> Covid-19 Client Alert

Practical Steps to Help Minimize Business Risk Under NY SHIELD Act Data Security Requirements

April 23, 2020

Authors and Key Contacts

If you have any questions about this alert, please contact any of the attorneys listed below.

Jessica L. Lipson
Partner & Co-Chair, Technology, Data Privacy & Intellectual Property Practice
P (212) 735-8683
F (917) 522-9573
jlipson@morrisonchen.com

David Lerner
Partner, Technology, Data Privacy & Intellectual Property Practice
P (212) 735-8609
F (917) 522-3109
dlerner@morrisoncohen.com

Shruti Chopra
Associate, Technology, Data Privacy & Intellectual Property Practice
P (212) 735-8628
F (917) 522-9928
schopra@morrisoncohen.com

With New York's statewide work-from-home mandate substantially increasing the potential risk of data breach incidents and private information loss, businesses operating in New York or processing New Yorkers' data should remember that the state's recently enacted Stop Hacks and Improve Electronic Data Security Act, commonly called the SHIELD Act, requires companies that collect, process or store private information about individuals to protect that data through reasonable means.

The law, which went into effect in March, is enforced by the office of the New York State Attorney General, which so far has given no indication that it will delay enforcement of the SHIELD Act as a result of the COVID-19 pandemic, nor, given the heightened risk, should any delay be expected.

The SHIELD Act identifies at a conceptual level some controls and procedures that are considered minimally required, including implementation of technical, administrative and physical measures to protect private information from unauthorized access and disclosure. As an example, administrative controls must include designating certain employees to oversee and coordinate security programs; identifying reasonably foreseeable internal and external risks and assessing the sufficiency of existing safeguards against them; and selecting service providers who can themselves comply with the SHIELD Act. Examples of technical safeguards include assessing technical risks in network and software design; and assessing risks in information processing and detecting and preventing attacks. Examples of physical safeguards include detecting and preventing intrusions into a company's physical space and systems; and properly disposing of data.

The law also expands the scope of private information subject to protection, and includes user names and passwords or other combinations of information that allow access to an online account (e.g., email or credentials to access retail websites), and biometric data such as eye scans or fingerprints.

Prior to the adoption of the SHIELD Act, enforcement was primarily limited to addressing data security deficiencies only after the occurrence of a breach, where, for example, the business had failed to comply with the state's breach notification laws or where the state could claim that a business, by actively misrepresenting the soundness of its data protection practices, had engaged in a deceptive business practice. In one case, the state sanctioned a business that had suffered a security attack although it had described its data management as "100% safe and secure," and "utilizing the latest security technology available."

The requirements imposed by the SHIELD Act, however, were specifically designed to expand the Attorney's General's arsenal of enforcement tools to examine and ensure that the private information of New York consumers is adequately protected, regardless of statements made about them. Moreover, the occurrence of a breach is not itself a condition of enforcement.

Without specific guidance yet from the Attorney General on the particular practices that might trip the SHIELD Act's requirements, businesses may want to look to actions taken to date by the Federal Trade Commission, enforcing Section 5 of the FTC Act. Although the federal act is focused on allegations of unfair and deceptive practices, the FTC has historically been more aggressive than New York in arguing that the failure to maintain "reasonable" data security and privacy practices is itself a violation of law.

Regulating largely through enforcement actions, consent decrees and settlements rather than by formal rulemaking, the Commission has also, like New York, concluded that misstatements and misrepresentations about privacy and security practices are unreasonable, and therefore unfair and deceptive, including misstatements:

- about the company's compliance with or participation in the Privacy Shield framework (which allows personal data transfer between the EU or Switzerland and the US);
- about how the company uses or shares the personal information of users and subscribers to the company's services or purchasers of its products; or
- in the company's privacy policies about the types of personal information it collects and how it collects, stores, uses, secures or disposes personal information of users and website visitors.

