New York Law Journal
Technology Today
WWW.NYLJ.COM
An ALM Publication
VOLUME 265—NO. 108
TUESDAY, JUNE 8, 2021

Cybersecurity Enforcement Activity From NYDFS Fashions Regulatory Expectations and Suggests More Enforcement Is To Come

By **Matthew L. Levine**

A stream of cybersecurity enforcement actions have now begun to flow from the New York State Department of Financial Services (DFS), including pursuant to its cybersecurity regulation known as "Part 500." See 23 N.Y.C.R.R. §500 et al. Regulated entities and cybersecurity practitioners should take note as the agency fashions regulatory expectations and signals that more enforcement is on the way.

First issued in March 2017, Part 500 contains a two-year implementation period intended to permit regulated entities to design and implement the required "robust" cybersecurity program. DFS took a patient regulatory approach during the interim period, encouraging firms to enact an adequate cybersecurity program and cheerleading for cybersecurity generally. See Matthew L. Levine, "**Anticipating the First Cybersecurity Action from NYDFS**," *New York Law Journal* (Jan. 6, 2020).

The regulation went fully into effect in March 2019. In July 2020 this grace period came to a jarring but not unexpected halt, when DFS commenced its first cybersecurity enforcement action under Part 500. The agency has now made clear to regulated industry that Part 500's "clearly defined standards for cooperative industry compliance, robust consumer data protection, vital cybersecurity controls, [and] timely reporting of Cybersecurity Events" are ripe for continued enforcement.

Emerging Regulatory Expectations

Routine Examinations Will Lead to Enforcement: Cybersecurity has been a focus of periodic examinations conducted by DFS since at least 2017. The "first day letter"—standard document requests that kick off an examination—routinely hones in on an entity's cybersecurity and information technology systems, including risk assessment, third-party

SHUTTERSTOCK

service providers and governance. Examinations also seek to identify unreported "Cybersecurity Events," as defined in Part 500. The head of DFS' Cybersecurity Division recently indicated that the agency conducts approximately 400 to 500 examinations annually that include an emphasis on cybersecurity. It is unsurprising that routine examinations are now maturing into enforcement actions.

The first DFS cybersecurity enforcement action resulting in a Consent Order arose from a routine examination. In 2020, DFS examiners sought to confirm that Residential Mortgage Services had not submitted any "Cybersecurity Event" notifications to the agency. The company then disclosed it had indeed suffered an unreported Cybersecurity Event

MATTHEW L. LEVINE *is a partner in the white-collar defense and regulatory investigations practice at Phillips Nizer and served as the first Executive Deputy Superintendent for Enforcement for NYDFS.*

18 months earlier resulting from a phishing scam—a clear violation of the 72-hour reporting rule. Examiners also uncovered other violations of Part 500, resulting in a $1.5 million penalty and required remediation for the company.

Emphasis on Multi-Factor Authentication: Part 500 requires covered entities to have implemented multi-factor authentication (MFA) no later than March 1, 2018, yet a number of firms did not timely comply with this critical deadline. DFS' two most recent cybersecurity enforcement actions arose from successful phishing attempts by malign actors, and both scams occurred at a time the victimized company had not yet fully implemented MFA.

In the case of National Securities, an insurance company, DFS found that it had not fully implemented MFA within its email environment until August 2020. This omission resulted in successful phishing attempts in 2018 and 2019 that exposed non-public information (NPI) of National Securities' customers and facilitated theft of customer funds. For another insurance company, First Unum, DFS determined that it failed to fully implement MFA as of September 2018, a time when the company suffered a phishing attack that likewise publicly exposed customers' NPI. Both companies paid a penalty under Financial Services Law (FSL) §408(a)—$3 million and $1.8 million, respectively—and First Unum also had to incur the cost of an independent consultant to audit and report on remediation.

These actions highlight the strong emphasis placed by DFS on compliance with the MFA requirement. Superintendent Linda Lacewell stated in connection with the First Unum matter that "[t]he cornerstone of our Cybersecurity Regulation is ensuring that all private data is protected, and this is not just an aspirational goal." Similarly, the head of DFS' Cybersecurity Division, Justin Herring, emphasized during a recent webinar that these enforcement actions reflect the agency's considered view that neglecting to properly implement MFA poses a "key threat" to financial institutions.

