ELANY BULLETIN

Excess Line Association
Of New York

120 Wall Street, 24th Floor
New York, New York 10005

Bulletin No. 2024-20
September 9, 2024

RE: REVISED DFS CYBERSECURITY REGULATION REQUIREMENTS

On November 1, 2024, 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.

Limited Exemption Standards Are Changing

Criteria to qualify for a limited exemption under Section 500.19(a) will change on November 1. The exemption will apply for licensees with any of the following:

- Fewer than 20 employees and independent contractors, including its affiliates
- Less than $7,500,000 in gross annual revenue in each of the last three fiscal years from all business operations of the licensee and the business operations in New York of the licensee's affiliates
- Less than $15,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all affiliates

Reminder: All full and limited exemptions must be filed with the DFS

New requirements for brokers that have not filed an exemption:

Chief Information Security Officer (CISO) (Section 500.4)

- The CISO's written report to the senior governing body must be updated to include plans for remediating material inadequacies.
- The CISO is required to timely report to the senior governing body or senior officers(s) on material cybersecurity issues, such as significant cybersecurity events and significant changes to the cybersecurity program.
- The senior governing body of the licensee must exercise oversight of the licensee's cybersecurity risk management, including:
    - Having sufficient understanding of cybersecurity-related matters to exercise such oversight, which may include the use of advisors
    - Requiring executive management or its designees to develop, implement, and maintain the licensee's cybersecurity program
    - Regularly receiving and reviewing management reports about cybersecurity matters
    - Confirming that the licensee's management has allocated sufficient resources to implement and maintain an effective cybersecurity program

Encryption (Section 500.15)

- A licensee must implement a written policy requiring encryption that meets industry standards
- Nonpublic information **in transit** over external networks must be encrypted.
- The use of effective compensating controls for encryption of nonpublic information **at rest** that have been approved by the CISO may continue to be used, but that approval must now be in writing and reviewed at least annually by the CISO

Incident Response and Business Continuity (Section 500.16)

- Incident response plans must contain proactive measures to investigate and mitigate cybersecurity events and ensure operational resilience, including incident response, business continuity, and disaster recovery plans
- Incident response plans must address:
    - The goals of the plan
    - The internal processes for responding to a cybersecurity event
    - Recovery from backups
    - The preparation of root cause analysis that describes how and why the event occurred, what business impact it had, and what will be done to prevent reoccurrence
    - Updating the plan as necessary
- Business continuity and disaster recovery plans (BCDR) must be reasonably designed to ensure the availability and functionality of the licensee's information systems and material services and protect the covered entity's personnel, assets and nonpublic information in the event of a cybersecurity-related disruption to its normal business activities. The BCDR must:
    - Identify documents, data, facilities, infrastructure, services, personnel and competencies essential to the continued operations of the covered entity's business
    - Identify the supervisory personnel responsible for implementing each aspect of the BCDR plan
    - Include a plan to communicate with essential persons in the event of a cybersecurity-related disruption to the operations of the covered entity, including employees, counterparties, regulatory authorities, third-party service providers, disaster recovery specialists, the senior governing body and any other persons essential to the recovery of documentation and data and the resumption of operations
    - Include procedures for the timely recovery of critical data and information systems and to resume operations as soon as reasonably possible following a cybersecurity-related disruption to normal business activities
    - Include procedures for backing up or copying, with sufficient frequency, information essential to the operations of the covered entity and storing such information offsite
    - Identify third parties that are necessary to the continued operations of the covered entity's information systems
- Each licensee shall ensure that current copies of the plans or relevant portions therein are distributed or are otherwise accessible, including during a cybersecurity event, to all employees necessary to implement such plans
- Each licensee shall provide relevant training to all employees responsible for implementing the plans regarding their roles and responsibilities

- Each licensee shall, at least annually, test its:
    - Incident response and BCDR plans with all staff and management critical to the response, and revise the plan as necessary
    - Ability to restore its critical data and information systems from backups
- Each licensee shall maintain backups necessary to restore material operations. The backups shall be adequately protected from unauthorized alterations or destruction

For brokers that have filed a 500.19(a) exemption, these are the new requirements:

Multi-factor Authentication (Section 500.12(a))

- Multi-factor authentication must be utilized for:
    - Remote access to the licensee's information systems
    - Remote access to third-party applications, including those that are cloud based, from which nonpublic information is accessible
    - All privileged accounts other than service accounts that prohibit interactive login. [Privileged account means any authorized user account or service account that can be used to perform security-relevant functions that ordinary users are not authorized to perform, including but not limited to the ability to add, change or remove other accounts, or make configuration changes to information systems. Section 500.01(n)]

Cybersecurity Awareness Training (Section 500.14(a)(3))

- A licensee must provide periodic, but at a minimum annual, cybersecurity awareness training that includes content on social engineering for all personnel
- Training must be updated to reflect risks identified by the licensee in its risk assessment

If you have any questions, please email ElanyInfo@elany.org. Please ensure the domain @elany.org is not blocked by your spam filter.