BLANKROME

Cybersecurity & Data Privacy


JUNE 2, 2020 • NO. 8

# NYDFS Issues New Guidance on COVID-19 Cybersecurity Risks

*As the coronavirus ("COVID-19") pandemic continues, cyber criminals have upped the intensity of their COVID-19-themed cyber-attacks designed to exploit the current crisis. With financial institutions representing primary targets for COVID-19 cyber-attacks, the New York Department of Financial Services ("NYDFS") issued new guidance to regulated entities regarding cybersecurity awareness. This guidance provides key tips on how to mitigate some of the most significant cyber risks. Regulated institutions should review this guidance and, where feasible, implement the best practices offered by the NYDFS.*

**Overview of New NYDFS Cybersecurity Awareness Guidance**

To aid financial institutions in combating the enhanced threat of cybercrime and criminals seeking to exploit the pandemic, the NYDFS recently issued guidance that identifies several critical areas of heightened cybersecurity risk that have developed as a result of COVID-19. Regulated entities must assess these risks and address them appropriately, both as required by the NYDFS's Part 500 Cybersecurity Regulation, and also with respect to the COVID-19 operational preparedness plans called for in previous NYDFS guidance.

**Remote Working**

The first area of enhanced risk identified by the NYDFS is remote working. The abrupt shift to mass remote working necessitated by COVID-19 has created new security challenges and vulnerabilities that are being exploited by cyber criminals. These heightened risks to regulated entities' networks and nonpublic information include:

- **Secure Connections.** Regulated entities should make remote access as secure as possible under their given circumstances. This includes the use of multi-factor authentication ("MFA"), which uses two or more identity components—such as a password and a fingerprint—to authenticate a user's identity, and secure virtual private network ("VPN") connections that encrypt all data while in transit. For additional information on enterprise VPN security, the Cybersecurity and Infrastructure Security Agency ("CISA") recently issued targeted guidance on this issue, which can be found here.

- **Company-Issued Devices.** As new devices are acquired or repurposed for remote working, regulated entities must ensure they are properly secured. This includes locking devices to prevent users from adding or deleting applications and installing appropriate security software, such as endpoint detection/response and mobile device management ("MDM").

- **Bring-Your-Own-Device Expansion**. Regulated entities that have expanded their bring-your-own-device ("BYOD") policies to enable mass remote working should be knowledgeable of the associated security risks and implement appropriate controls to mitigate those risks.

- **Remote Working Communications.** Remote working has increased reliance on video- and audio-conferencing applications, which are being increasingly targeted by cyber criminals. Regulated entities should configure these tools to limit unauthorized access and ensure that employees are educated on how to use them securely.

- **Data Loss Prevention.** Remote working carries the risk of employees using unauthorized personal accounts and applications—like email accounts—to remain productive while working remotely. Regulated entities should remind and instruct employees to refrain from sending sensitive personal and financial information to personal accounts and devices.

## Increased Phishing and Fraud

The second area of enhanced risk concerns online fraud and phishing attempts tied to COVID-19. For example, the Federal Bureau of Investigation ("FBI") has reported that criminals are using fake emails pretending to be from the Centers for Disease Control and Prevention ("CDC"), asking for charitable contributions, or offering COVID-19 relief, such as government checks.

As such, the NYDFS recommends regulated entities remind employees to be on alert for phishing and fraud emails, and revisit phishing training and testing at the earliest practical opportunity. In addition, with face-to-face work being severely curtailed, authentication protocols may need to be updated—especially for key actions such as security exceptions and wire transfers. For additional information on how to guard against the significant risk of COVID-19-themed phishing attacks, please view our COVID-19 Task Force article on this topic here.

## Third-Party Risk

The final area of enhanced risk relates to third-party vendors and service providers. The NYDFS notes the challenges created by COVID-19 have also impacted third-party vendors, meaning regulated entities must re-evaluate the risks associated with these critical service providers.

Specifically, the NYDFS recommends regulated entities coordinate with critical vendors to determine how they are adequately addressing new risks. In addition, regulated entities should also ensure they have an up-to-date third-party service provider security policy in place, as required by § 500.11 of the NYDFS Cybersecurity Regulation.

Regulated entities' third-party security policies should be designed to ensure the security of systems and sensitive data that are accessible to/held by third-party vendors, and should address to the extent applicable: (1) the identification and risk assessment of third-party vendors; (2) minimum cyber practices required to be met by vendors to do business with the regulated entity; (3) due diligence processes used to evaluate the sufficiency of vendors' cyber practices; and (4) periodic assessments of vendors based on their risk profile and the continued effectiveness of their cyber practices. Regulated entities' policies should also include relevant guidelines for due diligence and/or contractual protections relating to third-party vendors.

## Conclusion

Financial institutions have always been an attractive target for cyber criminals due to the tremendous amount of valuable information they hold. Those threats have risen to unprecedented levels as a result of COVID-19. Financial institutions will remain a top target for cyber criminals looking to cash in on the pandemic. Accordingly, regulated entities must remain vigilant and adhere to proper cybersecurity/privacy practices to effectively manage and mitigate these outsized risks directly tied to COVID-19 and avoid regulatory financial penalties.

As part of its COVID-19 Task Force, Blank Rome's Cybersecurity & Data Privacy team can assist in providing key counseling and guidance with respect to any issues or concerns relating to the unique security and privacy risks faced by financial instructions, as well the necessary policies, procedures, and protocols that are needed to fully mitigate the myriad of cyber risks associated with COVID-19, which will persist for the duration of the current health emergency. And if your organization suffers any type of security incident during the COVID-19 pandemic, Blank Rome's data breach

incident response team is available 24/7 and can provide immediate assistance with rapid response and crisis management following any type of breach or security event.

**For additional information, please contact:**

**David J. Oberly, Cincinnati Office**
**Associate, Cybersecurity & Data Privacy,**
**Privacy Class Action Defense**
**513.362.8711 | doberly@blankrome.com**