**New York State Department of Financial Services (“DFS”)**

**Cybersecurity Requirements for Financial Services Companies**

***What Small Title Agents Need to Know about the NYS DFS Cybersecurity Regulations***

**By: Christopher Gulotta, Esq., CIPP**

**Founder & CEO Real Estate Data Shield, Inc.**

The Amended NYS DFS Cybersecurity Regulations (the “Regulations”) became effective March 1, 2017. For the smaller agents, who come under the §500.19 exemptions, here are 10 critical compliance requirements, deadlines and considerations to keep in mind:

1. These Regulations are now effective. Yet the compliance journey is a long and tedious one and cannot be achieved overnight. It’s imperative that you understand what’s expected and start preparing now. Most title or settlement agents we work with who actively commit the time, capital and resources necessary, still require 3-6 months to become ALTA Best Practice and Information Security certified.
2. The Regulations are the first comprehensive “state” regulations to address the rising cybersecurity threats and risks. Other states will surely follow suit. While many of the requirements of these Regulations are already considered best practices under existing federal law (Gramm Leach Bliley Act or “GLBA”)) and federal regulations (FTC Privacy, Safeguard & Disposal rules), other requirements exceed the mandates of federal laws and regulations.
3. The scope of the protected information, is broader than GLBA’s personally identifiable financial information and includes: all nonpublic electronic information (even if it’s not personally identifiable or financial in nature), if its: (i) business related information “the tampering with which or unauthorized access or use of which would cause a material adverse impact to the business, operations or security of the Covered Entity”; or (ii) information concerning an individual which because of a unique identifier, can be used to identify a person.
4. The small Covered Entities exemptions (see: §500.19(a)(1)(2)&(3)), are defined generally as Covered Entities with: (1) fewer than 10 employees (including independent contractors), located in New York or responsible for the business of the Covered Entity; or (2) less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations; or (3) less than $10,000,000 in year-end total assets (calculated in accordance with GAAP). These “small” Covered Entities may be “exempt” from the more onerous requirements of the Regulation, but must still must comply with Sections: 500.02 (Cybersecurity Program); 500.03 (Cybersecurity Policy); 500.07 (Access Privileges); 500.09 (Risk Assessment); 500.11 (Third Party Service Provider Security Policy); 500.13 (Limitations on Data retention); 500.17 (Notices to Superintendent). And such small/exempt Covered Entities are still required to file the Notice of Exemption and all other Notices. It is important to note that merely because a title agency comes under the DFS small Covered Entity exemptions, does not mean they are exempt from GLBA or FTC Privacy, Safeguard or Disposal rule requirements.
5. Risk Assessments are critical under the regulations. Not only are such assessments required, but they are the documented basis for each Covered Entity to: (i) evaluate and categorize the identified cybersecurity risks or threats facing the Covered Entity; (ii) evaluate the confidentiality, integrity, security and availability of the Covered Entity’s Information Systems including the adequacy of existing controls; and (iii) establish how such risks will be mitigated and ho the cybersecurity program will address such risks.
6. Each Covered Entity, large or small (exempt or non-exempt) has to develop written policies and procedures to ensure that any Third-Party Providers with access to the Entity’s systems and Nonpublic information are included in the company Risk Assessment. “Minimum cybersecurity practices” must be met, initial and on-going due diligence and oversight are expected of the Covered Entity to confirm the Third Party Provider has their own policies and procedures for access controls, multi-factor authentication and incident response.
7. Timeline for Small/Exempt Covered Entities: (i) Effective Date of Regulations: March 1, 2017; (ii) Transitional Period ends: August 28, 2017; (iii) Notice of exception (Appendix B to the Regulations) must be filed within 30 days of the determination that the Covered Entity is exempt; and (iv) Certificate of Compliance must be filed on February 15th of each year for the prior year (Appendix A to the Regulations) (must be signed by the Chairperson of the Board of Directors or a Senior Officer); (v) March 1, 2018: Risk Assessment as prescribed in §500.09; (vi) October 1, 2018: Written policies and procedures for the periodic disposal of Nonpublic Information (see §500.13); and (vii) March 1, 2019: Develop a Third Party Service Provider Security Policy (see §500.11).
8. Incidence response: pursuant to §500.17, a Covered Entity must notify the superintendent “as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity event has occurred.”
9. Compliance Recommendations: Start now! The best place to start is with a risk assessment, preferably from an independent third party familiar with both the DFS regulations and with the internal work flows, process and data flows of title agents.
10. Recommended resources: ALTA has developed Best Practices 2.0 (2012) for Title Insurance & Settlement Agents. Pillar 3 and the recommendations contained therein, represent a great starting point for information security compliance. Title insurance underwriters also offer compliance solutions through educational webinars and Best Practice web pages and resource portals.

Conclusion

August 28, 2017 is less than five (5) months away. Each company will have its own timing challenges to meet the basic requirements of 23 NYCRR 500 based largely on their current compliance posture. Having an independent company assess your current risk posture, identify gaps and work with your IT and management teams to timely and compliantly bridge the gap is critical. Remember, in February of 2018, only 10 months away, *you* may be signing a NYS DFS Certification opining on your company meeting all the applicable DFS Cybersecurity requirements.

**Christopher Gulotta, Esq., CIPP, is the founder of Real Estate Data Shield, Inc., a New York based information security and compliance consulting company for title & settlement agents. Mr. Gulotta has over 25 years of title and settlement experience and is a Certified Information Privacy Professional. REDS offers security compliance solutions including web-based staff training, information security policy templates and Fractional CISO consulting services.**