First Cybersecurity Enforcement Action Filed by the New York Department of Financial Services

By: Jason Carney, Robert Goodall, and JJ Bollozos

In late July, the New York State Department of Financial Services (NYDFS) filed its first enforcement action under the 23 NYCRR Part 500 cybersecurity regulation (the Regulation), which was implemented in March 2017 as part of the agency's overall regulation of financial services companies. The action was filed against First American Title Insurance Company.

This Client Alert addresses the scope of the Regulation, the claims made in the enforcement action, and things to consider within Thomson Reuters (TR) in light of this action. Of note, even if TR is not directly regulated by the NYDFS in most of its businesses, TR may still be subject to the Regulation as a service provider to those customers that are in scope of the NYDFS. (*Note*: myPay Solutions is subject to the NYDFS's jurisdiction.) In addition, the Regulation and how the NYDFS enforces its requirements may provide insight into how other agencies, like the Federal Trade Commission (FTC), enforce similar laws and regulations.

1. What is the scope of the NYDFS Regulation?

The NYDFS Regulation became effective as of March 1, 2017 and includes 23 sections outlining prescriptive cybersecurity requirements for all "Covered Entities" doing business in New York. The "Covered Entities" in scope of the NYDFS Regulation are all entities operating or required to operate under a NYDFS license, registration, or charter or who are otherwise regulated by the NYDFS.[i] Typical Covered Entities include insurance companies, mortgage companies, state-chartered banks, private banks, foreign banks licensed to operate in New York, and licensed lenders.[1]

Importantly, the Regulation also applies to the third-party vendors and service providers to Covered Entities.

The Regulation governs "Nonpublic Information" (NPI), which is broadly defined as any electronic information that is not made publicly available via governmental records.[ii]

2. What does the NYDFS Regulation require?

The Regulation requires Covered Entities to assess their organization's cybersecurity risks and develop an effective cybersecurity program to proactively mitigate risks to NPI and their IT systems by implementing several controls, such as:

- **CISO & Personnel**: Appointing a qualified Chief Information Security Officer (CISO) and employing other qualified cybersecurity personnel, in which the CISO must annually report to the Board of Directors on the state of the cybersecurity program and material risks to the company's NPI and IT systems;[iii]

---

[1] ***Note on the limited exemptions***: Under Section 19 of the Regulation, organizations that employ less than ten employees, that have less than $5 million in gross annual revenue in each of the past three years from New York operations, or that hold less than $10 million in total assets at year-end are exempted from the Regulation. Additionally, licensed persons who are following the cybersecurity program of another regulated company or those who do not have any "Information Systems" and "Nonpublic Information" are also exempted. Note that entities or persons claiming exemption must file an Initial Notice of Exemption with the NYDFS prior to the annual certification date, which is usually by the following April 15th after the then-current certification year.

- **Policies & Procedures**: Maintaining policies and procedures for the protection of NPI and the IT systems that house NPI, including addressing topics from general information security to governance to specific controls to limited data retention to an incident response plan;[iv]
- **Organizational Controls**: Implementing organizational security controls, such as risk assessments, training and monitoring for all employees and users, access-based privileges, service provider oversight, and sound governance processes with direct oversight by senior management;[v]
- **Technical Controls**: Implementing technical security controls, such as application security, encryption, multifactor authentication, and audit/log trails;[vi] and
- **Monitoring & Testing**: Continuously evaluating the risks threatening the security of NPI and IT systems (including those systems accessed or held by third-party service providers) through ongoing monitoring and testing, such as through annual penetration testing, vulnerability assessments, monitoring of employees/users and service providers, and risk assessments.[vii]

Section 500.17 requires Covered Entities to notify the superintendent of a Cybersecurity Event "as promptly as possible ***but in no event later than 72 hours***"[viii] (emphasis ours). It is important to note that "Cybersecurity Event" is defined as "any act ***or attempt***, successful ***or unsuccessful***, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System"[ix] (emphasis ours); however, the notification requirement only attaches to those events that either (1) are reportable to another governmental, self-regulatory agency, or supervisory body or (2) have a reasonable likelihood of causing material harm to any material part of the normal operations of the Covered Entity.

Finally, each Covered Entity must certify – on an annual basis, by February 15th each year – that it has complied with the Regulation over the past year.[x]

The Regulation itself does not outline potential fines and, as they are not currently calculated for this first enforcement action, we have yet to see what fines would be assessed for companies that violate the Regulation; however, some say that fines are likely to mirror those provided under the NY Banking Law and, therefore, could be up to $75,000 per day of non-compliance.

3. What does this enforcement action against First American Title Insurance Company say?

The NYDFS alleges that First American Title Insurance Company (First American) failed to safeguard customer Nonpublic Information (NPI), which is any electronic information that is not made publicly available in governmental records[xi], as required by the Regulation. In the normal course of its business, First American possessed several hundred million title records, many of which included social security numbers, and credit card numbers.[xii] Nearly 200 million of these records were allegedly stored in a system facing the public internet, in which they could be accessed without authentication via a vulnerability that was easy to exploit.[xiii] More than 5,000 documents were allegedly exposed long enough to be cached and indexed by public search engines.[xiv]

The NYDFS conducted an examination once First American reported the security incident to the NYDFS. Upon examination, the NYDFS found that the vulnerability existed since 2014[xv] and it was detected by internal resources in 2018.[xvi] However, First American only first reported the incident to the NYDFS in May 2019[xvii] and only after being alerted to it by a prominent security researcher.[xviii]

The NYDFS outlines the violations with such particularity that it warrants a detailed review of the action notice, but, at a high-level, the NYDFS alleged that First American failed to maintain an effective:

a) Cybersecurity program;[xix]
b) Risk assessment process;[xx]

c) Compliance program for internal policies;[xxi]
d) Process for access-based restrictions to NPI;[xxii] and
e) Security awareness training program.[xxiii]

4. Why is this enforcement action important?

As the first enforcement action by the NYDFS under the Regulation, this may be the start of a trend by the NYDFS to increase its regulatory activity in this space to ensure companies are actually adhering to its requirements.

