Client Update

NY Cybersecurity Bill Shows "Reasonable Security" Standard Gathering Force

On November 1, 2017, New York Attorney General Eric Schneiderman announced a proposed bill called the Stop Hacks and Improve Electronic Data Security ("SHIELD") Act. The SHIELD Act would broaden New York's breach disclosure requirements. It also would require that all businesses, breached or not, adopt "reasonable" cybersecurity measures. Reasonable security has been steadily gaining traction as a legal standard both in the United States and globally. Whether or not the SHIELD Act becomes law, its introduction is a prompt to ask whether your cybersecurity program is "reasonable."

HOW WOULD THE SHIELD ACT CHANGE NEW YORK LAW?

- Entities failing to adopt "reasonable" security measures, or failing to notify affected consumers after a data breach, would be subject to an enforcement action by the New York Attorney General.
- Entities holding personal information of New York residents would be subject to New York's law, even if they do not do business in New York.
- New categories of information would be added that, if breached, would trigger disclosure requirements: username and password combinations, biometric information, and health information covered by the federal Health Insurance Portability and Accountability Act.
- There would be a safe harbor against New York AG enforcement actions for entities that have "reasonable" cybersecurity, as certified by an independent organization (such as the National Institute of Standards and Technology ("NIST")), or by compliance with specific requirements outlined in the proposed statute.

WHAT IS "REASONABLE" SECURITY?

The SHIELD Act joins a growing U.S. and international legal trend toward imposing substantive cybersecurity standards, not just breach notification requirements.

- The U.S. Federal Trade Commission has brought numerous enforcement actions against breached companies. The legal hook is that less-than-"reasonable" security allegedly

amounts to an unfair business practice under Section 5 of the FTC Act. An FTC blog launched in July distills these cases into a list of what the FTC considers reasonable security measures.

- The U.S. Securities and Exchange Commission has made clear that it expects broker-dealers and investment managers to have a comprehensive cybersecurity program in place.
- New York's Department of Financial Services has spelled out comprehensive, specific cybersecurity requirements for banks and insurance companies licensed in New York.
- U.S. federal courts have allowed common-law negligence claims to survive motions to dismiss in recent cases arising from the data breaches at Target, Sony, and The Home Depot. The essence of a negligence claim, of course, is that the company has a duty to maintain reasonable cybersecurity in the first place.
- Over a dozen U.S. states, including California, Florida, Nevada, and Texas, already have statutes requiring "reasonable" cybersecurity. California's Attorney General has opined that compliance with the California statute requires compliance with the Center for Internet Security's Critical Security Controls.
- The European Union's General Data Protection Regulation ("GDPR"), which takes effect in May 2018, requires businesses to have "appropriate technical and organisational measures to ensure a level of security appropriate to the risk"—essentially a reasonable security requirement by a different name. The GDPR sets out a non-exhaustive list of "appropriate" measures, including pseudonymization and encryption of personal data as well as "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures."

By definition, "reasonable" security is a moving target. As security best practices become broadly accepted in the technical community, they morph into legal requirements. What's reasonable today may not be reasonable tomorrow. The SHIELD Act is a useful snapshot of what the New York Attorney General considers reasonable right now:

- An internal cybersecurity program, run by employees designated to deal with data security, that identifies risks, assesses safeguards, trains employees in security procedures, contractually requires vendors to maintain appropriate safeguards themselves, and adjusts to changed circumstances;
- Regularly tested technical safeguards that assess network risks and can prevent, detect, and respond to attacks or system failures; and
- Physical safeguards that protect against unauthorized access to private information, together with policies and procedures that assess risks in information storage and disposal, and dispose of private information once it is no longer needed for business purposes.

The SHIELD Act also considers compliance with NIST Special Publication 800-53 or the International Standards Organization (ISO) Standard 27002 to be evidence of reasonable

security. Both NIST and ISO require businesses to be proactive in maintaining a data security program that includes technical and physical safeguards, and to continually assess risks so that safeguards can be updated.

WILL THE SHIELD ACT BECOME LAW—AND IF NOT, WHY CARE?

New York is notorious for passing legislation only when it is engineered by "three men in a room"—the Governor, Assembly Speaker, and State Senate Majority Leader. Observers will note that the Attorney General is not one of the three. Attorney General Schneiderman proposed legislation similar to the SHIELD Act in 2015. It did not become law.

Even if the SHIELD Act does not become law, it matters. Like the FTC, the New York Attorney General regularly brings enforcement cases on the premise that the hacked company's pre-breach security was not reasonable. (Hilton paid $700,000 in settlement to the AG just last week.) When the AG's office lays out its view of what constitutes reasonable security, that is a good roadmap for possibly avoiding enforcement action in New York.

The SHIELD Act promises to be a useful guidepost nationally and globally as well. Its standards closely resemble those of the FTC, the GDPR, existing laws in other U.S. states, and other sources of legal guidance on reasonable cybersecurity. Companies engaged in "legal health checks"—that is, comparing their own cybersecurity to current best practices and legal requirements, and then moving to close any gaps—will therefore be well advised to look closely at AG Schneiderman's proposal.

* * *

For questions or assistance, please do not hesitate to call on any member of the Debevoise Cybersecurity & Data Privacy global practice team.

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Christopher S. Ford
csford@debevoise.com

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com