Guidepost

NYDFS ISSUES ADDITIONAL COVID-19 GUIDANCE REGARDING CYBERSECURITY

The New York State Department of Financial Services has been issuing a stream of orders and guidance for regulated institutions concerning the COVID-19 pandemic. This week it issued another one directed at cybersecurity. DFS is widely known for its first-in-the-nation mandatory and comprehensive cybersecurity regulation (23 NYCRR Part 500), and this new guidance is intended to inform licensees that DFS has "identified several areas of heightened cybersecurity risk as a result of this [health] crisis."

The DFS guidance identifies three "heightened risks" faced by regulated institutions. First, it singles out increased risk to networks and "Nonpublic Information" (as defined by the regulation) due to "remote working," listing several areas of vulnerability in this category:

- secure connections (e.g., need for multi-factor authentication and/or VPNs);
- company-issued devices;
- Bring Your Own Device ("BYOD") expansion;
- remote working communications (e.g., Zoom; Webex, etc.); and
- data loss prevention (e.g., where employees use personal e-mail).

Second, the DFS guidance identified as a heightened risk "increased phishing" and "online fraud" related to COVID-19. The guidance referred to a recent report from the Federal Bureau of Investigation pinpointing several types of scams that appear to be on the rise, including "fake CDC Emails" and "counterfeit treatments or equipment." DFS advised regulated entities to remind employees "to be alert for phishing and fraud emails," and "revisit phishing training and testing at the earliest practical opportunity."

Third, the DFS guidance noted that the COVID-19 pandemic presented additional challenges for the third-party vendors of regulated entities. DFS advised licensees to "re-evaluate the risks to critical vendors" and coordinate with these vendors to ensure that they are meeting the increased risks occurring due to the pandemic. DFS went on to note that "following good cybersecurity practices [will enable] entities [to] identify, mitigate, and manage the risks" presented by the circumstances of this health and economic crisis.

Finally, DFS reminded regulated entities that cybersecurity reporting obligations remained in place: under "Section 500.17(a), covered Cybersecurity Events must be reported to DFS as promptly as possible and within 72 hours at the latest."

In light of the evolving threats and risks involved in the COVID-19 pandemic, we expect DFS to issue additional guidance for regulated entities, and will continue to provide relevant updates should they occur.