May 20, 2021

NYDFS Fines First Unum and Paul Revere Insurance Companies $1.8 Million for Violations Arising Out of Data Breaches

On May 13, 2021, the New York Department of Financial Services ("NYDFS") announced a consent order with First Unum Life Insurance Company of America ("First Unum") and Paul Revere Life Insurance Company ("Paul Revere") (collectively the "Companies"), which imposed a $1.8 million penalty for violations of NYDFS's Cybersecurity Regulation (23 NYCRR 500) ("Part 500"), including false certifications of compliance under 23 NYCRR 500.17. Following an investigation of two reported phishing incidents, the NYDFS found that the Companies violated Part 500 by failing to implement either multi-factor authentication ("MFA") or reasonably equivalent or more secure access controls, and that, for that reason, they also falsely certified compliance with Part 500 in 2018. In addition to paying the $1.8 million penalty, the Companies agreed to further improve their cybersecurity programs, including commissioning a third-party audit of its MFA controls. The violations "caused the exposure of a substantial amount of sensitive, non-public-personal data" belonging to the Companies' customers, "including thousands of consumers nationally and hundred in New York." [1]

This settlement comes on the heels of a $3 million consent order in April with National Securities Corporation ("NSC"), also a licensed insurance company, which failed to implement MFA, and did not notify the NYDFS of two data breaches. In addition, the NYDFS determined that NSC had also falsely certified compliance with Part 500 in 2018—this was the NYDFS's first enforcement action for such a false certification.

Background

Part 500 is a set of regulations that requires financial companies to implement specific security safeguards to better protect consumer data privacy. Certain provisions became effective in 2017, with other provisions entering into effect on a rolling basis thereafter. Part 500 applies to Covered Entities, defined as registered entities "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."[2]

---

1 New York Department of Financial Services, "Press Release – DFS Superintendent Lacewell Announces Cybersecurity Settlement with First Unum and Paul Revere Life Insurance Companies" (May 13, 2021), available at https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202105131

2 23 NYCRR 500.1(c)

Among other requirements, Part 500 requires Covered Entities to report certain classes of cybersecurity events to the NYDFS within 72 hours and to certify compliance with Part 500 on an annual basis.[3] A Cybersecurity Event is broadly 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."[4] Since March 1, 2018, Part 500 has also required Covered Entities to implement MFA or reasonably equivalent or more secure controls whenever there is outside access to a Covered Entity's internal networks.[5] MFA requires a user to provide two or more verification factors to gain access to a website, network, or other online resource and is widely used as the first line of defense in preventing cybercriminals from gaining unauthorized access to information systems, such as through phishing emails.

The enforcement action by the NYDFS against the Companies is only the fourth enforcement action under Part 500. The first enforcement action, filed in July 2020 against First American Title Insurance Company, is still ongoing.[6] The second enforcement action, concluded in March 2021, involved a Maine-based mortgage banker licensed in New York, Residential Mortgage Services, Inc. ("RMS"). The action resulted in a settlement under which RMS paid a $1.5 million fine and committed to a remediation plan for failing to both investigate and notify the NYDFS of a phishing-related data breach, and for not conducting a comprehensive cybersecurity risk assessment. In April 2021, the NYDFS resolved the third enforcement action under Part 500, citing NSC's failure to implement MFA, or reasonably equivalent or more robust controls, in addition to NSC's failure to timely notify the NYDFS of two phishing cyber events between 2018 and 2019, as grounds for the $3 million penalty. Due to these violations, the NYDFS determined that NSC also falsely certified compliance with Part 500 for 2018.

NYDFS's Findings

First Unum, the subject of the most recent enforcement action under Part 500, discovered a data breach on September 20, 2018, after a phishing email was sent to a large number of employees. Following an investigation, First Unum determined that non-public consumer information was accessible by an unauthorized third party between June 1, 2018, and October 20, 2018. First Unum notified the NYDFS of this data breach, which also impacted Paul Revere. At the time of this data breach, neither First Unum nor Paul Revere had fully implemented MFA for their respective email systems as required under Part 500.

First Unum discovered a second data breach on October 10, 2019, when an employee reported that suspicious emails that he did not draft were being sent out by his email program. After a prompt

3 23 NYCRR 500.17

4 23 NYCRR 500.1(d)

5 23 NYCRR 500.12

6 Our memorandum discussing that enforcement action is available at https://www.paulweiss.com/media/3980393/30july20-dfs-part-500.pdf.

investigation, First Unum found that another phishing attack had compromised fifteen email accounts between October 1, 2019, and October 10, 2019. First Unum also notified NYDFS of this data breach. At the time of the second data breach, First Unum had implemented MFA in its email environment, but a misconfiguration error allowed an unauthorized third party to bypass MFA and gain access to employees' email accounts.

