Simpson Thacher

Memorandum

New York Strengthens Its Data Breach Notice Laws

August 13, 2019

On July 25, 2019, Governor Cuomo signed two laws to increase consumer protection regarding data breaches: the Stop Hacks and Improve Electronic Data Security Act (the "SHIELD Act") and a law applying specifically to consumer credit reporting agencies.[1] These laws follow the trend seen in California, Washington and other states in terms of broadening the scope of businesses and the types of personal information covered by data breach laws.

The Shield Act

Broader Scope

The SHIELD Act expands the scope of New York's existing data breach notice law, but with changes that are incremental rather than drastic in nature.

- The existing law required individuals to be notified after unauthorized acquisition of their social security numbers, driver's license numbers and/or financial account data in combination with a password. The SHIELD Act adds individuals': (i) financial account data if a password is not necessary to access an account, (ii) biometric information (e.g., fingerprint) or (iii) email address combined with a password.

- The SHIELD Act now requires New York residents to be notified if their personal information is "accessed" (e.g., viewed) and/or "acquired" (e.g., possessed, downloaded or used for identity theft) by an unauthorized person. The prior law covered "acquired" data only.

- The SHIELD Act covers companies that own or license computerized personal information of New York residents, whether or not such companies "conduct business in New York" (a requirement under the prior law). This expands coverage to out-of-state businesses, even those with minimal in-state contacts, so long as any New York resident's personal information is involved.

[1] *See* Stop Hacks and Improve Electronic Data Security Act (S.5575B/A.5635) and Identify Theft Prevention and Mitigation Services Act (no good acronym applies; A.2374/S.3582).

- Finally, the SHIELD Act requires covered businesses to implement reasonable data security safeguards. Such safeguards were already required under, *inter alia*, the FTC Act, other sector-specific federal laws, the GDPR and the New York Department of Financial Services Cybersecurity Regulations (the "DFS Cyber Regulations"), so this should not be a new burden to most companies. In fact, a business is deemed to comply with this SHIELD Act provision if it is compliant with the data security provisions of the Gramm-Leah-Bliley Act, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH") or the DFS Cyber Regulations. Otherwise, a business must maintain a qualifying security program, which requires reasonable administrative, technical and physical safeguards that are described at a high level (and without reference to a particular technology standard) in the statute. Such procedures are to be viewed in a size-appropriate context for smaller businesses. The attorney general is authorized to bring claims of up to $5,000 per violation for failure to comply with the data security safeguards.

Notice Timing

The SHIELD Act does not change the existing law that notice to affected individuals of a data breach is required "in the most expedient time possible and without unreasonable delay" and must be accompanied by notice to the State Attorney General and other state agencies.[2] The SHIELD Act adds that notice is not required for an "inadvertent disclosure" by persons authorized to access the information, if the disclosure is not likely to result in misuse of the data or financial or emotional harm, or if notice is already being provided to individuals pursuant to certain other statutes. Further, if more than 500 New York residents are affected by a data breach and/or if a covered entity must notify the U.S. Department of Health and Human Services of a data breach pursuant to HIPAA and HITECH requirements, then the State AG must be notified within 10 days or 5 business days, respectively.

Enforcement/Effective Date

The State AG continues to have the right to seek injunctive relief and a civil penalty, and the maximum penalty has been increased to $20 per instance of failed notice, or $250,000 in the aggregate. The SHIELD Act and prior data breach notice statute do not have a private right of action, although affected individuals still have several other laws and theories providing for relief in the event of a data breach. The new breach notice provisions of the SHIELD Act take effect on October 23, 2019 and the cybersecurity protection provisions take effect on March 21, 2020.

[2] N.Y. GBL Art. 39-F § 899-AA, Notification of Unauthorized Acquisition of Private Information § 2, as amended by S.5575B/A.5635.

Identify Theft Prevention and Mitigation Services Act

The Identity Theft Prevention and Mitigation Services Act provides that, if a consumer credit reporting agency experiences a data security breach involving consumer social security numbers, unless the agency reasonably determines that the security breach is unlikely to result in harm to the affected consumers, it will be required to provide affected consumers, at no cost, with (i) reasonable identity theft prevention services and (ii) if applicable, identity theft mitigation services for a maximum of five years. Further, it must provide consumers with information on how to enroll in such services and to request a credit freeze. This legislation will take effect on September 23, 2019, and includes retroactive application for any security breach in the three years prior to the effective date.

For further information regarding this memorandum, please contact one of the following:

NEW YORK CITY

Lori E. Lesser
+1-212-455-3393
llesser@stblaw.com

Nicholas S. Goldin
+1-212-455-3685
ngoldin@stblaw.com

Janice G. Brunner
+1-212-455-3529
janice.brunner@stblaw.com

Melanie D. Jolson
+1-212-455-3346
melanie.jolson@stblaw.com

WASHINGTON, D.C.

Vanessa K. Burrows
+1-202-636-5891
vanessa.burrows@stblaw.com

PALO ALTO

Jeffrey E. Ostrow
+1-650-251-5030
jostrow@stblaw.com

Marcela Robledo
+1-650-251-5027
mrobledo@stblaw.com

Simpson Thacher Worldwide

UNITED STATES

New York
425 Lexington Avenue
New York, NY 10017
+1-212-455-2000

Houston
600 Travis Street, Suite 5400
Houston, TX 77002
+1-713-821-5650

Los Angeles
1999 Avenue of the Stars
Los Angeles, CA 90067
+1-310-407-7500

Palo Alto
2475 Hanover Street
Palo Alto, CA 94304
+1-650-251-5000

Washington, D.C.
900 G Street, NW
Washington, D.C. 20001
+1-202-636-5500

EUROPE

London
CityPoint
One Ropemaker Street
London EC2Y 9HU
England
+44-(0)20-7275-6500

ASIA

Beijing
3901 China World Tower A
1 Jian Guo Men Wai Avenue
Beijing 100004
China
+86-10-5965-2999

Hong Kong
ICBC Tower
3 Garden Road, Central
Hong Kong
+852-2514-7600

Tokyo
Ark Hills Sengokuyama Mori Tower
9-10, Roppongi 1-Chome
Minato-Ku, Tokyo 106-0032
Japan
+81-3-5562-6200

SOUTH AMERICA

São Paulo
Av. Presidente Juscelino
Kubitschek, 1455
São Paulo, SP 04543-011
Brazil
+55-11-3546-1000