> The agency has now made clear to regulated industry that Part 500's "clearly defined standards for cooperative industry compliance, robust consumer data protection, vital cybersecurity controls, [and] timely reporting of Cybersecurity Events" are ripe for continued enforcement.

Focus on Timely Notification: Another key focus of DFS examinations is on whether an entity reports a "Cybersecurity Event" to DFS within 72 hours, as required. An important policy objective of this provision is to permit the agency to share information received from such notifications with other regulated entities that may be vulnerable to an identical cyber-attack—*before* other entities are actually impacted by a looming threat. This was the thrust of DFS guidance issued in March 2021 following discovery of the "SolarWinds" supply-chain cyber-attack and a compromise to Microsoft Exchange Email Servers. DFS noted that reports it received, via its cybersecurity notification portal, of "unsuccessful attacks have been useful in identifying techniques used by attackers and enabling DFS to respond quickly to new threats and continue to protect consumers and the financial services industry."

Failure to comply with the 72-hour notice provision has resulted in enforcement consequences. In the enforcement action involving National Securities, DFS found that the insurer violated §500.17(a) by failing to timely notify DFS of two Cybersecurity Events occurring in April 2018 and March 2019. In the Residential Mortgage Services proceeding, DFS likewise found that the company failed to notify DFS of a Cybersecurity Event until nearly 18 months after discovery. With the large number of examinations underway of DFS entities, additional enforcement in this area is likely.

Some Open Issues for Regulated Entities and Cybersecurity Practitioners

While clarity about enforcement standards is emerging from the four cybersecurity enforcement actions commenced by DFS so far and some recent agency guidance,

open questions remain about DFS enforcement criteria.

How Many Violations Are There? One key issue relates to the number of violations that might be committed under the regulation, and what penalties may be assessed. Several mechanisms exist by which DFS can take action against an entity for a non-compliant cybersecurity program. For example, the agency can determine under the New York Banking Law, for those entities subject to it, that a licensed institution has engaged in "unsafe or unsound" conduct for cybersecurity lapses. Penalties accrue on a per-day basis, and each discrete violation can amount to a daily penalty of up to $250,000. See Banking Law §§39, 44, 44-a. In the Residential Mortgage Services matter, DFS relied on the Banking Law when finding a "safety and soundness examination" of the company uncovered "significant failures in compliance and reporting required under Sections 44 and 44-a" pertaining to cybersecurity compliance.

Because not all DFS entities are subject to the Banking Law, the agency issued Part 500 under the authority of the FSL which applies to all DFS-licensed entities including insurance companies and brokers, cryptocurrency exchanges, and online lenders. FSL §408(a) provides for a penalty of up to $1,000 per violation of Part 500; unlike the Banking Law (and some provisions of the Insurance Law), penalties are *not* assessed on a per day basis. The two most recent cybersecurity enforcement actions were against life insurance companies and DFS therefore imposed penalties pursuant to §408(a).

Yet the FSL does not define with precision what constitutes a "violation" under §408(a). Part 500 does suggest a number of potential violations tied to its requirements, such as failure to timely notify DFS of a Cybersecurity Event (§500.17(a)); failure to timely implement MFA (§500.12(b)); and failure to conduct an adequate cybersecurity risk assessment (§500.02(b)(1)). An open question may remain as to whether any specific violations under Part 500 may be subdivided further into multiple violations, sometimes referred to as the "unit of prohibited conduct" or "unit of prosecution." In the absence of an ability by DFS to charge multiple "sub-violations" of a specific violation type, the potential financial penalties faced by an institution might be modest in a particular case, and the corresponding impact of an enforcement action diminished.

> Cybersecurity remains an important policy objective for Governor Cuomo and DFS, and regulated entities and cybersecurity practitioners are likely to see a good deal more action flow from DFS before 2021 is done.

