NEW YORK STATE OF OPPORTUNITY. | Department of Financial Services

MEMORANDUM

TO: Chief Executive Officers of DFS Regulated Institutions

FROM: Superintendent Maria T. Vullo

DATE: December 21, 2018

RE: DFS Cybersecurity Regulation -- First Two Years and Next Steps

This memorandum provides an update on the New York Department of Financial Services (DFS)'s cybersecurity regulation, 23 NYCRR 500, which became effective March 1, 2017, with a two-year implementation period. Please share this memorandum with relevant personnel responsible for your institution's cybersecurity compliance.

The regulation requires all DFS regulated entities, subject to certain exemptions, to adopt the core requirements of a cybersecurity program, including a cybersecurity policy, effective access privileges, cybersecurity risk assessments, and training and monitoring for all authorized users, among other requirements. The regulation also requires the establishment of governance processes to ensure senior attention to these important protections. The final effective date for the regulation will be March 1, 2019, by which time, under section 500.11, DFS regulated entities are required to have written policies and procedures that are based on a risk assessment to ensure the security of nonpublic information and information systems that are accessed or held by third party service providers.

Accordingly, by March 1, 2019, all banks, insurance companies, and other financial services institutions and licensees regulated by DFS will be required to have a robust cybersecurity program in place that is designed to protect consumers' private data; a written policy or policies that are approved by the Board of Directors or a Senior Officer; a Chief Information Security Officer to help protect data and systems; and controls and plans in place to help ensure the safety and soundness of New York's financial services industry including encryption and multifactor authentication. The regulation sets forth certain limited exemptions, many of which still require certain cybersecurity programs and practices.

As Superintendent, I have made clear that the purpose of the DFS cybersecurity regulation is to bolster the financial services industry's defenses against cybersecurity attacks, in order to protect our markets and consumers' private information. The governance framework set forth in the regulation, along with DFS's ongoing oversight, including in regular and target examinations, are intended to assist in the bolstering of the industry's cybersecurity defenses, for the protection of industry, overall markets and consumers. Consistently with these important objectives, DFS examiners have been including cybersecurity in all regular examinations across the Department. Furthermore, DFS has established internal policies and procedures for the review and response to confidential information provided by regulated entities to DFS as part of the regulation's notice and other procedures.

Notices of Breach

Importantly, the DFS cybersecurity regulation requires regulated entities and licensed persons to submit notices to the Department of cybersecurity events as defined in the regulation to include both successful and certain unsuccessful attempts. The purpose of this notice provision is to provide the Department with information relevant to its supervision of the financial services industry, including to provide confidential assistance to regulated entities with respect to information learned by the Department that could be useful to further bolster industry's cybersecurity protections. The confidentiality of the Department's specific interactions with regulated entities with respect to cybersecurity is protected by law, including the Banking Law, Insurance Law and Financial Services Law. While individual interactions are confidential, this memorandum provides a broad overview of the Department's practices and general themes with respect to the Department's information gathering over the past year.

Pursuant to the regulation, the Department has received approximately 1,000 notices of cybersecurity events from regulated institutions. DFS investigators review these notices and, in consultation with our examination and supervisory teams, assess the information and take appropriate actions to address any concerns that relate to institutions' cybersecurity protections. In some cases, based on the information provided and any responses already undertaken by the regulated entity, no further action by DFS is deemed warranted. In other cases, DFS professionals may identify from the information provided a circumstance or trend that subject to confidentiality warrants providing certain information to other regulated entities regarding a potential threat. For example, the identification of a cyber breach relating to a third-party vendor that contracts with multiple institutions in a certain sector may warrant DFS providing information to those other DFS regulated institutions. In appropriate circumstances, DFS professionals may take other steps, including making sure that the appropriate law enforcement bodies have been alerted, that the institution is addressing any impacted consumer, and of critical importance that necessary steps are being taken to close and remedy the system issue that led to the breach. All of these actions are taken by DFS in consultation with the regulated institution in question, with the goal of protecting the institution and other DFS regulated institutions, as well as the customers of the affected institutions.

In general, DFS's experience based on reports of cybersecurity events has only emphasized the importance of Part 500's requirements, including the need for strong access controls and the protection of email systems including authorized users and training of employees. Part 500.03 requires all companies, including most small companies that are entitled to a limited exemption, to have policies and procedures for access controls. Importantly, the majority of successful breaches involve common software technology used throughout business operations and have involved phishing attacks, social engineering threats, and issues relating to password composition and security and email security.

