ELANY BULLETIN
EXCESS LINE ASSOCIATION OF NEW YORK
120 Wall Street, 24th Floor
New York, New York 10005

Bulletin No. 2025-09

March 25, 2025

RE: REVISED DFS CYBERSECURITY REGULATION – MAY 1, 2025 REQUIREMENTS

On May 1, 2025, the next set of New York Department of Financial Services (DFS) cybersecurity regulation (23 NYCRR 500) revised requirements will go into effect. Here is what brokers need to know.

1. **Brokers that have not filed a limited or full exemption** under the regulation must do the following:

   As per Section 500.5(a)(2), conduct "automated scans of information systems, and a manual review of systems not covered by such scans" to discover, analyze, and report vulnerabilities at a frequency determined by the broker's risk assessment, and promptly after any material system changes.

   Under Section 500.7, brokers must also:
   - Implement enhanced requirements regarding limiting user access privileges, including privileged account access
   - Review access privileges and remove or disable accounts and access that are no longer necessary
   - Disable or securely configure all protocols that permit remote control of devices
   - Promptly terminate access following personnel departures
   - Implement a reasonable written password policy to the extent passwords are used

   Finally, Section 500.14(a)(2) requires brokers to implement controls to protect against malicious code.

2. **Brokers that have filed a limited exemption** under Section 500.19(a) must comply only with the Section 500.7 requirements outlined above.

3. **Class A Brokers** (large organizations as defined by Section 500.1(d) of the regulation) must comply with:

   The Section 500.5(a)(2) requirements outlined above.

   The Section 500.7 requirements outlined above and additionally:
   - Monitor privileged access activity
   - Implement a privileged access management solution
   - Implement an automated method of blocking commonly used passwords for all accounts on information systems owned or controlled by the Class A company and wherever feasible for all other accounts. However, to the extent the Class A company determines that blocking commonly used passwords is infeasible, its CISO may instead approve in writing at least annually the infeasibility and the use of reasonably equivalent or more secure compensating controls.

   The Section 500.14(a)(2) requirement outlined above. In addition, they must, as per Section 500.14(b), implement an endpoint detection and response solution to monitor anomalous activity and centralized logging and security event alert solution. However, the Chief Information Security Officer may approve reasonably equivalent or more secure compensating controls, but approval must be in writing.

Should you have any questions regarding the content of this bulletin, please direct them to elanyinfo@elany.org.