July 29, 2019

Are you ready? Companies doing business with New York residents face tighter data security requirements and increased scrutiny of breaches

Karen H Bromberg; Marvin J Lowenthal

Last Thursday, Governor Andrew M. Cuomo signed the Stop Hacks and Improve Electronic Data Security ("SHIELD") Act, which amends New York's current data breach notification law and places increased obligations on businesses that handle private data. With the SHIELD Act, New York joins the growing list of states that have adopted legislation to strengthen consumer privacy protections.

Expanded Definitions of Protected Data and Businesses Subject to the Notification Law

The SHIELD Act expands the categories of data protected by New York's data protection laws and the set of businesses subject to those laws. Businesses operating in New York were already required to notify New York residents whose private information was acquired by an unauthorized person.[1] But the Act expands the definition of private information to include more data such as: (1) biometric data, (2) user names or emails combined with passwords or security questions and answers, and (3) financial account numbers that can be used alone to access an account.

Broadened Territorial Scope Impacts Businesses outside of New York

The Act also subjects more businesses to the notification requirements of New York's data protection laws by requiring any business that owns or licenses computerized data that includes private information of a New York resident to provide notice of breaches to such affected residents. Previously, only companies that conducted business in New York were required to comply with those notice provisions. The expanded definition requires businesses to protect these additional categories of data and disclose to consumers, the New York Attorney General, the New York Department of State, and the division of the New York state police, as well as consumer reporting agencies in certain circumstances, when a data breach exposes that data.

[1] The Act kept the definition of "personal information" the same: "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person." However the definition of "private information" was expanded to mean either "(I) personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired. . . . or (II) 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." (additions underlined). Publicly available information lawfully made available to the general public from government records is still excluded from the definition of private information.

Expanded Definition of what Constitutes a Security Breach

The new law broadens the definition of "data breach" to include situations where data is merely accessed by an unauthorized person, not just in situations where data is acquired, which has been the standard. Access may include viewing, copying, or downloading private information. Additionally, in the event that a breach occurs, the Act adds new information about how to inform affected persons, expands the information that must be given, and requires certain information be provided to the New York Attorney General.

More Rigorous Data Security Requirements

Businesses may be impacted most in the area of their security plans as the Act imposes security requirements for all businesses that own or license the private information of a New York resident and describes new safeguards that businesses must implement to protect data. To comply with the Act, each business must develop a data security program that employs administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the private information (unless the business meets one of the exceptions in the Act, which are for businesses that are already complying with certain federal or state data security obligations). As a starting point, this means, among other things, that organizations will need to conduct risk assessments, train their employees on data security, carefully select vendors with a demonstrated capacity of maintaining and committing to appropriate safeguards, and develop appropriate document retention programs and network security and incident response plans.

The new requirements for data security programs take effect in March 2020.

Increased Regulatory Enforcement

The New York Attorney General also gains expanded powers to pursue legal action against businesses that violate New York's data protection laws. First, the SHIELD Act gives the New York Attorney General authority to pursue civil penalties and injunctions against businesses that fail to establish appropriate safeguards. The Act authorizes the Attorney General to bring an action for damage of not more than $5,000 per violation. The Act also increases the penalties for a company's failure to provide proper notice of a data breach to affected consumers. Companies that knowingly or recklessly fail to provide proper notice may be subject to a civil penalty of the greater of $5,000 or $20 per failed notification. But more generally, the statute of limitations is extended, so the Attorney General can now bring actions for violations within three years of the date on which the Attorney General became aware of the violation or the date on which a proper notice was issued about the breach. The time limits can be expanded further if the violator takes steps to hide the breach.

Conclusion

While the SHIELD Act has not yet taken effect, complying with the law's mandates, with its far-reaching effects, could be an extended process. Companies should work with their compliance teams and legal counsel to implement adequate data security programs and breach-response strategies that satisfy these new legal requirements.

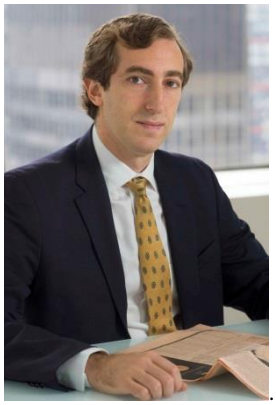
About C&G's Privacy & Data Security Group:

Attorneys in C&G's privacy & data security group advise clients on a broad range of privacy and data protection matters, including developing and implementing privacy policies and procedures, privacy-related litigation, regulatory investigations, global compliance, cross-border data transfers, website terms and conditions, social media and other new information technologies, cybersecurity and network intrusion issues, and contractual matters involving privacy and security.

The Authors:

Karen H Bromberg
Partner

+1 212 957 7604
kbromberg@cohengresser.com



Marvin J Lowenthal
Associate

+1 212 707 1334
mlowenthal@cohengresser.com

About Cohen & Gresser:

Cohen & Gresser is an international law firm with offices in New York, Seoul, Paris, Washington, D.C., and London. Founded in 2002, the firm has been recognized in a wide range of publications, including *Chambers* and *Legal 500*. We serve our clients in a number of practice areas, including Corporate, Employment, Intellectual Property & Technology, Litigation & Arbitration, Privacy & Data Security, Real Estate, Tax, and White Collar Defense & Regulation.

New York | Seoul | Paris | Washington DC | London

www.cohengresser.com
info@cohengresser.com
+1 212 957 7600

View C&G's Profile