COMPLIANCE
ADVISOR

NEW YORK CYBERSECURITY REGULATION COMPLIANCE GUIDE

A PUBLICATION BY

THE EXCESS LINE ASSOCIATION
OF NEW YORK

One Exchange Plaza • 55 Broadway

29th Floor

New York, New York 10006-3728

Telephone: (646) 292-5500

E-MAIL: elany@elany.org • www.elany.org

January 2018

The New York Department of Financial Services published its Cybersecurity Requirements For Financial Services Companies regulation (**23 NYCRR 500**) effective March 1, 2017. THE REGULATION APPLIES TO ALL NEW YORK-LICENSED EXCESS LINE BROKERS — FIRMS AND INDIVIDUALS, RESIDENT AND NON-RESIDENT, REGARDLESS OF LINES OF INSURANCE BROKERED.

The following are the highlights for New York-licensed excess line brokers. A hyperlink to the regulation appears above for more in-depth detail regarding requirements. Each requirement is accompanied by its initial compliance date and the regulation section number being discussed. In addition, requirements that apply to exempt licensees are noted.

LIMITED EXEMPTIONS (10/30/17, SECTION 500.19)

The regulation provides for limited exemptions:

500.19(a) applies to New York-licensed excess line brokerages that are below specified thresholds in either number of employees located or responsible for business in New York, gross annual revenue from New York operations in each of the last three fiscal years, or total assets. Any licensee that qualifies for a Section 500.19(a) exemption need only comply with specified requirements, but these include substantial items such as implementation of a cybersecurity program and policy, and performing periodic risk assessments. Licensees that neither maintain Information Systems[1] nor possess Nonpublic Information[2] may avail themselves of a limited exemption under Section 500.19(c) and need only comply with a subset of the 500.19(a) exemption requirements.

Section 500.19(b) offers a total exemption for licensees that are fully covered by the cybersecurity program of another covered entity' such as an individual broker who works for a firm that is licensed in New York. However, licensees claiming this exemption must still file a Notice of Exemption.

Licensees qualifying for an exemption must file on the New York Department of Financial Services **cybersecurity web portal**.[3] Filing is a notification mechanism; brokers do not receive "approval" from the Department of Financial Services." The initial deadline for filing for an exemption was October 30, 2017 but if a qualifying licensee missed the deadline, we suggest filing as soon as possible. A fresh exemption filing is required for any changes to exemption status.

CERTIFICATION OF COMPLIANCE (2/15/18, SECTION 500.17(B)) – APPLIES TO SECTION 500.19(A)/(C) EXEMPTS

Licensees must file the first annual Certification of Compliance by February 15th attesting to full compliance with the requirements of the regulation that were applicable to the licensee during 2017. Individuals with a Section 500.19(b) exemption do not need to certify. Certifications should be filed on the New York Department of Financial Services **cybersecurity web portal**.[4] Submission of supporting documentation is not required. The Chair of the Board of Directors or a Senior Officer(s) must execute the Certification. Certifications filed during 2017 are ineffective and must be resubmitted.

CYBERSECURITY PROGRAM (8/28/17, SECTION 500.02) — APPLIES TO SECTION 500.19(A) EXEMPTS

Licensees must maintain a Cybersecurity Program that is based on a licensee's Risk Assessment (discussed later) and must be focused on identifying, preventing, detecting, responding to, recovering from and reporting Cybersecurity Events.[5] All information related to a Program must be made available to the New York Superintendent of Financial Services upon request.

CYBERSECURITY POLICY (8/28/17, SECTION 500.03) — APPLIES TO SECTION 500.19(A) EXEMPTS

Licensees must have a written Cybersecurity Policy that is approved by a Senior Officer, the Board of Directors, a committee of the Board, or an equivalent governing body. The Policy must be based on the licensee's Risk Assessment (since the Risk Assessment is not due until March 1, 2018, the initial Policy need not reflect it) and document how the licensee intends to protect its Information Systems and any Nonpublic Information stored on those systems. The regulation specifies 14 areas that must be addressed to the extent possible.

RISK ASSESSMENT (3/1/18, SECTION 500.09) — APPLIES TO SECTION 500.19(A)/(C) EXEMPTS

Each licensee must conduct a periodic Risk Assessment of its Information Systems that can be used to develop its Cybersecurity Program. The Risk Assessment must consider the licensee's particular cybersecurity risks to the extent they may impact Nonpublic Information and Information Systems, and must be updated as relevant changes occur.

