

NY Department of Financial Services Issues Guidance to Regulated Entities Regarding Cybersecurity During the COVID-19 Pandemic

Article By:

Hunton Andrews Kurth's Privacy and Cybersecurity

On April 13, 2020, the New York Department of Financial Services ("NYDFS") issued [guidance](#) ("April guidance") to all New York State entities covered under NYDFS's cybersecurity regulation regarding assessing and addressing heightened cybersecurity risks due to the COVID-19 pandemic. In asking regulated entities to address risks "appropriately," the April guidance references NYDFS's earlier March 10, 2020 [guidance](#) calling on regulated institutions to submit to the agency (within 30 days of the guidance) plans "to address operational risks posed by the outbreak of a novel coronavirus," including "assessment[s] of potential increased cyber-attacks and fraud."

The April guidance identifies three areas of heightened cybersecurity risks due to the COVID-19 pandemic:

1. **Remote Working** – including the risks presented to regulated entities' networks and nonpublic information by remote access connections, company-issued devices, employees' personal devices, conferencing applications and unauthorized personal accounts and applications.
2. **Increased Phishing and Fraud** – including criminal spoofing of emails from the Centers for Disease Control and Prevention identified by law enforcement.
3. **Third-Party Risk** – including risks posed to critical vendors.

The April guidance identifies measures to address the heightened risks, including:

- Securing remote access through "Multi-Factor Authentication" (as defined under NYDFS's cybersecurity regulation) and VPN connections;
- Locking down devices so applications cannot be added or deleted by users, and installing appropriate security software, including for endpoint detection and response, and mobile device management;

- Considering mitigating steps, such as compensating controls, where personal devices are necessary;
- Configuring conferencing applications to limit unauthorized access and ensuring employees have guidance on the secure use of the applications;
- Reminding employees not to send “nonpublic information” (as defined) to personal email accounts and devices;
- Reminding employees to be alert for phishing and fraud emails, and revisiting training thereon;
- Considering updating authentication protocols, especially for key actions like security exceptions and wire transfers; and
- Coordinating with critical vendors to determine how they are adequately addressing new risks.

In addition, the NYDFS reminded regulated entities that covered “cybersecurity events” (as defined) must be reported to the agency “as promptly as possible and within 72 hours at the latest.”

Copyright © 2025, Hunton Andrews Kurth LLP. All Rights Reserved.

National Law Review, Volume X, Number 113

Source URL: <https://natlawreview.com/article/ny-department-financial-services-issues-guidance-to-regulated-entities-regarding>