> Covid-19 Client Alert

NY DFS Issues Guidance Cybersecurity Awareness During COVID-19 Pandemic

April 14, 2020

Authors and Key Contacts

If you would like any further information concerning cybersecurity and related compliance issues, please feel free to contact any of the attorneys listed below

David Lerner
Partner, Technology, Data Privacy & Intellectual Property
P (212) 735-8609
dlerner@morrisoncohen.com

Jessica L. Lipson, CIPP/US
Partner & Co-Chair, Technology, Data Privacy & Intellectual Property
P (212) 735-8683
jlipson@morrisoncohen.com

Jessica R. Colombo
Senior Counsel, Corporate
P (212) 735-8753
jcolombo@morrisoncohen.com

Shruti Chopra
Associate, Technology, Data Privacy & Intellectual Property
P (212) 735-8628
schopra@morrisoncohen.com

Timur N. Eron
Associate, Corporate
P (212) 735-8882
teron@morrisoncohen.com

In an effort to address the cybersecurity challenges facing businesses as a result of the novel coronavirus, the New York Department of Financial Services issued guidance for New York regulated entities. Although this guidance relates specifically to New York regulated entities, companies that may be regulated by other states and the SEC should take note as such regulators often follows NY DFS guidance. Cybersecurity remains a critical component of a company's infrastructure and while certain issues have been highlighted as a result of the coronavirus, companies should consider the NY DFS guidance not just relevant to the current crisis but as best practices in general.

A strong cybersecurity system requires implementing effective policies and training employees to comply with such policies. To ensure the security of remote access, guidance instructs DFS regulated entities to use multi-factor authentication and secure VPN connections that will encrypt all data in transit. Computers and devices used by remote workers should have anti-virus and security software should be properly secured, including having controls in place so that users cannot add or delete applications. While some remote workers may use their personal devices for work related matters, companies should review and potentially expand their Bring Your Own Device Policies to account for security risks such as data leakages and accidental disclosures that may arise as a result of the use of personal devices, and implement procedures to ensure that such devices are secured and have not been compromised (e.g., by having malicious applications downloaded on them).

Remote working often requires the use of video and audio applications and as such, regulated entities should ensure that these tools are configured to limit unauthorized access and that communications are encrypted. The NY DFS also warns that there have been a number of coronavirus related fraud and phishing attempts and authentication protocols may need to be implemented or updated.

DFS advised companies to also assess the training they provide to their employees to ensure that employees do not use personal email accounts in connection with nonpublic information, that employees know how to securely access video and audio applications and to, as always, remain vigilant about phishing and fraud communications (e.g., to confirm instructions prior to sending wire transfers).

Looking outside their organizations, DFS said that companies should be mindful of how the current health crisis has affected their third party vendors, and should re-evaluate the policies of critical vendors to ensure such vendors are adequately addressing new risks. Finally, regulated companies were reminded to report all covered cybersecurity events as promptly as possible and, in any event, no later than 72 hours after becoming aware of such event.

While this guidance currently only applies to NY DFS regulated entities, any business with a financial component, including investment advisers and broker-dealers, should continuously evaluate and update their cybersecurity programs and should be prepared for similar guidance to be promulgated from their own regulators.

* * * * * *

Morrison Cohen LLP has also created the COVID-19 Resource Taskforce, a multidisciplinary taskforce comprised of attorneys with deep expertise in a broad range of legal areas, to assist clients navigating the challenging and uncertain business and legal environment caused by the COVID-19 pandemic. We encourage clients to utilize our capabilities by reaching out to their primary Morrison Cohen attorney contact, who will put you in touch with the appropriate Taskforce person. You may also reach out directly to Joe Moldovan and Alec Nealon, the Taskforce co-chairs:

Joseph T. Moldovan
Chair, Business Solutions, Restructuring & Governance Practice
Co-Chair COVID-19 Taskforce
P (212) 735-8603
C (917) 693-9682
F (917) 522-3103
jmoldovan@morrisoncohen.com

Alec Nealon
Partner, Executive Compensation & Employee Benefits Practice
Co-Chair COVID-19 Taskforce
P (212) 735-8878
C (646) 318-4845
F (917) 522-9978
anealon@morrisoncohen.com