CHIEF INFORMATION SECURITY OFFICER (DESIGNATION OF CISO 8/28/17; CISO REPORT 3/1/18, SECTION 500.04)

Each licensee must designate a "qualified" (undefined term) Chief Information Security Officer (CISO) to implement and oversee the licensee's Cybersecurity Program and to enforce its Cybersecurity Policy. The CISO can be a third-party provider or an employee of an affiliate. ELANY recommends that exempt licensees appoint a responsible qualified individual to oversee their cybersecurity efforts even though this requirement does not apply to them under the regulation.

The CISO must report at least annually to the licensee's full Board of Directors (not a committee) or an equivalent body on the status of the Program and material risks. If there is no Board or equivalent body, the report must be made to a Senior Officer who is responsible for the licensee's Cybersecurity Program.

PENETRATION TESTING AND VULNERABILITY ASSESSMENT (3/1/18, SECTION 500.05)

A Cybersecurity Program must include monitoring and testing which is developed in accordance with the licensee's Risk Assessment and incorporates continuous

monitoring or other systems that detect vulnerabilities on a continuous basis. Manual periodic reviews of logs and firewall configurations do not qualify. In the event continuous monitoring or other similar protocols are not available, licensees must conduct annual penetration testing based on the Risk Assessment AND bi-annual vulnerability assessments, such as scans, that are designed to identify cybersecurity vulnerabilities. The first annual testing and assessment must be completed in a timely manner, but need not be completed by March 1, 2018.

AUDIT TRAIL (9/3/18, SECTION 500.06)

Each licensee must ensure, based on its Risk Assessment, that it can reconstruct material financial transactions sufficient to support normal operations AND put in place audit trails that can detect and respond to Cybersecurity Events that have a reasonable chance of harming any material part of the licensee's normal business operations.

ACCESS PRIVILEGES (8/28/17, SECTION 500.07) — APPLIES TO SECTION 500.19(A) EXEMPTS

A licensee's Cybersecurity Program must limit user access privileges to Information Systems that contain Nonpublic Information. This action must be based on the licensee's Risk Assessment and access privileges must be reviewed periodically.

APPLICATION SECURITY (9/3/18, SECTION 500.08)

Cybersecurity Programs must include written procedures, guidelines and standards to ensure the secure development of applications developed in-house, and for assessing the security of externally developed applications. These procedures, guidelines and standards must be periodically reviewed, assessed and updated as necessary by the Chief Information Security Officer or a qualified designee.

CYBERSECURITY PERSONNEL AND INTELLIGENCE (8/28/17, SECTION 500.10)

Each licensee must utilize "qualified" (undefined term) cybersecurity personnel to manage the licensee's cybersecurity risks and to perform, or oversee, the core cybersecurity functions specified by its Cybersecurity Program. Such personnel must be provided with training and updates sufficient to deal with relevant cybersecurity risks. In addition, the licensee must verify that key cybersecurity personnel take steps to maintain knowledge of changing threats and countermeasures.

THIRD PARTY SERVICE PROVIDER SECURITY POLICY (3/1/19, SECTION 500.11) — APPLIES TO SECTION 500.19(A)/(C) EXEMPTS

Licensees must implement written policies to ensure the security of Nonpublic Information and Information Security Systems that are accessible by Third Party Service Providers.[6] Policies must reflect the licensee's Risk Assessment. Licensees must perform due diligence to ensure the adequacy of Third Party Service Providers,

but sole reliance on a Third Party Service Provider's own Certification of Compliance does not constitute adequate due diligence.

A producer, employee, representative or designee of a licensee need not have his or her own Third Party Service Provider policy if they follow the policy of the licensee.

MULTI-FACTOR AUTHENTICATION (3/1/18, SECTION 500.12)

A licensee must institute controls that are based on its Risk Assessment, which may include multi-factor authentication (password + email/text code, etc.) or risk-based authentication, to protect Nonpublic Information and Information Systems. Unless the Chief Information Security Officer authorizes an alternative system that offers equivalent or greater security, multi-factor authentication must be used for anyone entering the licensee's internal network from an external network.

