APRIL 21, 2020

For more information, contact:

Phyllis Sumner
+1 404 572 4799
psumner@kslaw.com

Scott Ferber
+1 202 626 8974
sferber@kslaw.com

Ehren Halse
+1 415 318 1216
ehalse@kslaw.com

William Johnson
+1 212 556 2125
wjohnson@kslaw.com

Kyle Sheahen
+1 212 556 2234
ksheahen@kslaw.com

King & Spalding

NY DFS Cybersecurity Regulation in the Face of COVID-19

The New York Department of Financial Services' (DFS) cybersecurity regulation imposes significant requirements on financial services companies doing business in New York.[1] DFS, which enforces the regulation, has remained outspoken and active on cybersecurity issues throughout the COVID-19 crisis. Since March 10, DFS has issued a series of industry letters addressing various COVID-19 related issues,[2] including:

Guidance to Department of Financial Services Regulated Entities Regarding Cybersecurity Awareness During COVID-19 Pandemic (on April 13),[3] which identifies several areas of heightened cybersecurity risk as a result of the COVID-19 crisis, including security challenges from the abrupt shift to mass remote working, increased phishing and fraud, and third-party risk, and reminds regulated institutions to assess the risks and "address them appropriately."

Guidance to New York State Regulated Institutions on Operational Risk Arising from the Outbreak of the Novel Coronavirus (on March 10), which requires regulated institutions to submit a response to DFS describing the institution's plan of preparedness to manage the risk of disruption to services and operations arising from COVID-19.[4] According to the guidance, the plan should be "sufficiently flexible to effectively address a range of possible effects that could result from an outbreak of COVID-19, and reflect the institution's size, complexity and activities." "[A]t a minimum," the plan should include assessments of, among other things: preventative measures tailored to the institution's specific profile and operations to mitigate the risk of operational disruption; all facilities (including alternative or back-up sites), systems, policies and procedures necessary to continue critical operations and services if members of the staff are unavailable for long periods or are working off-site; potential increased cyber-attacks and fraud; and preparedness of critical outside-party service providers and suppliers. The guidance also requires that those in charge of governance and oversight at institutions ensure that the

plan is reviewed and updated. This portion of the guidance underscores that boards of directors or the equivalent are responsible for ensuring that appropriate plans are in place and that sufficient resources are allocated to implement such plans. In addition, the guidance mandates that senior management is responsible for ensuring effective policies, processes, and procedures are in place to execute the plan and for communicating the plan throughout the institution to ensure consistency in approach so that employees understand their roles and responsibilities.

Against this backdrop, DFS issued an order on March 12, 2020 providing "temporary relief" from certain requirements, including extending the filing deadline for the 2019 cybersecurity compliance certifications from April 15, 2020, to June 1, 2020.[5] The relief order is welcome recognition of the challenges that institutions face in these extraordinary times, but it should not be construed as a compliance hall pass or enforcement forbearance. Notably, the relief order states that remotely working personnel "shall remain subject to the full supervision and oversight of such regulated entities and persons, and such regulated entities and persons shall maintain appropriate safeguards and controls, including but not limited to those related to data protection and cybersecurity, to ensure continued safety and soundness of such regulated entities and persons." In addition, the 72-hour deadline for providing notice of a cybersecurity event to the DFS Superintendent has not been extended. Further, as the industry letters show, DFS is laser-like focused on cybersecurity in the face of COVID-19. Notably, in the April 13 letter described above, while acknowledging that "[t]he COVID-19 pandemic has disrupted normal operations in the financial services industry and beyond, and cyber criminals are exploiting the crisis," DFS cautioned, "[d]espite the extraordinary challenges, regulated entities should remain vigilant."[6]

All signs point to DFS's prioritization of cybersecurity regulation enforcement. Since taking over DFS in 2019, Superintendent Linda A. Lacewell has taken steps to fortify enforcement efforts, including forming a "consumer protection task force" in January 2020 and hiring several high-profile former prosecutors in leadership roles. Although DFS has not yet brought an enforcement action under the cybersecurity regulation, it has investigated and resolved through settlement cybersecurity compliance issues. DFS currently has a backlog of approximately two years' worth of reported events, accounting for over 1,000 incidents that could possibly result in enforcement. At a February 2020 speech, in response to questions about when enforcement of the cybersecurity regulation would begin, Superintendent Linda A. Lacewell said, "it will come – be ready."

For companies looking for insight into possible consequences for noncompliance, the text of the cybersecurity regulation does not explain how penalties and fines may be calculated or assessed. During the public comment period prior to the March 1, 2017 effective date of the regulation, DFS responded to requests for additional detail about the enforcement mechanisms by saying only that the existing language is "sufficient." Enforcement actions under the cybersecurity regulation could stem from the general authority of DFS under the New York Banking Law, which allows for penalties for violations as high as $2,500 per day during which a violation continues, $15,000 per day in the event of any reckless or unsound practice or pattern of misconduct, and $75,000 per day in the event of a knowing and willful violation.[7]

Given the potentially significant penalties at DFS's disposal, strict compliance with the cybersecurity regulation is critical, even under the challenging circumstances presented by COVID-19.

---

[1] *See* 23 NYCRR 500, available at https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf.

[2] https://www.dfs.ny.gov/industry/coronavirus

[3] https://www.dfs.ny.gov/industry_guidance/industry_letters/il20200413_covid19_cybersecurity_awareness. This replaces a previous April 3 industry letter on the same topic. https://www.dfs.ny.gov/industry_guidance/industry_letters.

[4] https://www.dfs.ny.gov/industry_guidance/industry_letters/il20200310_risk_coronavirus.

[5] https://www.dfs.ny.gov/system/files/documents/2020/03/ea20200312_covid19_relief_order.pdf.

[6] https://www.dfs.ny.gov/industry_guidance/industry_letters/il20200413_covid19_cybersecurity_awareness.

[7] *See* NYBNK § 44.