But the FTC has also looked at specific practices themselves, rather than only statements made about those practices, in prosecuting enforcement actions, including a company's:

- failure to use readily available vulnerability scanning, penetration testing, or other security measures, that would have detected an existing security vulnerability allowing an employee to connect an insecure storage device to a company's backup network; or
- a failure to use existing technology to adequately secure customer and consultant private information, including drivers' licenses, bank account data, and geolocation data.

This developing focus on the failure of a business to employ readily available technology to protect confidential, valuable or private data may well become the basis of future enforcement efforts, both by the FTC and, equally importantly, by New York's Attorney General under the SHIELD ACT. Based on the evolving standard, businesses should expect that the following deficiencies could well be considered "unreasonable," and should therefore take care to anticipate and avoid them:

- failing to make an inventory of the location where all sensitive data is stored within a company, or on its behalf by its service providers;
- failing to use strong encryption algorithms to secure stored data (although encryption is arguably of limited value given that it is largely ineffective against the typical form of intrusion which occurs through the use of authentic access credentials obtained through phishing or other fraudulent means);
- failing to maintain and test disaster recovery and business continuity plans, including the integrity and availability of current data backups;
- failing to insist on complex and unique user passwords that must be changed regularly in order to gain system access;
- failing to require multi-factor authentication as an access condition (two or more different verification methods such as a password plus a unique one-time separately generated code);
- failing to store the user credentials themselves securely;
- failing to limit the number of unsuccessful login attempts before account blockage;
- failing to set limited rights and privileges to control the nature, quantity and scope of access accorded to a company's vendors and customers;

- failing to conduct due diligence on the data management practices of vendors and customers who access company systems/networks;
- failing to segment company data in order to encapsulate a breach and prevent its spread beyond the access of the person whose system access account was compromised;
- failing to adopt active monitoring and notification technology so that the company's data security staff has an opportunity to prevent unusual or anomalous data inquiry or transfer events;
- failing to maintain a comprehensive and regularly supervised training regimen to sensitize a company's employees to the risks to data security posed by human error; or
- failing to dispose of the personal information collected once the legitimate business need for which it was collected has ended.

While it was already imperative for companies collecting and processing private information of individuals to protect that data, considering the dispersal of most companies' employees to work remotely throughout the COVID-19 emergency, the cybersecurity and data privacy staff of affected companies should consider carefully whether the protocols adopted prior to the onset of the pandemic remain sufficiently robust to deal with the increased risks caused by the decentralization of information access. Companies should ensure that all remote devices are themselves hardened against malicious intrusion (as, by example, requiring all devices to be running the most up-to-date operating system and anti-virus software), and whether security procedures have been updated to handle the possibility that compromised machines, from otherwise trusted personnel, could in turn compromise the integrity of the company's central data systems.

Both the FTC Act and the SHIELD Act can easily be employed by the FTC or the Attorney General to second-guess businesses that failed to take appropriate precautions to protect data, and given the changed circumstances of a business's data access and processing operations in these unprecedented times, it is more important than ever to reevaluate the measures that a company employs.

* * * * * *

Morrison Cohen LLP has created the COVID-19 Resource Taskforce, a multidisciplinary taskforce comprised of attorneys with deep expertise in a broad range of legal areas, to assist clients navigating the challenging and uncertain business and legal environment caused by the COVID-19 pandemic. We encourage clients to utilize our capabilities by reaching out to their primary Morrison Cohen attorney contact, who will put you in touch with the appropriate Taskforce person. You may also reach out directly to Joe Moldovan and Alec Nealon, the Taskforce co-chairs:

Joseph T. Moldovan
Chair, Business Solutions, Restructuring & Governance Practice
Co-Chair COVID-19 Taskforce
P (212) 735-8603
C (917) 693-9682
F (917) 522-3103
jmoldovan@morrisoncohen.com

Alec Nealon
Partner, Executive Compensation & Employee Benefits Practice
Co-Chair COVID-19 Taskforce
P (212) 735-8878
C (646) 318-4845
F (917) 522-9978
anealon@morrisoncohen.com