreseeable risks; (3) assessing sufficiency of safeguards to control these risks; (4) training and managing employees; (5) contracting with service providers to require such safeguards; and (6) making adjustments in response to changed circumstances.
  - Reasonable technical safeguards include: (1) "assess[ing] risks in network and software design" and "in information processing, transmission and storage"; (2) "detecti[ng], prevent[ing] and respond[ing] to attacks or system failures"; and (3) "regularly test[ing] and monitor[ing] . . . key controls, systems and procedures[.]"
  - Reasonable physical safeguards include: (1) "assess[ing] risks of information storage and disposal"; (2) "detect[ing], prevent[ing] and respond[ing] to intrusions"; (3) "protect[ing] against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information"; and (4) "dispos[ing] of private information within a reasonable amount of time after it is no longer needed for business purposes."
- ***Small Businesses*.** Reasonableness of administrative, technical and physical safeguards may be tailored to "the size and complexity of a small business, the nature and scope of the small business's activities, and the sensitivity of the personal information" collected.[27] A "small business" is defined as a person or business with fewer than 50 employees, less than $3 million in gross annual revenue in each of the prior three fiscal years, or less than $5 million in year-end total assets.[28]
- ***Penalties*.** The SHIELD Act does not create a private right of action, but failure to comply with the data security requirements is a violation of Section 349 of the Chapter and the state attorney general may bring an action to enjoin any such violations and to obtain civil penalties pursuant to Section 350-d.[29]

Identity Theft Prevention and Mitigation Services

On July 25, 2019, Governor Cuomo also signed a bill that requires consumer credit reporting agencies to offer reasonable identity theft prevention services and, if applicable, identity theft mitigation services for a period not to exceed five years and at no cost to consumers, in the event of a breach of the security of the system of such credit reporting agency that includes any social security number.[30] A consumer credit reporting agency would not be required to offer such services, if after appropriate investigation, the agency determines that the breach is unlikely to result in harm to consumers.

IMPLICATIONS FOR BUSINESSES

The SHIELD Act expands the scope of persons and businesses that will be required to notify New York residents whose personal information is the subject of a security breach and lowers the standard for determining when notification may be required. In addition, persons and businesses maintaining the private information of New York residents that are not already subject to and in compliance with certain other federal and New York state regimes may need to review and reassess the safeguards inherent to existing data security programs to ensure compliance with the new requirements.

*   *   *

ENDNOTES

[1] 2019 New York Senate Bill No. 5575.

[2] N.Y. Gen. Bus. Law §§ 899-aa(2), 899-bb.

[3] *Id*. § 899-aa(1)(b).

[4] *Id*. § 899-aa(1)(c).

[5] *Id*. § 899-aa(2).

[6] *Id*. § 899-aa(2)(a).

[7] *Id*.

[8] 15 U.S.C. §§ 6801–6809.

[9] 45 C.F.R. §§ 160, 164.

[10] 42 U.S.C. §§ 300jj *et seq*.; 17901 *et seq*.

[11] 23 NYCRR 500.

[12] N.Y. Gen. Bus. Law § 899-aa(2)(b).

[13] *Id*.

[14] *Id*. § 899-aa(8)(b).

[15] Substitute notice may be provided in cases where (1) the cost of notification exceeds $250,000; (2) over 500,000 persons are to be notified in the affected class; or (3) the business does not have sufficient contact information for such persons. *Id*. § 899-aa(5)(d).

[16] *Id*.

[17] *Id*. § 899-aa(5)(d)(1).

[18] *Id*. § 899-aa(8)(a).

[19] *Id*. § 899-aa(9).

[20] *Id*. § 899-aa(6)(a).

[21] *Id*. § 899-aa(6)(c).

[22] *Id*.

[23] N.Y. Gen. Bus. Law § 899-bb.

[24] *Id*. § 899-bb(2).

[25] *Id*. § 899-bb(2)(b)(i).

[26] *Id*. § 899-bb(2)(b)(ii).

[27] *Id*. § 899-bb(2)(c).

[28] *Id*. § 899-bb(1)(c).

[29] *Id*. § 899-bb(1)(d)-(e).

[30] 2019 New York Senate Bill No. 3582.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.

CONTACTS

New York		
H. Rodgin Cohen	+1-212-558-3534	cohenhr@sullcrom.com
Mitchell S. Eitel	+1-212-558-4960	eitelm@sullcrom.com
John Evangelakos	+1-212-558-4260	evangelakosj@sullcrom.com
Jared M. Fishman	+1-212-558-1689	fishmanj@sullcrom.com
Nicole Friedlander	+1-212-558-4332	friedlandern@sullcrom.com
Scott D. Miller	+1-212-558-3109	millersc@sullcrom.com
Matthew A. Schwartz	+1-212-558-4197	schwartzmatthew@sullcrom.com
Kamil R. Shields	+1-212-558-7996	shieldska@sullcrom.com
Alexander J. Willscher	+1-212-558-4104	willschera@sullcrom.com
Michael M. Wiseman	+1-212-558-3846	wisemanm@sullcrom.com
Washington, D.C.		
Eric J. Kadel, Jr.	+1-202-956-7640	kadelej@sullcrom.com
Stephen H. Meyer	+1-202-956-7605	meyerst@sullcrom.com
Jennifer L. Sutton	+1-202-956-7060	suttonj@sullcrom.com
Samuel R. Woodall III	+1-202-956-7584	woodalls@sullcrom.com
Los Angeles		
Anthony J. Lewis	+1-310-712-6615	lewisan@sullcrom.com
Palo Alto		
Nader A. Mousavi	+1-650-461-5660	mousavin@sullcrom.com
Sarah P. Payne	+1-650-461-5669	paynesa@sullcrom.com