In addition, NYDFS's jurisdiction includes substantially all financial and insurance businesses doing business in New York. Because American banking and financial services industries tend to concentrate in New York, this regulation will indirectly apply to many financial services (and their service providers) across the entire country. (Note that, in this case, First American operates in New York via a California corporation.)

Outside of the direct implications on Covered Entities, this Regulation broadly influences both non-financial industries' and various regulators' approach to cybersecurity measures.[xxiv] As such, the actions taken by the NYDFS become an additional source of regulatory and financial risk to all companies. Already, the Federal Trade Commission's upcoming GLBA update is reportedly taking a cue from NYDFS as a "safeguard rule" is being proposed that would mimic some of specific control provisions (specifically, Sections 500.02-17) in the NYDFS Regulation.

5. What actions should companies take to avoid similar actions?

While the NYDFS Regulation applies to Covered Entities today, this first enforcement action is still evolving and additional facts are expected to be alleged by First American in due course. Regardless, TR should consider taking these three steps to lower their potential exposure under the NYDFS or similar regulations:

i. Figure out where you are, and carry it forward.

Benchmark your current cybersecurity program against this emerging enforcement action and the underlying Regulation. Sections 500.02-500.16 explicitly outline the list of controls that NYDFS expects Covered Entities to implement across their organization. It is a concise list that will (or should) easily map to your list of current security controls.

Carry the analysis forward by identifying the issues your organization is managing that relate to the Regulation and NYDFS's expectations. Consider the state of your remediation for these controls and decide whether your exposure level is acceptable in the context of this and similar enforcement actions.

ii. Sweat the small stuff.

This enforcement action implies that First American's problems were, in part, rooted in flagrant disregard to the risk of the vulnerability at hand. Many of the charges, however, could be common occurrences in many companies so it is important to stay vigilant and maintain your focus on common-sense hygiene principles that are foundational to your cybersecurity program.

Here are some questions to consider:

- Where are your risk assessments? And if you don't know, why not?
- What are the risks outlined in these assessments and have you classified them appropriately?

- Can you determine whether a given remediation is on track? Are the remediation timelines too long in light of the risk?
- Have you cross-walked your controls against the checklist requirements of the Regulation?
- When were your information security policies last updated? Have they been updated to align with new risks and threats to your company?
- When new employees acclimate to your environment, do they tend to have the same concerns (*e.g.*, isn't this "public information?", "why isn't [x] done?")?
- Would you trust your company with your own NPI? If not, why not and what can you do to fix the issues?

Importantly, if vulnerabilities are discovered then you should immediately investigate, ring-fence, and resolve the noted weaknesses.

*iii. Ensure an external party doesn't force **your** hand.*

A powerful wrinkle in this enforcement action is that the incident was only escalated to the NYDFS when an influential security researcher, Brian Krebs, discovered the vulnerability and wrote about it on his Krebs on Security blog. In Krebs's May 2019 post, he detailed conversations he had with First American stakeholders and made it plain that the vulnerability had a broad applicability.

Coincidentally and despite First American first discovering the vulnerability in 2018, First American didn't report this as an incident to the NYDFS until May 2019 even though Section 500.17 requires companies like First American to notify the superintendent of a Cybersecurity Event "as promptly as possible but in no event later than 72 hours."[xxv] This is likely no coincidence.

External researchers can bolster a firm's security, but they can also ruin somebody's day. Check your notification processes and incident response plans to ensure it accounts for the notice procedures and timelines in all laws and regulations that apply to your businesses. How would yours handle this scenario?

---

[i] 23 NYCRR Part 500 §500.01(c)
[ii] 23 NYCRR Part 500 §500.01(g)
[iii] Id. at §§500.04(a)-(b), 500.10, & 500.14
[iv] Id. at §§500.03, 500.13, & 500.16
[v] Id. at §§500.02, 500.03, 500.07, 500.09, 500.10, 500.11, & 500.14
[vi] Id. at §§500.06, 500.08, 500.12, & 500.15
[vii] Id. at §§500.05, 500.06, 500.09, 500.10, 500.11, & 500.14
[viii] Id. at §§500.17
[ix] Id. at §§500.01(d)
[x] Id. at §§500.17
[xi] Id. at §§500.01(g)
[xii] In re: First Am. Title Ins. Co., NYDFS Statement of Charges and Notice of Hearing, No. 2020-0030-C ¶18.
[xiii] Id. at ¶24.
[xiv] Id.
[xv] Id. at ¶2.
[xvi] Id. at ¶5.
[xvii] Id. at ¶35.
[xviii] Id.
[xix] Id. at ¶38.
[xx] Id. at ¶39.
[xxi] Id. at ¶25.
[xxii] Id. at ¶45.
[xxiii] Id. at ¶52.
[xxiv] See New York State Department of Financial Services, *Department of Financial Services Announces Cybersecurity Charges Against a Leading Title Insurance Provider for Exposing Millions of Documents with Consumers' Personal Information*, 22 July 2020, https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202007221.
[xxv] 23 NYCRR Part 500 §500.17