More specifically, a significant number of the events reported to DFS involved breaches that stemmed from employees providing credentials in response to attractive emails that trick a user to provide confidential information. In these cases, the intruder sends a legitimate-seeming e-mail to a company's employee or employees. These attacks are carefully planned to appear from a source that the employee will trust, perhaps even appear to be an email from a customer or client of that employee and a subject that will peak their interest. The employee is prompted

to enter his or her e-mail credentials, and the intruder gains access to the company's e-mails on the system, which can contain consumers' personal identifying information.

These many events remind us to make sure that all persons who can access a company's systems have the proper protections, and are using the appropriate protections. Third parties who access a company's systems or data can cause serious breaches where such third parties were using unsecured email accounts. Other access issues that arise include "credentials churning" attacks, by which the company's access portal is bombarded with access attempts using usernames and passwords from other breaches. In these situations, the attackers know that many users reuse the same username and password for numerous websites, and therefore try to use the user names and passwords that have been the subject of known breaches to see if they will allow access here.

In many cases, the protections required by the DFS regulation could have prevented these incidents: for example, strong access controls and training as required by the regulation are critical to avoiding the phishing attacks that threaten the market. We also emphasize the need for education and training which can help ensure that all parts of the organization are aware of and follow proper cybersecurity procedures. DFS has emphasized working with its licensees and regulated persons to improve their programs, and licensees should embrace opportunities to improve and advance their cybersecurity readiness and systems. While all aspects of the DFS regulation are important, recent attacks on emails and transmissions highlight the importance of full compliance with the following provisions of the DFS regulation:

- Multi-factor Authentication (500.12): Breaches occur more easily when the company does not have multi-factor authentication in place, or where the multi-factor authentication protection malfunctioned. In fact, as more businesses have adopted multi-factor authentication, the Department has seen a decline of reportable events.

- Encryption (500.15): Strong access control and encryption for data in transit and at rest mitigate the loss and are critically important.

- Training (500.14): Ongoing training is essential. All staff needs basic cybersecurity training to avoid events like successful phishing scams, and ongoing reminders and training to ensure protections from errors that could have significant consequences.

Certificate of Compliance

DFS's regulation requires each entity to conduct an annual review and assessment of its cybersecurity program's achievements, deficiencies and overall compliance with regulatory standards and to certify the institution's compliance with the regulation on an annual basis. The DFS compliance certification is a critical governance pillar for the cybersecurity program of all DFS regulated entities. The first certification deadline was February 15, 2018, which was successful and provided DFS with information from which we have been working to improve our processes. DFS currently is preparing for the second annual certifications of compliance due by **February 15, 2019**. By this date, all regulated entities and licensed persons must file a Certification of Compliance covering calendar year 2018, confirming the entity or person's compliance with the DFS cybersecurity regulation. In January 2019, prior to the February 15, 2019 certification deadline, any regulated person or licensed entity that is entitled to an

exemption must file a new Notice of Exemption notifying DFS of the current exempt status. All of t**hese filings must all be filed electronically via the improved DFS cybersecurity portal.**

2019 Filing Calendar: Notices of Exemption and Certificates of Compliance

Any DFS regulated entity or licensed person that is entitled to an exemption must file a Notice of Exempt status for the calendar year 2019 prior to filing the annual certification for calendar year 2018 on February 15, 2019. This requirement applies even if you previously notified DFS of your exemption status, as the assessment of exemption status is an annual requirement.

Prior to February 15, 2019, all regulated institutions must file the annual certification of compliance, covering calendar year 2018, setting forth the institution's compliance with the cybersecurity regulation for those provisions that were applicable in 2018. The DFS Web Portal provides a secure reporting tool to facilitate compliance with the filing requirements of 23 NYCRR Part 500.

Additional information concerning the DFS cybersecurity regulation is available on the DFS Website including:

- 2019 Cybersecurity Filing Schedule
- Information concerning requirements under the cybersecurity regulation
- Step by step instructions regarding filing exemptions and compliance certifications
- FAQs and other helpful information concerning the DFS cybersecurity regulation
- Information concerning DFS Cybersecurity Secure Portal for filings

Conclusion

During the prior year, DFS and its regulated entities and licensed persons collectively have enhanced the financial services industry's cybersecurity protections for New York, providing national standards and leadership on this critically important issue. Through our ongoing supervision and examinations, DFS has noted many institutions' increased adoption of governance and system protections to protect consumers and industry data. The cybersecurity events that have been filed with DFS and any deficiencies identified through the certification and examination processes indicate both the severity of this ongoing threat, as well as the dedicated work being undertaken to combat these threats, bolster defenses, and prevent future attacks. As the DFS cybersecurity regulation reaches its final implementation deadline on March 1, 2019, and with DFS examination and supervision systems in place, DFS professionals are ready to continue to work with regulated institutions and other stakeholders to improve cybersecurity protections for New York's financial services industry.