

Bulletin No. 2021-16

July 26, 2021

RE: DFS ISSUES RANSOMWARE NOTICE

The New York Department of Financial Services (“DFS”) has published a [notice](#) to all New York State regulated entities outlining new ransomware guidance and urging new controls. The notice applies to all licensed brokers, both resident and nonresident. Although the notice is addressed to “entities” and most of the contents are more likely to be relevant to entity licensees, the DFS has clarified to ELANY that both entity and individual licensees are included.

The notice states, “[T]he Department expects regulated companies to implement these controls whenever possible” and then discusses various controls, some of which exempt licensees do not currently need to comply with under the [DFS’ cybersecurity regulation](#), and some of which are based on a section of the regulation ([500.03](#)) that does not specify now-expected controls.

The DFS has told ELANY that the notice is not intended to supersede the regulation. Instead, it is meant to accomplish two goals. First, it provides licensees with information on controls that the DFS believes are important and that the DFS expects licensees to consider implementing, depending on their risk assessments. It is important to note that the DFS views the risk assessment as controlling a licensee’s approach to cybersecurity and that licensees should be able to explain what controls they considered based on their risk assessment, and why they chose not to implement certain controls.

Second, the DFS is putting licensees on alert that the regulation will be revised, and the notice includes some of the specific requirements that will likely be included in the revision. The DFS shared with ELANY that limited exemptions will be maintained and they understand that small brokers have limited resources compared to larger licensees, however some new requirements will likely be imposed on exempt licensees. Most prominently, licensees with a limited exemption can expect the current exemption from multi-factor authentication requirements to be removed.

The DFS hopes to publish a proposed revised regulation later in 2021 with a 45-day comment period.

All current ELANY bulletins and other current ELANY publications can be found on our website at <http://www.elany.org>.

Follow ELANY



The notice states that the DFS expects all licensees to implement the following controls, subject to exemptions and individual risk assessments (based on ELANY's discussion with the DFS):

- Email filtering and anti-phishing training
- Vulnerability/patch management
- Multi-factor authentication
- Disabling Remote Desktop Protocols access
- Password management
- Privileged access management
- Monitoring and response
- Tested and segregated backups
- Incident response plan

Brokers that have filed a limited exemption pursuant to the regulation should note that the notice contains several expectations that they are currently exempt from under the regulation: cybersecurity awareness training, multi-factor authentication, periodic penetration testing, privileged access management, and an incident response plan. Again, while the notice contains no caveat for exempt licensees, the DFS has informed ELANY that the exemptions are still in effect. In addition, the DFS expects certain controls that are not specifically required by the regulation to be implemented by non-exempt brokers, such as disabling Remote Desktop Protocols access and implementation of an endpoint detection and response solution. While not currently required by the regulation, the controls outlined in the notice are what the DFS believes are important and they will be expecting an explanation, based on a licensee's risk assessment, as to why they were not implemented.

Should you have any questions regarding the content of this bulletin, please direct them to Howard Greene at hgreene@elany.org or (646) 292-5591.

All current ELANY bulletins and other current ELANY publications can be found on our website at <http://www.elany.org>.

Follow ELANY