Notably, DFS has taken the position that at least one of the Part 500 violation categories may be broken down further to constitute multiple violations. In announcing administrative charges against First American Title Insurance Company last year, DFS identified violations of nine different subparts of Part 500. According to the Statement of Charges, these violations were caused by a vulnerability in an external-facing website that exposed hundreds of millions of documents containing sensitive NPI, such as customers' Social Security and bank account numbers. One of the Statement's charges (Charge VI) asserts that the company failed to timely encrypt documents containing NPI, in violation of §500.15. Another of the Statement's charges (Charge VII) alleges the company failed to implement a fully functional vulnerability management program, "thereby exposing millions of documents containing NPI to potential malicious actors," in violation of §500.02(b)(2).

The DFS press release announcing the Statement of Charges alleges "that each instance of Nonpublic Information encompassed within the charges constitutes a separate violation" of Part 500. With potentially hundreds of millions of sensitive consumer records exposed, and a maximum fine of $1,000 per violation, the fine imposed following a liability finding in this case could be astronomical. Given First American's stated intention to defend these charges, additional clarity over the definition of a "violation" under Part 500 may come from this

administrative proceeding—and a likely court battle under Article 78 should the hearing officer determine that First American is in fact liable.

Did Someone Commit Perjury? During the DFS rulemaking process, several commentators criticized the Part 500 requirement calling for either the board or a senior official of a covered entity to certify annually that the entity's cybersecurity program complies with the regulation. One commenter declared that "Section 500.17(b) manufactures potential criminal and/or civil liability for senior executives, as representatives of the Covered Entity." New York Penal Law §210.05 makes it a Class A misdemeanor (up to one year imprisonment) for a person to "intentionally make a false statement which he or she does not believe to be true under oath in a subscribed written instrument." Understandably, Part 500's certification requirement was one of its most controversial when put into effect in March 2017.

It will likely remain so. DFS has now charged the violation of making a false certification in three different matters—twice in Consent Orders and once in the pending First American proceeding. In the National Securities Order, DFS charged that the entity's "filing of a Certification of Compliance … with the Cybersecurity Regulation for the 2018 calendar year [] was false" because the company "was not in compliance with the [regulation] at the time of certification." DFS issued the same charge in its Order against First Unum, determining that the company and an affiliate "falsely certified compliance with the Cybersecurity Regulation for … 2018, in violation of 23 NYCRR §500.17(b)."

In neither case did DFS make any detailed finding of the degree of intent associated with the false certification. Any such finding was a probable point of debate in negotiations over the respective Consent Orders. That is because a strong finding of intent underlying a false certification charge might also lead to a criminal charge of perjury against members of the Board or the senior officer who falsely attested to the certification. And DFS' failure to make a criminal referral to a prosecuting authority under such circumstances might leave it open to criticism.

This issue may get a more developed treatment in the administrative hearing against First American. DFS alleges there that First American's Chief Information Security Officer certified compliance with Part 500 for the years 2017, 2018 and 2019, and that, for each of these years, First American "*was aware* there were material deficiencies in its cybersecurity program at the time it certified. As a result, the certification filed by [First American] for [each of 2017, 2018 and 2019] was false and constitutes a violation of 23 NYCRR §500.17(b)." This charging language is observably stronger regarding the level of intent than that found in the National Securities and First Unum Orders.

Looking Ahead

The hearing in the First American matter is currently scheduled for August 2021 and multiple issues relating to cybersecurity enforcement could be raised and resolved in this administrative litigation. More generally, Superintendent Lacewell noted in a recent webinar that DFS is "devoting energy" to cybersecurity enforcement, and the head of the Cybersecurity Division stated recently there may be as many as a half-dozen serious cybersecurity enforcement investigations currently in the docket. In sum, cybersecurity remains an important policy objective for Governor Cuomo and DFS, and regulated entities and cybersecurity practitioners are likely to see a good deal more action flow from DFS before 2021 is done.

Reprinted with permission from the June 8, 2021 edition of the NEW YORK LAW JOURNAL © 2021 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-256-2472 or reprints@alm.com. # NYLJ-06082021-494560