BOB TREUBER, EXECUTIVE DIRECTOR

NYSLTA MEMO TO MEMBERS REGARDING NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES REGULATION 23 NYCRR 500

CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

As you may be aware NYS Department of Financial Services has issued a regulation for cybersecurity (23 NYCRR 500) effective March 1, 2017. However, there are staggered dates for required compliance throughout the regulation.

The regulation requires those regulated by the DFS, including insurance companies and agents, to establish and maintain cybersecurity programs to protect consumers' personal sensitive data and to better secure the financial services industry.

All licensed title insurance agents are advised to read the regulation and become familiar with the compliance requirements. NYSLTA Members can access the regulation on the member web site in the GOVERNMENT REGULATION FILE LIBRARY http://nyslta.site-ym.com/page/GovRelations.

This memo is not intended to be a substitute for reading the regulation in its entirety. Rather, this memo is intended as a general introduction to the cybersecurity regulation and should not be viewed as legal advice or as comprehensive guidance.

Notes:

- We suspect that most agents will qualify for a limited exemption pursuant to Section 500.19. However, even if you qualify under this limited exemption you are not completely exempt from the Regulation, as this is a limited exemption only.

- Yellow highlighting of a header indicates that *this section* is entitled to the limited exemption for small business pursuant to Section 500.19.

- 180-day implementation (August 28, 2017) requirement from effective date (March 1, 2017), unless otherwise noted below.

Section 500.00 Introduction:

- " … Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted, while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances. Accordingly, this regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization's cybersecurity program and file an annual certification confirming compliance with these regulations. A regulated entity's cybersecurity program must ensure the safety and soundness of the institution and protect its customers…."

Section 500.01 Definitions:

- This section defines 14 key terms used throughout the regulation. A few being as follows:
    - (c) Covered Entity is "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law." Person is defined as "any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association."
    - (g) Non Public Information (NPI) – All electronic information that is not publicly available information and is: 1) business related information that the tampering with would cause a materially adverse impact on your business AND 2) Personal information limited to SSN, driver's license no, credit card no., password, biometric records in *combination with* name or number, etc. Personal information applies only to individuals, not corporations or other entities.
    - (h) Penetration Testing language includes *by attempting unauthorized penetration of databases or controls from the Covered Entity (CE) IT system*
    - (i) Definition of Person excludes governmental entities.

Section 500.02 Cybersecurity Program:

- Each Covered Entity ("CE") shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the CE's Information Systems. The key parts of your cybersecurity program are: detect, respond, recover and report. (500.02 § 3,4,5,6)

Section 500.03 Cybersecurity Policy:

- Each CE shall implement and maintain a written policy or policies, approved by a Senior Officer or the CE's board of directors.

Section 500.04 Chief Information Security Officer:
(1 YEAR IMPLEMENTATION DATE; FEBRUARY 28, 2018 for Section 500.04(b))

- Each Covered Entity shall designate a qualified individual (a Chief Information Security Officer, CISO) responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy…
- (b) the CISO to make a written report to the board at least annually of "material cybersecurity events".
- CISO can be employed or be a third party.

Section 500.05 Pen Testing and Vulnerability Assessments:
(1YEAR IMPLEMENTATION DATE; FEBRUARY 28, 2018)

- Requires annual Penetration Testing and bi-annual vulnerability assessments to be developed in accordance with the CE's risk assessment; offers CE's additional access-control options beyond multifactor authentication. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, CE's shall conduct annual Penetration Testing of the CE's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the CE's Information Systems based on the Risk Assessment.

Section 500.06 Audit Trail:
(18 MONTH IMPLEMENTATION DATE; AUGUST 30, 2018)

- Regulation requires audit trails which are designed to: reconstruct material financial transactions sufficient to support normal operations and obligations of the CE (5 years); detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity (3 years).

Section 500.07 Access Privileges.

- This section uses "Risk Assessment" to consider limiting access privileges to NPI.

Section 500.08 Application Security:
(18 MONTH IMPLEMENTATION DATE; AUGUST 30, 2018)

- CE's cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications, and procedures for evaluating the security of externally developed applications.
- All such procedures, guidelines and standards shall be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the CE.

Section 500.09 Risk Assessment:
(1 YEAR IMPLEMENTATION; FEBRUARY 28, 2018)

- CE to conduct a periodic Risk Assessment and the CE's cybersecurity program to be updated as reasonably necessary.

Section 500.10 CS Personnel and Intelligence

- Each CE shall utilize qualified cybersecurity personnel OR third party providers and provide them with cybersecurity updates and training sufficient to address relevant cybersecurity risks; and verify that key cybersecurity personnel or third party providers take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

Section 500.11 Third Party Service Provider Security Policy:
(2 YEAR IMPLEMENTATION; MARCH 1, 2019)

- Each CE shall implement written policies and procedures designed to ensure the security of Information Systems and NPI that are accessible to, or held by, Third Party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the CE.