LIMITATIONS ON DATA RETENTION (9/3/18, SECTION 500.13) — APPLIES TO SECTION 500.19(A)/(C) EXEMPTS

Each licensee must, as part of its Cybersecurity Program, have policies and procedures for the periodic disposal of Nonpublic Information that is no longer necessary for business operations or other business purposes, subject to applicable record retention requirements. This requirement does not apply where disposal is not feasible due to the manner in which the information is maintained.

TRAINING AND MONITORING (TRAINING 3/1/18; IMPLEMENTATION OF POLICIES 9/3/18, SECTION 500.14)

As part of its Cybersecurity Program, a licensee must have policies, procedures and controls in place to both monitor the activity of authorized Information System users and detect unauthorized access or tampering with Nonpublic Information by authorized users. In addition, a licensee must provide regular cybersecurity awareness training for all personnel updated to reflect its Risk Assessment. The regulation does not define acceptable training but ELANY suggests that training include elements such as how to protect against phishing emails, CEO fraud and ransomware, as well as protecting passwords.

ENCRYPTION OF NONPUBLIC INFORMATION (9/3/18, SECTION 500.15)

Each licensee's Cybersecurity Program must implement controls based on its Risk Assessment, including encryption, to protect Nonpublic Information both in transit via external networks and at rest. If encryption of Nonpublic Information is deemed by the licensee to be infeasible, the Chief Information Security Officer may authorize other controls.

INCIDENT RESPONSE PLAN (8/28/17, SECTION 500.16)

A licensee must establish an incident response plan as part of its Cybersecurity Program to respond to Cybersecurity Events that materially impact the confidentiality, integrity or availability of the licensee's Information Systems or any part of its business.

The plan must address processes, goals, roles, communication, identification and remediation of control weaknesses, reporting and documentation, and evaluation of the plan following a Cybersecurity Event.

NOTICES TO SUPERINTENDENT (NOTICES 8/28/17, SECTION 500.17(A)) — APPLIES TO SECTION 500.19(A)/(C) EXEMPTS

Licensees must notify the Superintendent of the New York State Department of Financial Services within 72 hours following a determination that a Cybersecurity Event has occurred if notice is required to any government body, self-regulatory agency or any other supervisory body (i.e. NYS Information Security Breach and Notification Act) OR the Cybersecurity event has a reasonable likelihood of materially harming any material part of the covered entity's normal operations. A Cybersecurity Event that involves harm to consumers must be reported.

---

1 **"Information Systems"** is broadly defined and includes any electronic system that collects, processes, maintains, uses, shares, disseminates or disposes of electronic information. A broker management system or email system come under this definition.

2 **"Nonpublic Information"** is defined as all electronic information that is not publicly available and is:
- Business related information that if tampered with or breached could, or did in fact, cause a material adverse impact on the licensee
- Information about a third-party that combines a name, number, or other identifier with one of the following:
  - Social Security number
  - Driver's license or non-driver ID card
  - Account number, credit or debit card number
  - Security code, access code or password that permits access to an individual's financial account
  - Biometric records
- Health or health care information, payment for the provision of health care information

3 The Department of Financial Services may permit a firm to make a coordinated filing of Notices of Exemptions on behalf of its New York-licensed employees or captive agents. This option is only available for filings of 50 or more employees or captive agents, and only if all employees or captive agents qualify for the same exemptions. A qualifying firm should contact the Department of Financial Services at **CyberRegComments@dfs.ny.gov** from the email to which its cybersecurity portal account is associated.

4 The Big I New York has received instruction from the Department of Financial Services that LLCs, which typically have neither a Board nor Senior Officers, should look to the definition of a "Senior Officer(s)" as "the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a Covered Entity, including a branch or agency of a foreign banking organization subject to this Part." Such an individual(s) should execute the Certification and select the "Senior Officer(s)" checkbox.

5 A **"Cybersecurity Event"** is any attempt, whether successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on that system.

6 The regulation defines a **"Third Party Service Provider"** as a person or non-governmental entity that is not an affiliate of the licensee, provides services to the licensee, and is permitted to access Nonpublic Information as part of providing services to the licensees.

THE EXCESS LINE ASSOCIATION
OF NEW YORK

One Exchange Plaza • 55 Broadway

29th Floor

New York, New York 10006-3728

Telephone: (646) 292-5500

E-MAIL: elany@elany.org • www.elany.org