BRACEWELL

INSIGHTS

New York Cyber Enforcement Steps Into the Breach

July 9, 2018

Last month, the New York State Department of Financial Services (NYDFS) proclaimed, "In an era of weakened federal government oversight, strong state regulation is essential in order to safeguard our markets, ensure strong consumer protections and hold regulated entities accountable for their actions. New York will continue to lead in supporting a robust state financial services regulatory regime." NYDFS asserted its role as a cyber-regulator with back-to-back announcements that stake out its position as a leader in cybersecurity enforcement and consumer protection.

On June 27, 2018, just two days after NYDFS announced its finalized regulations that extend increased cybersecurity measures to credit reporting agencies, NYDFS—along with seven other state banking regulators—announced that Equifax had agreed to a raft of corrective measures in the aftermath of its 2017 data breach. As characterized by NYDFS Superintendent Maria Vullo: "DFS continues to take aggressive action in holding Equifax Inc. accountable for the massive data breach that exposed the sensitive and private information of millions of Americans." That breach compromised the data of 143 million people in the United States, including approximately eight million in New York.

The ***consent order*** requires Equifax to undertake corrective actions in the following areas:

- Information Security: The Equifax board must review and approve a written assessment that identifies foreseeable threats to the confidentiality of personally identifiable information (PII), the likelihood of those threats, potential damage to business operations, and appropriate safeguards and mitigating controls.

- Audit: The board or audit committee must oversee the establishment of a formal and documented internal audit program.

- Board and Management Oversight: The board or technology committee must improve the company's information security policy, including approval of a written program and review of the company's suite of policies and incident management procedures.

- Vendor Management: The company must improve oversight and documentation relating to critical vendors and controls to ensure the safeguarding of information.

- Patch Management: The company must improve standards and controls for patch management to reduce the number of unpatched systems and the length of patching

timeframes.

- Information Technology Operations: The company must enhance its oversight of IT operations, in particular as it relates to disaster recovery and business continuity function.

While the order did not mandate supervision by an independent monitor, it did impose significant reporting obligations on the company. Equifax is required to submit to regulators a list of all planned, in process, or implemented remediation projects; an independent party (which may be the company's internal audit function) must test the controls related to remediation efforts and report on the effectiveness of those controls. The company must also provide quarterly written reports to regulators on the progress of its compliance with the provisions of the order. NYDFS was joined in the consent order by banking regulators in Alabama, California, Georgia, Maine, Massachusetts, North Carolina, and Texas.

The Equifax consent order comes only two days after the announcement by NYDFS that credit reporting agencies that ran more than one thousand credit reports on New York consumers in the last year are now required to register with NYDFS and join the banks, insurance companies, and other financial institutions that are subject to the regulator's cybersecurity regulations. See 23 N.Y.C.R.R. Part 201, ***here***. NYDFS distinguished itself as the first state agency to regulate cybersecurity when its regulations when into effect in March 2017. (See Bracewell commentary on the 23 N.Y.C.R.R. Part 500 cybersecurity regulations ***here***.) Credit reporting agencies have until November 1, 2018 to comply with the new NYDFS cybersecurity requirements.

Under the newly finalized regulations, credit reporting agencies are required to register with the NYDFS and to submit annual reports to the agency; NYDFS is also authorized to request information at any time. Notably, NYDFS can revoke or suspend a credit reporting agency's registration if "the superintendent determines the registrant or any member, principal, officer or director of the applicant, is not trustworthy and competent to act as or in connection with a consumer credit reporting agency ... or has failed to comply with any minimum standard," including failure to comply with reporting requirements.[1] The regulations enumerate a number of grounds for revocation or suspension and prohibited practices, including unfair, deceptive, or predatory practices under New York or federal law; fraudulent practices under New York or federal law; and refusal to communicate with the authorized representative of a consumer regarding a credit report.[2]

Without valid registration, a credit reporting agency is prohibited from doing business with New York consumers or entities regulated by NYDFS.[3]

New York clearly views itself as a heavyweight—or perhaps *the* heavyweight—regulator in this area. Because the businesses that NYDFS regulates operate in complex commercial environments, one can expect that any vendors or other organizations that share their data will be similarly regulated. And as long as NYDFS views itself as a stand-in for federal oversight, it will further extend its regulatory reach.

---

[1] 23 N.Y.C.R.R. § 201.02.

[2] 23 N.Y.C.R.R. §§ 201.05 and 201.06

[3] 23 N.Y.C.R.R. § 201.03.