Section 500.12 Multi-Factor Authentication:
(1 YEAR IMPLEMENTATION; FEBRUARY 28, 2018)

- Risk Assessment by CE to determine whether Multi-Factor Authentication should be used as part of the entity's effective controls of its information. CISO may propose alternate secure controls for access to internal networks from external networks. Note: Open to interpretation based on Risk Assessment.

Section 500.13 Limitations on Data Retention:
(18 MONTH IMPLEMENTATION DATE; AUGUST 30, 2018)

- Each CE must have policies and procedures in place for the secure disposal on a periodic basis of any Nonpublic Information. Data must be disposed of when no longer necessary

for business operations or for other legitimate business purposes, except where targeted disposal is not reasonably feasible.

Section 500.14 Training and Monitoring:
(a) (18 MONTHS IMPLEMENTATION; AUGUST 30, 2018)
(b) (1 YEAR IMPLEMENTATION; FEBRUARY 28, 2018)

- Each CE a) must implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with NPI by such Authorized Users; and (b) each CE must conduct regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment.

500.15 Encryption of NPI:
(18 MONTH IMPLEMENTATION DATE; AUGUST 30, 2018)

- Each CE shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.
- If encryption is infeasible the CE may use effective controls approved by CISO.
- CISO to review above method annually.

Section 500.16 Incident Response Plan:

- Each Covered Entity shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations.

Section 500.17 Notices to Superintendent:

- Requires that regulated entities notify the DFS of an incident within 72 hours of *determining* that a cyber event has transpired. Part (b) of this section requires an annual written statement to the superintendent by February 15th. See sample form annexed.

Section 500.18 Confidentiality:

- States that "information provided…is subject to exemptions from disclosure under…" various laws.

Section 500.19 Exemptions:

- Known as the small business LIMITED exemption –applicable to most agents.
- Limited exemption applicable if:

    - fewer than 10 employees OR
    - less than 5 million in revenue the last 3 years OR
    - less than 10 million in assets in the last 3 years); must have more than 10 million in assets (NOT annual revenue) to require compliance with all the regulation provisions.
- If CE meets one of the above criteria then exempt from sections 500.04, 500.05, 500.06, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of the regulation.
- Under subsection (b), an employee, agent or representative of another CE is exempt from the regulations to the extent that it is covered under that CE's Cybersecurity Program.
- Under subsection (c), if a CE does not operate any Information Systems and does not control or possess NPI, it is exempt from Sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15 and 500.16.
- Form (Notice of Exemption) to be filed if exempt. Notice of Exemption has to be filed within 30 days of determining that you are exempt (realistically, within the 180-day effectiveness period). See sample form annexed.

Section 500.20 Enforcement:

- This regulation will be enforced by the superintendent.

Section 500.21 Effective Date:

- March 1, 2017.
- Certificate of Compliance is required commencing February 15, 2018.

Section 500.22 Transitional Periods:

- CE's shall have 180 days from the effective date of this Part to comply with the requirements set forth in this Part, except as otherwise specified.
- The following provisions shall include additional transitional periods. CE's shall have:

    - 1 year from the effective date of this Part to comply with sections 500.04(b), 500.05, 500.09, 500.12, and 500.14
    - 18 months from the effective date of this Part to comply with sections 500.06, 500.08, 500.13, 500.14 (a) and 500.15
    - Two years from the effective date of this Part to comply with section 500.11.

SEE ANNEXED FOR SAMPLE REQUIRED FORMS TO BE FILED

Dated: March 3, 2017
Prepared by: JMP/WLC/RGT

COMPANY LETTERHEAD

Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations (Pursuant to Section 500.17)

RE: ABC Title Agency, LLC

February 15, 20XX*

* Must be submitted by February 15th each year

The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:

The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;

(1) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the

Cybersecurity Program of (ABC Title Agency, LLC) as of x/x/2xxx (date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended 2xxx (year for which Board Resolution or Compliance Finding is provided) complies with Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York.

Very truly yours,

NAME, TITLE and DATE
Signed by the Chairperson of the Board of Directors or Senior Officer(s)

For DFS Portal Filing Instructions see:
http://www.dfs.ny.gov/portal.htm

Dated: March 3, 2017
Prepared by: JMP/WLC/RGT

COMPANY LETTERHEAD

Notice of Exemption

ABC Title Agency, LLC

March 1, 2017

In accordance with 23 NYCRR § 500.19, ABC Title Agency, LLC hereby provides notice that ABC Title Agency, LLC qualifies for the following Exemption(s) under 23 NYCRR § 500.19 (check all that apply):

- ☐ Section 500.19(a)(1)
- ☐ Section 500.19(a)(2)
- ☐ Section 500.19(a)(3)
- ☐ Section 500.19(b)
- ☐ Section 500.19(c)
- ☐ Section 500.19(d)

If you have any question or concerns regarding this notice, please contact: NAME, TITLE PHONE NUMBER, EMAIL ADDRESS

Very truly yours,

NAME, TITLE and DATE

For DFS Portal Filing Instructions see:
http://www.dfs.ny.gov/portal.htm

Dated: March 3, 2017
Prepared by: JMP/WLC/RGT