



Cybersecurity Programs Will Become Increasingly Scrutinized By The Insurance Regulators; NY And NAIC Rules Explained

By Daniel A. Cotter

A. New York Cybersecurity Regulation

On March 1, 2017, 23 NYCRR 500¹ became effective. The New York Cybersecurity Regulation applies to anyone “operating under a license, registration, charter, certificate, permit, accreditation or similar authorization under” the banking law, insurance law, or financial services law of the State of New York. However, for certain small organizations, they are exempt.² Until last summer, no known enforcement action had been initiated by New York pursuant to 23 NYCRR 500. That all changed on July 21, 2020, when the New York Department of Financial Services (“NYDFS”) filed an action against First American Title Insurance Company and then amended the same³.

According to the statement of charges: “From at least October 2014 through May 2019, due to a known vulnerability on Respondent’s public-facing website (the “Vulnerability”), these records were available to anyone with a web browser.” The records included “bank account numbers and statements, mortgage and tax records, Social Security numbers, wire transaction receipts, and drivers’ license images.”⁴ The charges allege that even after learning of the Vulnerability in 2018, First American did not remediate it for a period of time. The charges refer to journalist Brian Krebs report that First American “had exposed 885 million documents — dating as far back as 2003 and many containing NPI — by rendering the documents openly accessible to the public.”⁵

After setting out the facts in detail, the NYDFS charged First American with violations of: 1) 23 NYCRR 500.02 (maintenance of cybersecurity program), 2) 23 NYCRR 500.03 (written policy or policies), 3) 23 NYCRR 500.07 (limit user access privileges), 4) 23 NYCRR 500.09 (periodic risk assessment), 5) *N.Y. Comp. Codes R. & Regs. tit. 23, § 500.14(b)* (cybersecurity awareness training), and 6) *N.Y. Comp. Codes R. & Regs. tit. 23, § 500.15* (implantation of controls, including encryption).

NYDFS’ regulated entities, and insurers in other jurisdictions which have enacted versions of the NAIC cybersecurity model law, will watch this action closely. The NYDFS often has been a leader in the development and enforcement of laws that have spread to other states. Businesses who fall under the oversight of the

[Read more on page 16](#)



Cotter

Daniel A. Cotter

Howard and Howard, PLLC

Dan Cotter, Esq. is an attorney with the firm of Howard and Howard, PLLC, Chicago Illinois. He is a member of the ABA TIPS Insurance Regulation Committee. Mr. Cotter speaks about cybersecurity on ABA TIPS IRC podcast available on demand- see ABA TIPS website

New York State Enacts First Regulation Of Cybersecurity Programs And Enforces Fine Against New York Company in 2020; Other States To Follow In Trend To Regulate Cybersecurity



Cybersecurity... continued from page 5

NYDFS should review their cyber policies and practices to ensure they are in good shape in light of the regulations that have been in place for more than three years and have begun to be enforced by the NYDFS.

While the First American action is the first action against an insurer for alleged violations of 23 NYCRR 500, it was not the first action. In March 2021, the NYDFS entered into a consent order⁶ with Residential Mortgage Services, Inc., a mortgage banker and mortgage servicer licensed in New York. The NYDFS, unlike most departments of insurance, regulates a variety of other financial services companies.⁷

B. NAIC Model Insurance Data Security Model Law

In late 2017, after much discussion and in large part based on the New York Cybersecurity Regulation, the NAIC adopted the Model Insurance Data Security Model Law.⁸ To date, eleven states have adopted the Model Law (often with modifications).⁹ That includes three states that adopted the Model Law during 2020: Virginia on March 10, 2020;¹⁰ Indiana on March 20, 2020;¹¹ and, Louisiana on June 11, 2020.¹² At least five other states are considering adopting the Model Law.¹³

In 2019, Maryland adopted a code provision and issued a bulletin¹⁴ dealing with data security, but it is not as detailed or formal as the Model Law.¹⁵

Insurance regulators continue to focus on cybersecurity and privacy obligations of those companies they regulate. We expect more states to adopt the Model Law in coming years, as the issue of computer hacks continues to grow.

For example, in March 2021, CNA Financial suffered a “sophisticated cybersecurity attack” that crippled the large insurer for several days.¹⁶ Regulators might consider the Model Law to address the needs of insurers to protect themselves.

Conclusion

Cybersecurity is a continued area of law where all organizations, including insurers, face increased attacks and danger due to hackers. The 23 NYCRR 500 and Model Law initiatives are attempts by regulators to ensure that insurance organizations have in place robust cybersecurity programs and processes to help prevent major breaches. ➤

NAIC Has Created A Model Law, Which Many States Are Adopting; Other States Are Creating Their Own Rules To Combat Sophisticated Cybersecurity Attacks



Endnotes

- 1 N.Y. COMP. CODES R. & REGS. tit. 23, § 500 (2017).
- 2 *N.Y. Comp. Codes R. & Regs. tit. 23, § 500.19(a) (2017)*. Exemptions apply for those with fewer than 10 employees in New York; for companies with less than \$5 million in annual revenues; and, entities with less than \$10 million in assets.
- 3 https://www.dfs.ny.gov/system/files/documents/2020/07/ea20200721_first_american_notice_charges.pdf. The DFS filed an amended complaint, available at https://www.dfs.ny.gov/system/files/documents/2021/03/ea20200721_first_american_notice.pdf
- 4 *Id.*
- 5 *Id.*, p. 33.
- 6 https://www.dfs.ny.gov/system/files/documents/2021/03/ea20210303_residential_mortgage_0.pdf.
- 7 This was not always the case. The consolidation of the New York State Insurance Department and the New York State Banking Department happened in 2011, when the state legislature and Governor Andrew Cuomo effectuated the consolidation, creating the New York Department of Financial Services.
- 8 <https://content.naic.org/sites/default/files/inline-files/MDL-668.pdf>.
- 9 The eight states are: South Carolina, Ohio, Michigan, Mississippi, Alabama, Connecticut, New Hampshire, and Delaware.
- 10 *Va. Code Ann. § 38.2-621 to 38.2-629 (2020) (West)*.
- 11 *Ind. Code Ann. § 27-2-27-1 to 27-2-27-32 (West) (2020)*.
- 12 H.B. 614 (2020).
- 13 https://content.naic.org/sites/default/files/inline-files/Model_%23668_Map06.17.20.pdf.
- 14 Bulletin 2019-14, <https://insurance.maryland.gov/Insurer/Documents/bulletins/19-14-Breach-of-Security-of-a-Computer-System-Notification-Requirement.pdf>.
- 15 *Md. Code Ann., Ins. § 4-406 (West)*.
- 16 See, <https://www.cpomagazine.com/cyber-security/cyber-insurance-firm-suffers-sophisticated-ransomware-cyber-attack-data-obtained-may-help-hackers-better-target-firms-customers/>.

F I N D Y O U R C O M M U N I T Y



TIPS
CONNECT

americanbar.org/tipsconnect