BLANKROME

Cybersecurity and Consumer Finance

APRIL 6, 2020 • NO. 1

NYDFS Mandates Submission of COVID-19 Emergency Plans for Regulated Financial Institutions

As cybersecurity threats stemming from the novel coronavirus ("COVID-19") pandemic continue to increase, the New York Department of Financial Services ("NYDFS") has issued two pieces of guidance that require all regulated institutions—such as state-chartered banks and credit unions, branches of foreign banking organizations, broker-dealers, licensed lenders, and money transmitters—to submit preparedness plans addressing their management of the significant operational and financial risks they now face stemming from the COVID-19 pandemic by April 9, 2020. Those institutions that have not already finalized their plans should take immediate action now to ensure the ability to meet the April 9 deadline.

Significantly Enhanced Cybersecurity Risks Prompt Action from the NYDFS

In addition to threatening the health of the nation, COVID-19 has also created a significant threat to the security of businesses' information technology systems as cybercriminals attempt to exploit the crisis—and the panic caused by the pandemic—by substantially increasing the frequency of their cyber attacks in an attempt to unlawfully gain access to highly sensitive electronic data. This enhanced threat is particularly significant for financial institutions, which already rank among the most prevalent targets for cybercriminals.

Recognizing the potential vulnerabilities arising from this public health emergency, the NYDFS recently issued guidance requiring all regulated institutions to submit operational and financial plans to ensure they have adequate measures in place to address these critical risks.

Operational Preparedness Plan

First, to ensure that regulated institutions have preparedness plans in place to address the operational risks posed by COVID-19, the NYDFS has mandated that all institutions submit operational preparedness plans, which describe how they will address any disruptions to their services and operations that may develop as a result of the current public health emergency. The NYDFS instructs that their operational preparedness plans must generally describe the entity's plan for managing operational risks, and should be sufficiently flexible to effectively address a wide range of potential issues that could arise from COVID-19. In addition, all operational preparedness plans must specifically include, at a minimum, the following:

- tailored preventative measures to mitigate the risk of operational disruption, including the impact on customers;

- a documented strategy addressing the impact of the outbreak in stages, including an assessment of how quickly measures can be adopted and how long operations can be sustained under different stages of the outbreak;
- an assessment of all facilities, systems, policies, and procedures necessary to continue critical operations and services if complications arise regarding staffing and personnel, including an assessment of remote working capabilities;
- an assessment of potential increased cyberattacks and fraud;
- employee health protection strategies to sustain an adequate workforce during the outbreak;
- an assessment of the preparedness of critical third-party vendors and service providers;
- the development of a communication plan to effectively communicate with multiple categories of stakeholders; and
- testing, governance, and oversight of the plan to ensure its effectiveness.

Financial Risk Management Plans

Similarly, to ensure that regulated institutions are adequately identifying, monitoring, and managing the potential financial risk arising from COVID-19, the NYDFS has also mandated that all institutions submit financial risk management plans, which describe the measures they have in place to address any adverse financial impact that they may experience as a result of the current public health emergency. The NYDFS instructs institutions that their financial risk management plans must adequately assess and monitor the potential financial risk that may develop from COVID-19. In addition, all financial risk management plans must specifically include, at a minimum, assessments of the following:

- the overall impact of COVID-19 on earnings, profits, capital, and liquidity;
- the credit risk ratings of customers, counterparties, and business sectors impacted by COVID-19;
- the credit exposure to customers, counterparties and business sectors impacted by COVID-19;
- the scope and the size of credits adversely impacted by COVID-19 that currently are in, or potentially may move to, non-performing/delinquent status;
- the valuation of assets and investments impacted by COVID-19; and
- the reasonable steps that can be taken to assist those adversely impacted by COVID-19.

Plan Implementation Responsibility

According to both pieces of NYDFS guidance, the board of directors of regulated institutions must ensure the appropriate plans are in place and sufficient resources are allocated to implement these plans. Similarly, senior management must ensure that the necessary policies, processes, and procedures are implemented to execute and communicate the plan.

Compliance Pointers

As indicated above, both plans must be submitted to the NYDFS by April 9, 2020. Completed plans should be e-mailed to the NYDFS's designated e-mail address: banking.covid19@dfs.ny.gov.

Although the NYDFS has provided a very tight window to satisfy these plan requirements, institutions should not assume that non-compliance will go unaddressed simply because of the current public health emergency. This is especially so in light of the recent comment issued by the NYDFS emphasizing the importance of ensuring that "institutions have preparedness plans in place to address operational and financial risk posed by the outbreak of a novel coronavirus known as 'COVID-19,'" strongly signaling that the department will be vigilant in enforcing timely compliance with the mandate.

During the plan preparation process, institutions should review their existing cybersecurity programs, incident response plans, and other materials required for compliance with the NYDFS Part 500 Cybersecurity Regulation. These materials may contain a documented pandemic response strategy scaled to the stages of a pandemic outbreak—such as the six pandemic intervals described by the Center for Disease Control and Prevention—and a comprehensive program to ensure the continuance of critical operations, which includes evaluating and monitoring service providers.

Finally, in addition to the above guidance, the NYDFS also recently issued its Order Granting Temporary Relief to COVID-19 Affected Regulated Entities and Persons which, among other things, extends the NYDFS Part 500 Cybersecurity Regulation Certificate of Compliance filing deadline from April 15 to June 1, 2020. For additional information on the NYDFS Temporary Relief Order, please view our COVID-19 Task Force's alert on this topic here.

Conclusion

At this juncture, cyber criminals have already upped the frequency of their attacks hoping to take advantage of the anxiety and fear that has been generated as the COVID-19 crisis grows larger, and financial institutions will undoubtedly remain a top target for cyber criminals for the duration of the current health crisis. Thus, while fairly burdensome, the NYDFS's COVID-19 operational preparedness plan requirements can assist institutions in ensuring they have the proper security measures in place to defend against this heightened cyber risk, as well as the ability to respond immediately to any data breach that may take place during the course of the pandemic.

At the same time, compliance with the NYDFS's financial risk management plan requirements can also aid institutions in ensuring they are fully prepared to respond and adapt to any adverse economic effects that may arise domestically or globally in the future as a result of COVID-19.

As part of its COVID-19 Task Force, Blank Rome's Cybersecurity and Data Privacy and Consumer Financial Services teams can assist with providing key counseling and guidance with respect to any issues or concerns relating to regulated institutions' NYDFS operational preparedness and financial risk management plan requirements, as well as the necessary policies, procedures, and protocols that institutions should have in place to effectively manage and mitigate the unique cybersecurity, operational, and financial risks posed by COVID-19.

For additional information, please contact:

Jennifer J. Daniels, Pittsburgh Office
Partner, Cybersecurity & Data Privacy
412.932.2754 | daniels@blankrome.com

Scott E. Wortman, New York City Office
Partner, Consumer Financial Services
212.885.5359 | swortman@blankrome.com

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