Violations and Penalties

NYDFS concluded that the Companies violated several sections of Part 500:

- First Unum and Paul Revere did not fully implement MFA in their email systems for all users until August 29, 2019, and no reasonably equivalent or more secure access controls were approved in writing by the Companies' CISO, in violation of 23 NYCRR 500.12(b).
- First Unum's MFA misconfiguration allowed a number of IP addresses to bypass the MFA setting between July 2019 and October 2019, in violation of 23 NYCRR 500.12(b).
- First Unum and Paul Revere falsely certified compliance with Part 500 for 2018, in violation of 23 NYCRR 500.17(b), as neither entity had fully implemented MFA that year.

As a result of these violations, the NYDFS required the Companies to pay a $1.8 million penalty and improve their cybersecurity frameworks. Among other things, the Companies are required within 120 days to provide a comprehensive written Cybersecurity Risk Assessment of their information systems to NYDFS, and to submit to a third party audit of their MFA controls.

Implications

Although the NYDFS's enforcement of Part 500 is still at an early stage, a few themes have emerged from these enforcement actions that help to clarify what types of violations that the NYDFS may be focused on.

- First, based on the last two enforcement actions, it appears that NYDFS will now be citing false certifications of compliance as an additional violation in Part 500 enforcement actions. In the April and May 2021 enforcement actions, the NYDFS not only outlined how First Unum, Paul Revere, and NSC failed to implement MFA, but also determined that the resulting non-compliance with Part 500 meant that the companies' prior certification of compliance had been false. This false certification was cited as an additional violation, on top of the underlying violations. In the March 2021 action against RMS, the NYDFS noted that RMS's violations "directly undermine[d] the accuracy" of its Certification of Compliance but did not tack on false certification as a separate and distinct violation. Notably, NYDFS has yet to cite failure to certify under Part 504 in its AML/sanctions-related enforcement actions.

- Additionally, by failing to notify NYDFS of a successful cybersecurity event, a Covered Entity may be subject to fines by NYDFS. For example, fines were imposed on RMS and NSC after the NYDFS's investigation uncovered data breaches that were not reported in a timely manner.

- Finally, although it is clear that successful data breaches, such as the phishing attacks against RMS and NSC, should be reported to the NYDFS, it remains to be seen what types of unsuccessful attacks should be reported, and the NYDFS's guidance appears to leave this determination up to companies. The NYDFS has acknowledged that Covered Entities are the targets of cybersecurity events on a regular basis, many of which are unsuccessful. To help clarify this point, the NYDFS FAQs state while "most unsuccessful attacks will not be reportable" the NYDFS "seeks the reporting of those unsuccessful attacks that, in the considered judgment of the Covered Entity, are sufficiently serious to raise a concern."[7] Further, "in making a judgment as to whether a particular unsuccessful attack should be reported, a Covered Entity might consider whether handling the attack required measures or resources well beyond those ordinarily used by the Covered Entity, like exceptional attention by senior personnel or the adoption of extraordinary non-routine precautionary steps." Thus, while the NYDFS concludes that most unsuccessful attacks are not reportable, the burden is on the Covered Entity to determine whether an unsuccessful attack is serious enough to report.

While enforcement of Part 500 is still in its early stages, the NYDFS has shown that it will use its authority to incentivize companies in the financial sector to strengthen their cybersecurity practices and notify consumers and regulators in the event of a broad range of cybersecurity events. The NYDFS's enforcement posture underscores the importance of promptly responding to cybersecurity and data breach incidents and implementing a robust cybersecurity framework.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

---

7 New York Department of Financial Services, "FAQs: 23 NYCRR Part 500 – Cybersecurity" available at https://www.dfs.ny.gov/industry_guidance/cyber_faqs

H. Christopher Boehning
+1-212-373-3061
cboehning@paulweiss.com

Michael E. Gertzman
+1-212-373-3281
mgertzman@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Richard C. Tarlowe
+1-212-373-3035
rtarlowe@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

Associate Cole Rabinowitz and Staff Attorney Bertie Cheng contributed to this Client Memorandum.